Ontology Development for Run-Time Safety Management Methodology in Smart Work Environments Using Ambient Knowledge

Mahsa Teimourikia, Mariagrazia Fugini

Via Ponzio 34/5, Department of Electronics, Information, and Bioengineering (DEIB), Politecnico di Milano, Milan, Italy

Abstract

This paper presents the development of a decision support system for run-time safety management in Smart Work Environments (SWEs). Our approach consists of four main phases: i) definition of the basic steps of a methodology for run-time safety management; ii) development of an ontological knowledge-base of safety in work environments; iii) definition of constraints on the ontology based on organizations' safety protocols; iv) communication of relevant information to each actor in the safety management team. We propose a generic ontological model of safety expertise, based on Occupational Safety and Health Regulations (OSHA), that is employed as Knowledge required in our safety management methodology based on the MAPE-K (Monitor-Analyze-Plan-Execute and Knowledge) loop. We present the RAMIRES (Risk-Adaptive Management in Resilient Environments with Security) tool, implementing this methodology. RAMIRES is developed as a dashboard, supporting the safety management team in understanding the risk and its consequences, and to support decision making in risk treatment. RAMIRES interacts with the SWE and the safety management team (actors) in order to: i) communicate the risks and preventive strategies to actors; ii) obtain more data about the observed areas to understand the risk and its consequences; and iii) execute the automatic preventive strategies and support actors in the execution of human-operated preventive strategies. In this paper, we show the details on concepts designed in the safety ontology and illustrate how these concepts can be extended to provide an abstract model of a specific use case. Furthermore, we propose the definition of constraints on the ontology using logic-based rules. Finally, we discuss the advantages and limitations of the proposed methodology regarding the resilience of the environment.

Keywords:
safety; Internet of Things; smart work environment; decision support system; risk prevention; risk management; adaptive security.

1. Introduction

Risk management in critical and risk-prone environments based on events that arise on the fly is still an open issue (Hollnagel, 2014). Considering that about 90% of workplace injuries can be traced back to unsafe work practices and behaviors (EU-OSHA, accessed: 2016), proper safety management is essential to treat the risks that arise based on unsafe activities and situations, to which we refer to as *run-time safety management*. Until a few years ago, monitoring activities of workers and their safe usage of work equipment was very challenging if not impossible (Gubbi et al., 2013). Nowadays, Smart Work Environments are making it possible to monitor activities, workers, tools, and machinery in workplaces, with a potential exploitation for safety management.

As an emerging technology, Internet of Things (IoT), has provided a promising opportunity in the appearance of cyber-physical systems (Ahmad et al., 2016) and "Smart Work Environments" (SWEs) (Almada-Lobo, 2016; Lee, 2015), by providing the infrastructure that enables advanced services by interconnecting physical and virtual "things" based on the existing and evolving ubiquitous technologies. In the SWE, smart objects interact based on semantic services (De et al., 2011). From the architectural point of view, an SWE evolves on Service-Oriented Architecture (SOA) that provides a decentralized architecture to facilitate the adoption of IoT Services to define the interaction among the smart objects (Colombo et al., 2014). IoT Services include sensing and control of the physical "things". Therefore, in an SWE that employs IoT Services, *safety* and *security* are important issues that should be tackled carefully, to guarantee the safety of the workers while protecting the security of critical objects and infrastructures (Hossain et al., 2015; Sadeghi et al., 2015; Sicari et al., 2015).

Safety management in an SWE is a knowledge-intensive task (Zhang et al., 2015). In addition to the safety knowledge that captures the safety expertise, the following should also be considered: i) the knowledge about work activities, safety-related skills and experiences of workers; ii) tools and machinery used for an activity; and iii) the environment's characteristics in which the work activity is being performed in. Different work activities and use of tools and machinery, as well as the workers' ability to perform tasks safely, may imply different potential risks. In order to conduct run-time safety management in risk-prone SWEs, safety knowledge should be represented in a computer-interpretable and semantically inferable way, which should be computationally feasible for run-time performance.

Because of dynamic characteristics of the SWE and considering that various monitored data are available in this environ-

ment, by an ontology, dynamically sensed data can be properly analyzed and used for safety management. The purpose of this paper, is to introduce a methodology for adopting the existing risk management standard ISO 31000:2009 (Purdy, 2010) in run-time safety management in the SWE based on the MAPE-K (Monitor-Analyze-Plan-Execute and Knowledge) loop that is usually employed in dynamic and self-adaptive systems (Iglesia and Weyns, 2015). Considering the guidelines and directives in Occupational Safety such as OSHA (OSHA, accessed: 2016) and the European version EU-OSHA (EU-OSHA, accessed: 2016) and risk management standards such as ISO 31000:2009 (Purdy, 2010), we design a generic ontology, for Knowledge management in MAPE-K loop, to capture the safety expertise needed for various steps in safety management, namely, risk identification, assessment, and treatment. It is worth mentioning that the goal of this work is not introducing a risk assessment and analysis method, but to provide a methodology to adopt various existing risk assessment methods for automated or semi-automated safety management at run-time based on the existing risk management standards.

The safety ontology captures the safety knowledge in different steps of the proposed MAPE-K loop (Iglesia and Weyns, 2015). Using the MAPE-K pattern we try to map the ISO 31000:2009 to be adopted in run-time safety management.

To clarify the use of the proposed ontology, a scenario is considered based on a real-world JHA document available on (MIA, accessed: 2016). The adopted JHA document is extended to create a use case including the concepts related to the SWE. Using this use case, we show how this generic safety ontology can be instantiated to build an abstract model for specific use cases and we show how it is possible to define constraints on the introduced ontology based on organizations' safety protocols.

Moreover, to facilitate risk treatment in the SWE, it is critical to design a dashboard that enables communication of relevant information to different actors in the safety management team in a meaningful way. We introduce *RAMIRES (Risk-Adaptive Management in Resilient Environments with Security)* as a safety management dashboard that implements the proposed MAPE-K methodology and provides an interface to communicate relevant information for assisting the safety management team in treating Risks.

We consider security (Whitman and Mattord, 2011) for the SWE, using an adaptive Access Control System (ACS) (Hu et al., 2015) we introduced previously in (Fugini et al., 2016). While security might be an issue in some organizations, a risk-adaptive ACS is in place to control the access of different actors to elements that are available via the dashboard. Also, actors and the RAMIRES need to be authorized to be able to execute actions on resources in the SWE. In this paper, we show the interactions of RAMIRES with the ACS for adapting security rules based on the risk description provided by RAMIRES; and we illustrate how RAMIRES and actors get authorized for various actions by the ACS. Finally, we add details about the implementation of the introduced approach and discuss the challenges and limitations in the implementation process.

This paper is organized as follows: Section 2, discusses the state of the art. In Section 3, the methodology for run-time safety management and the ontological model of safety are introduced and examples are illustrated. Section 4, details RAMIRES as a Safety Management System that implements the proposed methodology with a dashboard for decision support in risk treatment, and gives a scenario for showing its functionalities and interactions. In Section 5, we make a discussion on advantages and limitations of the presented methodology and tools. In Section 6, implementation details are described. And finally, Section 7, concludes the papers and discusses future works.

2. Related Work

Occupational safety as defined in OSHA (OSHA, accessed: 2016) is concerned with health and welfare of workers in the work environments. More specifically, occupational safety management is an area concerned with the management of risks arising in work environments because of faults in machinery, unsafe behaviors of workers, ignoring the safety procedures and unsafe work conditions such as high level of noise or unprotected toxic materials (Hoyos and Zimolong, 2014). In recent years, the adoption of IoT-based technology in work environments has led to the emergence of the Smart Work Environment (SWE) which is also referred to as Smart Factory (Wang et al., 2016). Currently, the availability of data that are sensed from the ambient, to people and "smart objects" have facilitated the extraction of knowledge about what happens in the environment (Bessis et al., 2013). Thanks to the "Industry 4.0" paradigm (Lee, 2015), and to the increasing adoption of Internet of Things (IoT), advanced sensing and controlling IoT Services are available in SWEs that enable monitoring of the environment and automated execution of required actions on smart objects (Lee, 2015).

Languages and knowledge representation technologies in different forms such as logic and ontologies, are studied to capture knowledge on various domains, including knowledge that enables evaluation of safety domain (Zhang et al., 2015). Semantic reasoning is one of the most used technologies for facilitating automated and semi-automated safety management (Wang and Boukamp, 2011). Ideally, an ontology should capture a shared understanding of the domain of interest, and in addition, provide a formal and a machine-readable model of the domain. In recent years, ontologies have been used as a way to share, reuse and process various parts of *safety domain knowledge* specific to different use-cases (Zhang et al., 2015; Lu et al., 2015; Zhang et al., 2014; Wang and Boukamp, 2011).

Wang and Boukamp (2011) consider Job Hazard Analysis (JHA) (OSHA, accessed: 2016), as the basis of their safety model for construction work environments, with the purpose of automating the analysis of JHA documents. They propose a framework that adopts knowledge about activities, job steps, and risks from the JHA documents and includes ontological reasoning mechanisms for identifying safety rules applicable to given work activities.

In another work, Lu et al. (2015) design an ontology-based knowledge model for automated construction of safety checks

that aims at integrating safety planning and construction execution planing by linking safety knowledge to construction processes and products. In this work, the authors introduce the concept of precursor in their ontology model, that represents conditions, events, and sequences that preceded and led up to an accident. Precursors are basically the work team, the physical system and the environment.

While IoT technology has facilitated the gathering and analysis of ambient data that can be used in various contexts such as identification of risks, safety management in SWEs is an open issue, as discussed in (Smith, 2013; Bahr, 2014). The feasibility of semantic approaches for automated safety knowledge management procedures, is proven by the mentioned researches. However, there are some limitations regarding run-time safety management in the SWE as following.

Firstly, based on the reviewed literature and to the best of our knowledge, there is a lack of a generic methodology for run-time safety management that can be used in various application areas and industries. Secondly, considering SWEs, the new challenges that they introduce and their new requirements regarding safety, a methodology should be designed to tackle these challenges and needs. Moreover, safety management incorporates various steps based on the standards and directives (i.e., OSHA) that should be clarified and adopted in the introduced methodology, specifically considering the SWE requirements. Finally, incorporating the balance between safety and security is a challenging task and needs to be tackled with care as explained in what follows.

In the SWE, problems of security and privacy arise, when, based on the risks identified in the environment, more privileges would be needed (compared to those that are normally available based on the security rules) to access the required data or IoT Services, for safety management purposes. For example, the safety management team might need to view the exact position of workers at risk. This privilege is not available in safe situations for privacy purposes. Therefore, security should be adapted dynamically so that privileges would be granted upon need and later be revoked. In this direction, Sicari et al. (2014) tackle security for IoT applications. Bertino et al. (2014) discuss the trade-offs between the strength of security and privacy, and the assurance of the availability of required information for decision making about risk. In a previous work (Fugini et al., 2016), we have introduced an approach for the adaptiveness of the security policies to the risks that arise in the SWE.

With the goal of improving flexibility in security authorizations by adapting the security rules with respect to the identified risks, this paper leverages the security model proposed in (Fugini et al., 2016). Our proposed adaptive security model is in the streamline of access control (Hu et al., 2014), and in particular adopts the Attribute-Based Access Control (ABAC) model (Hu et al., 2014) to dynamically grant and revoke privileges based on risks identified in the SWE. In this work, we try to show the interactions of the introduced safety management methodology with the ACS in relation with the adaptive security rules.

Finally, to achieve *resilience* in the SWE, we analyze the proposed methodology using the environment resilience indicators defined in the literature to highlight the limitations for future extensions. Resilience is more and more considered as a measure of safety in an environment (Bergström et al., 2015). Resilience corresponds to a particular incident and the ability to recover from it (Takahashi et al., 2013). It is usually measured in a qualitative way employing some indicators or by empirical studies that are done on data gathered from questionnaires. The resilience indicators are studied in works such as (Lee et al., 2013). In this paper, we also consider the SWE resilience, and we use the indicators introduced in the literature (Lee et al., 2013), adapted to be used in the SWE, to qualitatively analyze our proposed run-time safety methodology.

3. Run-Time Safety Management Methodology

In this section we introduce the approach to run-time safety management methodology. We first start with defining the basic terminologies that are used later on:

3.1. Preliminary Definitions

Safety in our work refers to occupational safety and health as defined by OSHA (OSHA, accessed: 2016). Occupational Safety is concerned with health and welfare of the workers and employees engaged in an industry or an organization.

RAMIRES is a tool that implements the run-time risk management methodology we introduce in this paper. In what follows, we detail the entities composing RAMIRES that are then used in the ontological model of the safety knowledge. Here, we highlight the relationships between RAMIRES, the SWE, and the ACS. In the SWE, *Hazardous Event* represents out-of-range parameters that are monitored using sensor networks. The SWE contains sensors and actuators that monitor the ambient data and manipulate the *things*.

According to ISO 31000:2009, hazardous events initialize the risk analysis phases where they are assessed to determine the risks and their consequences. For doing this, there might be a need to request more details on the ambient data gathered from the SWE to be able to conduct risk analysis. Then, risk consequences need to be evaluated and later be treated by preventive strategies.

In RAMIRES, we only consider *risk prevention* through preventive strategies. This is because computer-based systems are not reliable tools for treating crisis and emergencies such as fire, explosion and etc., as they might be damaged themselves during the crisis. We consider preventive strategies to be executed either by RAMIRES (if automatic) or by actors in the safety management team (if human-operated).

3.2. Objectives

In this paper, our aim is to create a unified approach for run-time safety management. To do this, we define the following Objectives:

O1. Defining an ontology to capture safety expertise using generic classes of entities in the SWE (i.e., workers, tools and machinery, work activities and the environment) and their relation with the hazardous events, risks and their consequences, and preventive strategies to treat the risk.

O2. Defining an abstract system model by specializing generic ontology classes to create instances related to a specific industry.

O3. Identifying a way to instantiate the resulting classes at run-time to create a concrete model representing the current state of the work environment.

O4. Specifying a way to analyze this model for the purpose of run-time safety management.

In this paper, we focus on O1 and O2, and leave the rest for future works.

3.3. Methodology Overview

Previously, we considered a MAPE (Monitor-Analyze-Plan-Execute) loop for risk assessment and adaptive security (Fugini et al., 2012b, 2016). In this work, we extend this model as we refer to ISO 31000:2009, as a risk management standard, that introduces the risk management steps at a high level. Here, we map these steps into our MAPE loop for the purpose of run-time safety management, where:

1) *Monitor* is the step in which the SWE entities are monitored for risk identification. According to ISO 31000: 2009 (Purdy, 2010), monitoring is the process in which relevant elements are monitored to signal a risk.

2) *Analyze* is the second step where risk assessment should be conducted. According to ISO 31000:2009 risk assessment includes: i) *risk identification* to understand what risks could happen, how, when, and why; ii) *risk analysis* for developing and understanding each risk and its consequences and the likelihood of those consequences; iii) *risk evaluation* for making a decision about the priority and the intensity (i.e., level) of the identified risk.

3) *Plan* is the next step which should include planning of preventive strategies based on the results of the previous phases. This is a part of the Risk Treatment process in ISO 31000:2009, where preventive strategies are selected to eliminate or to reduce the risk. Preventive strategies can be selected from the existing pre-defined strategies (usually defined in JHA documents), or are adaptively selected based on a risk treatment model (Fugini et al., 2012b). Planning preventive strategies involves evaluation and selection from the existing options by performing a cost-benefit assessment of the new risks that might be generated by each option and then prioritizing the selected treatment through a planned process. The output of this step should be the prioritized list of preventive actions that are needed to treat the risk assigned to the responsible actors in the safety management team.

4) *Execute* is the final step in the loop, which has the goal of automatically executing or assisting the execution of the preventive strategies. Preventive strategies are categorized as automated and human-operated. *Automated strategies* are the ones that can be executed automatically (e.g., activating the alarms, stopping a press machine). Whereas, *human-operated strategies* need the involvement of safety management actors to be executed (e.g., evacuation of an area, the safety inspection of a machinery, etc.). In this step, the automated strategies are executed and the safety management actors are supported to execute the preventive strategies assigned to them.

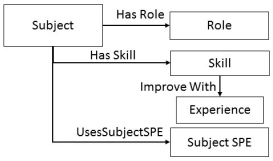

Figure 1: Details on Subject in the Safety Ontology

In this work, we extend this methodology to MAPE-K (Monitor-Analyze-Plan-Execute and Knowledge) loop (Iglesia and Weyns, 2015). The Knowledge, based on O1, is represented by a generic safety ontology, that captures the safety concepts in different steps of the introduced MAPE-K loop.

3.4. O1: The Generic Safety Ontology

The starting point to perform run-time safety management is to design a core *safety model* with its generic classes capturing the safety knowledge (O1). To achieve this, OSHA (OSHA, accessed: 2016) and EU-OSHA (EU-OSHA, accessed: 2016) regulations are considered as the knowledge sources for identifying relevant concepts for our safety ontology. These include occupation safety regulations, reports and best practices. In the following, we present the safety ontology concepts related to each step of the MAPE-K loop.

3.4.1. The Safety Ontology Concepts for Monitor Step of MAPE-K Loop

To start with, we have extracted the main relevant concepts in the SWE that should be monitored for run-time safety management. First, we consider the entities in the SWE that both might cause risks and also need to be protected from the risks.

1) *Subjects*, that are the workers in the environment. They might make mistakes, forget to use safety garments, misuse tools and machinery or ignore the safety procedures. According to OSHA and EU-OSHA, different industries should employ Training Needs Assessment (TNA) (OSHA, accessed: 2016), in order to identify and define the safety and health training needed for performing a specific work activity. The training that each subject gets is defined as his/her skills which improve with experience and practice. Furthermore, in each industry the hierarchy of organizational roles are defined that indicate the range of responsibilities and abilities of the employees (i.e., subjects). Therefore, the organizational role of the subject has an important impact on his/her ability to perform the work activities safely. Moreover, for each work activity, depending on the tools and machinery used in that activity, according to OSHA and EU-OSHA, the subject is advised to use certain Safety Protection Elements (Subject-SPE) for protection from the potential risks).

Important concepts, which can affect the safety are extracted from OSHA and EU-OSHA directives and regulations. Therefore, *Subjects* are represented by: i) their organizational roles; and ii) their safety related skills and experience gained from organizational safety training; and iii) the safety protection elements that they are currently using. Figure 1 depicts the subject as a class with its properties in the ontology.

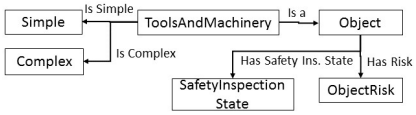

Figure 2: Details on Object in the Safety Ontology

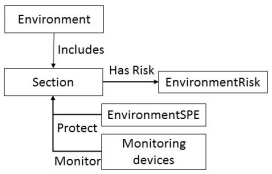

Figure 3: Details on Environment in the Safety Ontology

2) *Objects*, and more specifically tools and machinery in the work environment, can be faulty, can function improperly due to poor maintenance or due to failures and defects.

Tools and machinery are the devices and physical machinery that the workers use to perform their tasks, such as trucks, presses, hammers and so on. These devices are risk-prone and the fault in their functioning, or their misuse can create risks. Not all the tools and machinery are equipped with sensors and actuators that facilitate the execution of remote actions on them. Hence, the safety model represents only those tools and machinery that support the implementation of safety control strategies aiming at switching the device off or changing the device state to avoid the risks. Tools and machinery are classified as *simple* (e.g., motors, electricity plugs, wires, pipes and etc.) and *complex* (e.g., truck, press machine, and so on). A complex tool or machinery consists of a set of simple ones, being modeled by means of the safety controls of its components. For instance, a press machine is described using its components' safety controls such as the availability of stop button for emergency stopping the machine. Also, a truck is typically a complex machinery due to its various components such as the engine, the wheels and etc. In the safety model, the following properties are represented for a tool or machinery: i) the current safety guards and controls; ii) the overall risk identified for the tool or machinery; and iii) the current state of the safety inspection on the device. Figure 2, depicts the Object class and its properties as the part of the overall safety ontology.

3) *Environment*, which is the surveilled area where the presence of hazards (e.g., existence of combustible gases and chemical agents) or specific characteristics of the environment (e.g., unprotected roof-tops, or slippery surfaces) might lead to potential risks. Environment includes Sections as its building blocks and is represented considering: i) the potential risks for different Sections; ii) available safety protection elements in the Section; and iii) the sensors and monitoring devices available at each Section to monitor the critical conditions such as air pollution levels, temperature and etc.

4) *Activities*, which are work procedures carried out by the Subjects. The Activities can be broken down into simple *tasks* that are the building blocks of that Activity. Each Task in the Activity is associated to potential risks that are usually defined

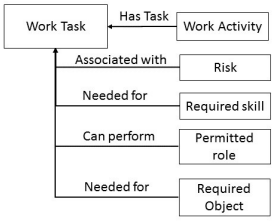

Figure 4: Details on Activity in the Safety Ontology

in JHA documents. Activities include various tasks as their building blocks that have properties including: i) potential risks for each task; ii) required skills from the subject who performs the task; iii) permitted roles to perform the task considering the subjects' organizational role; and iv) required objects for performing the task. Figure 4 shows the Work Activity class as a part of the safety ontology.

To enable monitoring the described entities using sensing IoT Services, we define the concept of *monitoring devices* that are the sensors, cameras, wearable monitoring tools and etc. Two types of monitoring devices are represented in the safety model: passive and active. *Passive devices* are the monitoring tools that are employed for sensing IoT Services and are used for capturing ambient data, such as temperature and humidity values, and for monitoring the work activities. *Active devices* provide the ability to operate a change on the state of the environment using actuators (i.e., used for control IoT Services), e.g., air conditioning, pressure control tools, and etc.

Finally, the properties of the SWE entities (i.e., Subject, Object, Environment and Work Activity) together with the values monitored by the Monitoring Devices (i.e., ambient data, and current work activities being performed) are the outputs of the *Monitor* step of the MAPE-K loop which will be employed as the input of the next step which is *Analyze*.

3.4.2. The Safety Ontology Concepts for the Analyze Step of MAPE-K Loop

The main purpose of the Analyze step of the MAPE-K loop in our methodology is risk assessment. In this step, based on the inputs provided by the Monitor step we conduct risk assessment that includes risk identification, risk analysis and risk evaluation. In order to capture the knowledge in this step, we extract the required concepts from ISO 31000:2009, OSHA, and EU-OSHA standards and regulations.

As a part of the risk identification, monitored data and the SWE entity properties are evaluated to identify reasonably foreseeable hazards that may give rise to a risk. This incorporates detection of out of range values that are considered essential in risk identification. To highlight the important values for identifying the hazardous event, safety experts in different industries can define *Safety Indicators (SIs)* considering the safety needs of the specific industry. We consider four categories for (SIs), namely: *Subject-specific SIs* (e.g., skill level, decreased mental alertness, fatigue, loss of concentration); *Object-specific SIs* (e.g., object risk level, and failure rate); *Environment-specific SIs* (e.g., fall rate); and *Activity-specific SIs* (e.g., injury rate,

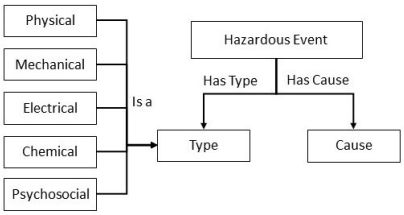

Figure 5: Details of Hazardous Event in the Safety Ontology

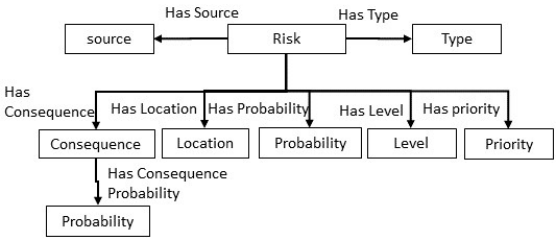

Figure 6: Details of Risk in the Safety Ontology

proximity of hazardous activities to one another, and compatibility of work activities).

Based on the defined SIs, *Hazardous Events* are identified. The hazardous event is characterized by the *type* that indicates the specific hazard and the entity that is causing it (i.e., the Subject, Object, Environment, and Work Activity). The following types of the hazardous event are considered based on OSHA: i) *physical* (e.g., fire, heat, radiation); ii) *mechanical* (e.g., problems in machinery and devices); iii) *electrical* (e.g., voltage, current, static charge); iv) *chemical* (e.g., flammables, toxic elements); v) *psychosocial* (e.g., stress, fatigue).

The *Hazardous Event* might lead to a *Risk* that has a *type* (e.g., fire) and a *source* (e.g., gas pipe). This can be checked in the risk analysis process that eventually calculates the probability of the *Risk*. In case the *Hazardous Event* indicates a *Risk*, further analysis should take place in order to identify the consequences of the risk (e.g., fatal injury of workers, non-fatal injury, occupational disease, harm to infrastructure, and etc.) and the probability of those consequences. Furthermore, during the next step, namely risk evaluation, the decision is made about the priority of attention and the level (i.e., the intensity) of the identified *Risk*. Moreover, the *location* in the environment affected by the *Risk* is another concept that is required in the risk treatment. As depicted in Figure 6, the mentioned concepts are defined as part of the main safety ontology.

3.4.3. The Safety Ontology Concepts for Plan Step of MAPE-K Loop

In the Plan step, the main goal is deciding about *Preventive Strategies (PSs)* as a part of risk treatment process in ISO 31000:2009. The Preventive Strategies as the main concept in this step can be characterized based on the SWE entity that it is applied to, namely, i) *Subject-specific PS* (e.g., informing the person at risk, controlling the correct usage of subject safety protection elements such as hard hats, gloves, face shield and etc.); ii) *Object-specific PS* (e.g., scheduling

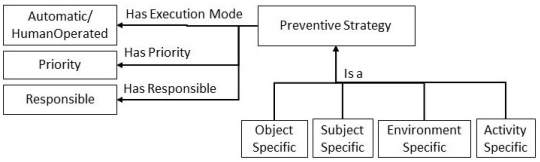

Figure 7: Details of Preventive Strategy in the Safety Ontology

safety inspection for machinery, turning off the machinery, etc.); iii) *Environment-specific PS* (e.g., adjusting the ambient temperature, starting air conditioning, evacuation, etc.); and iv) *Activity-specific PS* (e.g., inform supervisors about unsafe work activities). Furthermore, in this step the following properties are calculated: the Priority of the PS; its Responsible that shows the person or system responsible for executing the PS; and its Execution Mode that shows if the PS can be executed automatically or by one of the safety management team actors. Figure 7 shows the main concepts of the Plan step as a part of the main ontology.

3.4.4. The Safety Ontology Concepts for the Execute Step of the MAPE-K Loop

In the Execute step, the main goal is realizing the planned strategies from the previous step. As previously mentioned, in the plan step the Preventive Strategies for treating the *Risk* are listed together with their execution mode (i.e., automatic and semi-automatic); the responsible entity (if it is automatic it refers to the Control-based IoT-Service to execute the actions automatically; otherwise, if it is human-operated, this points out the person in charge of the safety management team for executing the action); and the priority that highlights the importance and the order in which the strategies should be executed.

Since safety is a highly critical concept, the use of completely-automated safety management is not recommended nor achievable, in our opinion, because even the most accurate algorithms for risk identification and assessment can be error-prone. Also, some task requires human confirmation and intervention. In this regard, automated procedures to assist safety management with the help of a Decision Support System (DSS) (Power et al., 2015) can be very useful. Therefore, in this work, a DSS is proposed that, based on the proposed methodology and a machine-aided approach for safety management, suggests the relevant safety preventive strategies for risk treatment, leaving the final decision about the execution of the critical tasks to the safety management team.

In the Execute Step, we consider the execution of automatic PSs that are realized using the control-based IoT Services. Having a security system controlling the access to the IoT Services, the safety management system should be authorized to employ the required IoT Services for executing the automatic preventive strategies. IoT Services as a part of safety ontology is categorized into sensing and control services. Sensing services are used in the Monitor step and the Control services are employed in the Execute step.

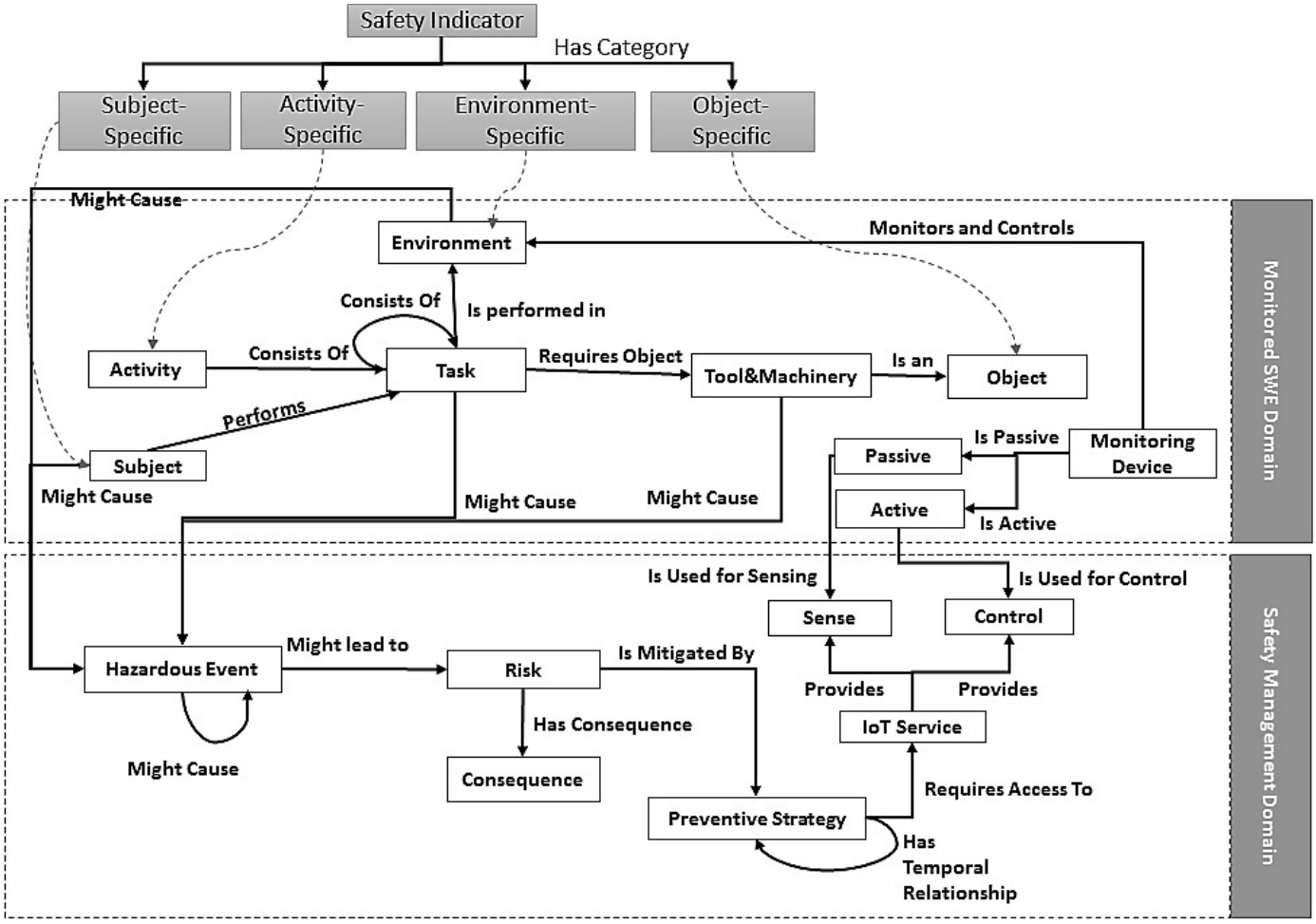

Figure 8: The Overall Safety Ontology

3.4.5. The Ontology for Safety Knowledge

Finally, here we discuss the final safety ontology employed in our MAPE-K loop for run-time safety management. For clarity, class properties and some of the subclasses that are explained in details previously are omitted to present the relationship between the main concepts (i.e., classes) in the safety ontology. Figure 8 depicts the overall Safety ontology incorporating the concepts that were described previously. For clarity, Figure 8 illustrates the concepts in two domains of *Monitored SWE* and the *Safety Management*, where the *Monitored SWE Domain* contains the classes related to the SWE that are monitored and if needed manipulated via sensing and control IoT Services. On the other hand, the *Safety Management Domain* includes classes needed for an efficient safety management according to the ISO 31000:2009. Furthermore, Safety Indicators are defined in four categories that are: *Subject-Specific*, *Object-Specific*, *Environment-Specific*, and *Activity-Specific*, which define the relevant aspects that should be monitored based on the needs of specific industries.

As shown in Figure 8, work tasks (represented with the *Task* class) might consist of other work tasks. Moreover, the *Hazardous Event* class represents a hierarchical relationship between hazardous events as one *Might Cause* another. Also, preventive strategies are usually executed in an order based on their priorities. Therefore, as shown in Figure 8, the *Preventive Strategy* class is denoted by *Has Temporal Relationship* to highlight the temporal order of execution.

3.5. O2: The Abstract Safety Management System Model

Using the safety ontology, an abstract model can be created using OWL subclasses to capture the entities in a specific SWE and describing the specific safety concepts for different work activities. The resulting model is adopted as an input for RAMIRES, where the knowledge encoded in the abstract system model is used in run-time safety management.

The introduced safety ontology model uses OWL classes for design time modeling. Here, the OWL instances are used to model the run-time SWE composition respecting safety. In what follows, we use an example adopted from a real-world scenario JHA document and adapted for including concepts of the SWE.

3.5.1. An Illustrative Example

Figure 9 shows an example, helping to illustrate the abstract model in the SWE. The example is created around a work environment where humans perform work activities with tools in

a potentially dangerous environment, like an industrial plant. Here, instances of the safety ontology classes model a scenario taken from OSHA directives for Forklift Operations. However, this example is adapted for the SWE and some details are emitted for the sake of simplicity.

In this example, *Operating Forklift* is the work activity that includes work tasks, such as *Driving Lift Truck*, that is performed by a *Forklift Operator* in the *Work Environment* and requires *Lift Truck* as an object. The *Forklift Operator* has the organizational role of *Operator*; has *Safe Work Procedures* skill with *High* level of experience; and uses a *Hard Hat* as a safety protection element. We consider *Hazardous Event* and *Risk* as the same class (i.e., assuming that a hazardous event always leads to a risk). *Driving Lift Truck* might cause several risks, namely, *Tripping Over*, *Colliding Other Vehicles*, and *Hitting Pedestrians* who in our case are other workers.

For simplicity, we focus only on the risk for *Hitting Pedestrians*, which has a *High* level of intensity, and has *Injury/Death* as its consequence with a *High* likelihood. In case the *Hitting Pedestrians* risk is identified, the preventive strategies suggested for treating it are: *Alarm the Operator to Stop*, that has an execution mode indicating that it is *Human Operated*, has *High* priority, and has *Forklift Operator* as the responsible; and *Stop the Truck Automatically*, that has an execution mode indicating that it is *Automatic*, has *High* priority, and has RAMIRES as the responsible. For the latter, as it is an automatic strategy, RAMIRES requires access to the *Remote Stop Control IoT Service* that allows RAMIRES to automatically stop the truck. Moreover, using sensing IoT Services, it is possible to *Sense the Distance of Truck and Pedestrians*.

3.5.2. Indicating Constraints on the Ontology

The above example is helpful in describing the ontology knowledge of a work activity scenario. However, it cannot be used to express the constraints based on organization's safety policies (e.g., mandatory use of specific safety garments for specific actions). The Semantic Web Rule Language (SWRL) is a standard language, developed by W3C that is used to express rules as well as logic (W3C, 2016) in Semantic Web. The rule language is adopted to specify the safety rules and constraints for run-time safety management, as it can be easily integrated with the safety ontology. To show the use of SWRL in defining safety rules related to the defined abstract model for Forklift Operations we use some examples as follows:

Rule 1. Considering work task "Driving Lift Truck" which is shown as a variable (?*wt*) that is performed by subject (?*s*), the subject should wear a hard hat otherwise the subject should be alarmed to stop.

Considering Rule 1, the SWRL safety rule would be:

$$R_1 : DrivingLiftTruck(?wt) \wedge WTperformedBy(?wt, ?s) \wedge WTSNotUseSPE(?s, HardHat) \rightarrow PSHasAction(AlarmOperatorToStop, ?s)$$

Here, *DrivingLiftTruck*, *WTperformedBy*, *WTSNotUseSPE*, and *PSHasAction*, are the ontology classes and object relations that are defined in the safety ontology. *DrivingLiftTruck* is the subclass of *Object* representing the "Driving Lift Truck"; *WTperformedBy*, *WTSNotUseSPE*, and *PSHasAction* are object relations in the ontology that indicate the following:

- *WTperformedBy* indicates the *Driving Lift Truck* in the *Work Task* class is performed by the worker ?*s* in the *Subject* class.
- *WTSNotUseSPE* indicates the worker ?*s* (who is performing the *Driving Lift Truck* work task as indicated by *WTperformedBy*) is not using the *SPE*, the *Hard Hat*.
- Finally, *PSHasAction* shows the action *Alarm Operator to Stop* as a part of the *Preventive Strategy* class that is applied on the worker ?*s*. In simpler worlds, the action is to alarm worker who is driving the lift truck to stop driving.

In this example, HardHat, and AlarmOperatorToStop, are named individuals that are defined specifically for the scenario.

Rule 2. Considering work task "Driving Lift Truck" (?*wt*), where there is a sensing IoT Service (?*sd*) that measures the distance of the truck from the workers (?*d*). If d is less than 5 meters, then the driver is alarmed with a sound.

Considering Rule 2, the SWRL safety rule would be:

$$R_2 : DrivingLiftTruck(?wt) \wedge WTperformedBy(?wt, ?s) \wedge SenseDistanceService(?sd) \wedge SIoTMeasureValue(?sd, ?d) \wedge swrlb : lessThan(?d, 5) \rightarrow PSHasAction(AlarmWithSound, ?s)$$

In this rule, it is indicated that if the sensed distance of the truck from workers is less than 5 meters the truck should be stopped automatically. In this example, *SIoTMeasureValue* is an object relation that shows sensing IoT service ?*sd* has value ?*d*. The built-in functions or predicates in SWRL specifications are used in this example, namely, *swrlb:lessThan*. The predicate *swrlb:lessThan(?d,5)* indicates "if the distance d is less than 5 meters or not". Here, *AlarmWithSound* is a named individual representing the action "alarm the driver with a sound".

4. RAMIRES: The Safety Management Dashboard

In this Section, we explain RAMIRES as the safety management dashboard that is developed as an extension to our previous works in (Fugini et al., 2012a,b; Fugini and Teimourikia, 2015; Fugini et al., 2016). RAMIRES implements the proposed methodology and assists actors in decision making about risks. In addition, when necessary, RAMIRES interacts with the SWE to acquire more information during the risk and consequence assessment processes. Since some IoT services needed to control and sense the SWE are sensitive, RAMIRES also interacts with the adaptive ACS to be granted the necessary permissions.

The goal of RAMIRES is to assist in achieving resilience in the SWE. Therefore, RAMIRES's overall goal is not about avoiding risks, as they can happen at any time, but it is to maintain and regain a stable state prior, during and after an event (Bergström et al., 2015). To achieve resilience, minimization of failure, early detection and treatment of hazards, minimization

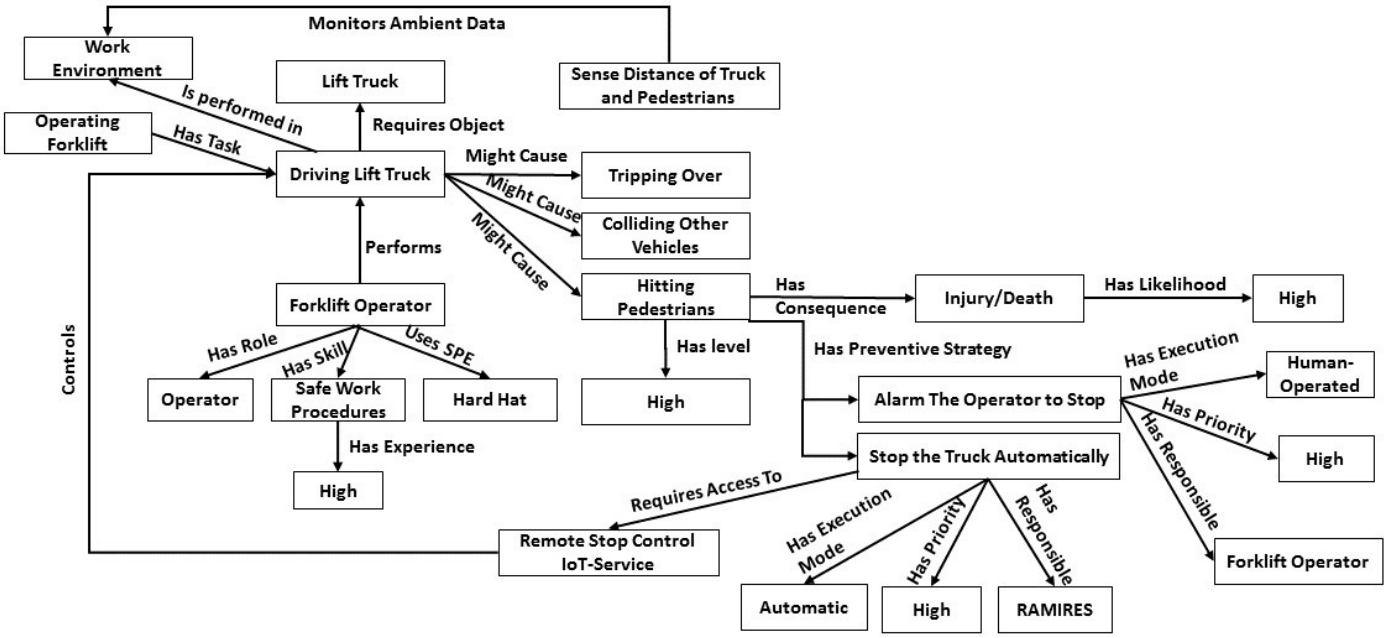

Figure 9: An Illustrative Example: Forklift Operations

of consequences of a risk, and flexibility are required. By continuously monitoring the environment early detection of hazards is possible. Moreover, early and full assessment of the risk and consequences, planning of preventive strategies, and facilitating the collaboration between actors improves the treatment of risk.

RAMIRES is a general framework implementing the introduced methodology. It is general in the sense that the proposed methodology and the corresponding ontology are introduced at a high level so that they can be extended and be used in different application areas and industries. And hence, various monitoring, risk assessment and evaluation methods may be implemented on top of RAMIRES. Therefore, here we consider the inputs and outputs of different phases and consider the steps as black boxes.

To perform in a resilient manner, the following functionalities are considered in RAMIRES, which are reported in Figure 10, where a Business Process Management diagram shows assessment and decisions steps and the involved components. The *Gateway, Monitoring and Control System* (simply referred to as the gateway) connects RAMIRES to the SWE. As depicted in Figure 10, when there is a hazardous event, the gateway reports it causing RAMIRES to start the risk and the consequence assessment processes. Interactions with the environment may be needed to characterize and assess the risk and its consequences.

For instance, we consider a scenario, where a subject is using the press machine without the safety guards that remove the hands of the subject from the descending die. In this scenario, a hazardous event is reported. During the risk analysis process, RAMIRES considers the skills of the subject performing the task, the machinery in use (i.e., the press machine) and etc. However, for planning preventive strategies, RAMIRES needs to know the exact position of the subject at risk which

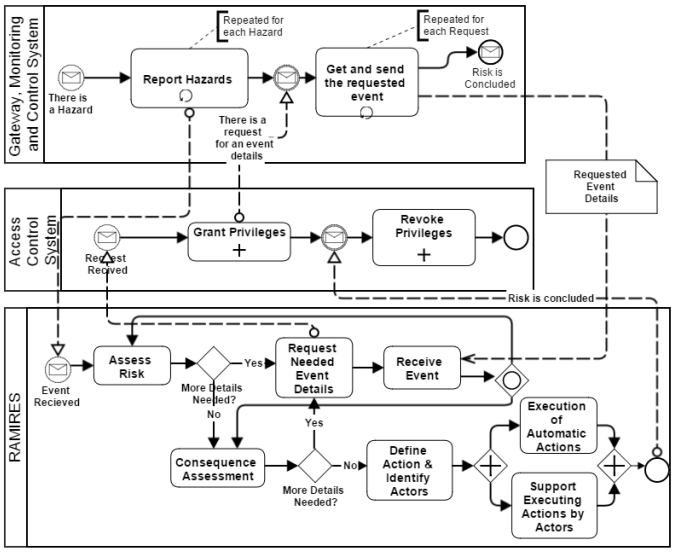

Figure 10: Safety management steps adopted by RAMIRES and interactions with the ACS and the SWE (Taken from (Fugini and Teimourikia, 2015))

was not provided. So, RAMIRES will ask to receive the required data. RAMIRES manages such interactions requesting new events from the environment as depicted in Figure 10. RAMIRES then proposes preventive strategies. And it executes the automatic actions while supporting the execution of human-operated strategies. In case an actor requests to view a monitored data item needed in the process of risk treatment, if the adaptive security rules allow such view, RAMIRES asks for more events, and updates the dashboard so that the requesting actor is enabled to view the requested data.

In this dashboard, useful information (e.g., map of the en-

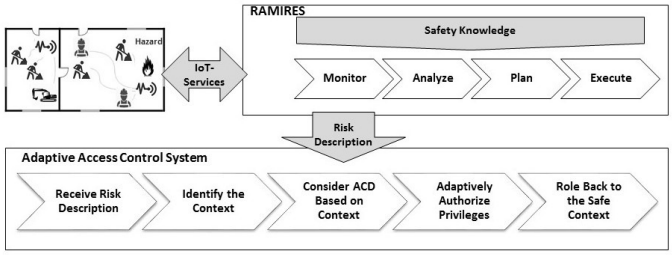

Figure 11: *RAMIRES* functional architecture: tasks and interactions

vironment, location of the risk, and sensed ambient data) are illustrated to assist decision making in face of risks. The architecture of RAMIRES is depicted in Figure 11. RAMIRES employs the sensing and control IoT Services to either sense the ambient data, or to execute the automatic preventive strategies. As IoT Services are protected using the adaptive ACS, RAMIRES needs authorization to access the required IoT Services.

As presented in Figure 10, ACS manages security issues related to the requests, by adaptively granting and revoking permissions. ACS defines security rules enforced to authorize actors or RAMIRES to use IoT Services or access data. For instance, it grants privileges to safety management teams to observe an area in more details to view the positions of workers at risk.

The adaptive ACS is introduced in details in our previous work (Fugini et al., 2016). To summarize, the ACS is based on the Attribute-Based Access Control (ABAC) model, considering security and risk attributes for Subjects, Objects and Environment. Security rules are defined based on these attributes to permit or deny access to IoT Services. Rules are organized in Access Control Domains that indicate the applicable security rules for different contexts (e.g., safe context, fire risk context, etc.). In order to adapt the security model based on the identified risks, meta-rules are defined that consider the risk description received from RAMIRES, and will make changes in attributes or change the context, as shown in Figure 11.

During risk treatment, *dashboard views* for each actor, in the safety management team, are generated according to the dynamically-adapted security rules. The authorization result of the ACS based on adaptive security rules are tuples with the following format: *<actor, resource, action>* representing which actions are permitted to be used by an actor on a resource. Using the authorization results, it is possible to create the personalized views.

The categories of information to be shown in the personalized dashboard views are predefined, namely, the following can be shown on the dashboard: tools and machinery as the objects; ambient data from passive monitoring devices; a map of the environment; localization data on the persons; risk-related data such as type, level, likelihood, location and consequences with its risk map; and the human-operated preventive actions recommended by RAMIRES with their priority and the responsible actor.

In what follows, we indicate a scenario and then show a prototype of RAMIRES in this scenario.

4.1. Risk Treatment Scenario in SWE

We set a scenario used to show RAMIRES functionalities. Considering an SWE, such as a smart plant or smart production industry, we assume that, in the Monitor step, sensing IoT Services are available to detect the presence of flammable gas using passive sensors. RAMIRES uses the Safety Ontology (Knowledge) in the Analyze step, to derive the presence of flammable gas (that relates to the risk of fire), and identifies the Risk attributes, namely: level; location of fire (and possible affected areas); and consequences and their likelihoods. During this step, considering the Safety Ontology, some values might be missing, so RAMIRES has to query the environment to obtain more information about what is happening in the environment. After computing the risk description in this step, RAMIRES sends it to the ACS so that relevant adaptations are applied to the security rules. At the same time, RAMIRES plans the preventive strategies in the Plan Step. Then, it simultaneously executes the automatic strategies and supports the execution of human-operated strategies.

In this scenario, we assume having three actors in the safety management team: a Risk Responsible (RR), a Risk Operator (RO), and a Risk Team Head (RTH). The ROs can be grouped in teams dynamically when the risk arises, and are assigned a RTH. As actors need to be authorized to use IoT Services or access required information, their security attributes and access privileges are managed by the ACS.

As depicted in Figure 12, different information is displayed to the RR, ROs and the RTH respectively, according to their privileges, and based on the results of security authorizations.

To clarify, we set some examples, considering one of the actors in our scenario. The security authorization results (i.e., $< Actor, Resource, Action >$) for RR are as follows:

$< RR, C1, View >$
$< RR, C2, View >$
$< RR, C1, ZoomInCamera >$
$< RR, H1, ViewHumidityValue >$
$< RR, G1, ViewGasContentValue >$
$< RR, T1, ViewTemperature >$
$< RR, Tool, ViewStatus >$
$< RR, Tool, ViewStatusHistory >$
$< RR, Map, ViewMap >$
$< RR, Map, ViewHazardOnMap >$
$< RR, Map, ZoomInMap >$
$< RR, RiskDescription, ViewRiskDescription >$
$< RR, RiskDescription, ViewHistory >$
$< RR, RiskDescription, ViewList >$
$< RR, RiskMap, ViewRiskMap >$
$< RR, Workers, ViewPosition >$
$< RR, Actors, ViewPosition >$
$< RR, PreventiveStrategy, ViewAll >$

According to the authorization results, the dashboard that is presented to the RR shows the environment map with the positions of the hazard. The RR can zoom-in to view more details

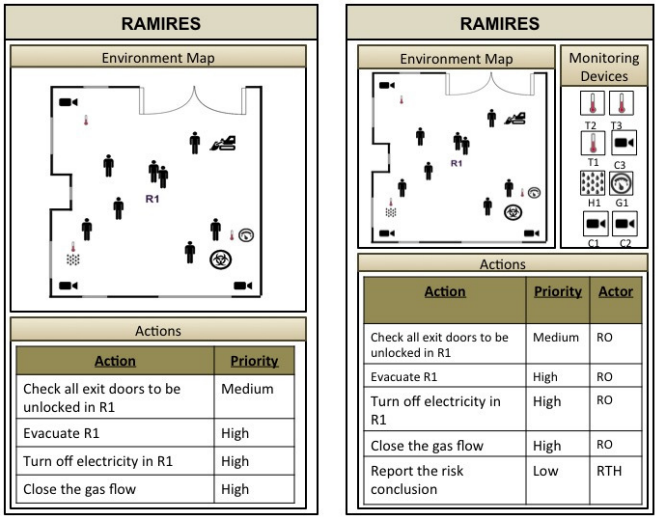

Figure 12: Sample dashboard for the RO (left-hand side), and for the RTH (right-hand side)

on the selected part of the map. Furthermore, RR is able to view the risk map that is generated in *RAMIRES*. The RR is also able to view: the status of tools and machinery, and the history of their status data; current and previously recorded data from the sensors and monitoring devices; the positions of persons in the affected environment by risk and the safety management actors on the field; and also the history of previous risks that happened in the environment. Moreover, RR is able to view the complete list of the preventive strategies suggested by RAMIRES, their priorities and responsible actors assigned to them.

On the other hand, the RO and the RTH have their own views of the dashboard, as reported in Figure 12. The RO can only view the preventive strategies proposed to him/her with their priorities, and the map of the environment with the anonymous locations of the persons on it, together with the position of the monitoring devices and hazardous events. Instead, the RTH can also view the preventive strategies recommended to RO and the current values of the monitoring devices to be able to treat the risk properly.

5. Discussion

In this Section, the goal is to discuss strengths and limitations of the proposed approach and of RAMIRES regarding the resilience of the environment. We also discuss the role of uncertainty in this work, at the end of this Section.

We consider the indicators introduced by Lee et al. (2013) and Bergström et al. (2015) to analyze RAMIRES in its contribution in achieving the resilience of the environment. Lee et al. (2013) and Bergström et al. (2015) introduce qualitative indicators for evaluation of resilience in the categories of *situation awareness*, *management of keystone vulnerabilities*, and *adaptive capacity*.

Situation awareness refers to being aware of what that is happening in a specific environment. Lee et al. (2013) consider the following indicators to measure situation awareness:

1) *Roles and responsibilities* refer to the capability of organizations to give a clear picture of the crisis and clarify the role of each person in such situation. Regarding this aspect, RAMIRES can be used as an interface that communicates the preventive strategies based on the roles of each actor, helping to get a clear view of the risk treatment strategies that should be executed by each person. One of the limitations of RAMIRES is that it cannot count for unavailability of actors and how another available actor should be selected to fill the role.

2) *Understanding and analysis of hazards and consequences* refer to the efforts that organizations make for risk assessment and its communication. In RAMIRES, the methodology for safety management is used in automated risk assessment using the knowledge provided by the ontology that would be updated with real-time data provided by sensing IoT Services. Utilizing computer-readable knowledge can advantage organizations in low-cost and faster risk assessments. Furthermore, RAMIRES communicates the results of risk assessments to the actors.

3) *Connectivity awareness* refers to the knowledge of the organizations about external risks that might effect them. RAMIRES does not consider elaborating on external risks.

4) *Insurance awareness* refers to identification of alternative resources and safe guards to be adopted to minimize the damages or take *corrective actions* when preventive strategies were not enough to prevent the risks. RAMIRES as a computer-aided tool only focuses on risk prevention. Since the main goal is to assist treatment of risks of safety, computer systems may not be considered completely reliable when facing a crisis such as fire, earthquake and etc. Therefore, an alternative approach should be proposed for these situations.

4) *Recovery priorities* refers to the ability to define and prioritize the recovery solutions (that we refer to as preventive strategies) of the organization and to communicate it to the actors. One of the goals of RAMIRES is to prioritize the preventive strategies and communicate them to the actors. However, it does not yet consider the specific indication of the organization's recovery priorities.

5) *Internal and external situation monitoring and reporting* that considers the ability of the organizations in proactive monitoring and early warning of emerging risks. This is one of the main advantages of RAMIRES that proactively monitors the environment for risks and enables timely communication of risks and the corresponding preventive strategies to the actors.

6) *Informed decision making* refers to ability of organizations to make decisions based on up-to-date data and on the experts' knowledge. In RAMIRES, continuous monitoring of environment provides the up to date data on the current situation regarding safety. Moreover, the ontology captures the safety expertise and makes it available for non-expert users.

Another category of indicators proposed by Lee et al. (2013) is the *management of keystone vulnerabilities*, which focuses on norms and values of organizations in identifying vulnerabilities that lead to risks. Here are the main indicators in this category:

1) *Planning the strategies* refers to the plan and development of strategies to identify and treat the vulnerabilities. At this stage, RAMIRES is designed to assist in treating the risks, however, it can easily be extended to consider vulnerabilities man-

agement both in the ontology and as an assessment and communication tool.

2) *Participation in exercises* considers the adoption of simulation exercises for practice response plans and validate the strategies. In the methodology, simulated data can be used for training of the personnel. In the use case scenario, an example of the abstract model of a specific situation is demonstrated.

3) *Capability and capacity of internal resources* evaluates the ability of the organization to treat risks internally. RAMIRES enables organizations to implement their own risk assessment and planning strategies in a semi-automated way and facilitates decision making for risk treatment for internal safety management team.

4) *Capability and capacity of external resources* evaluates the connectivity to external entities and ability of the organizations to efficiently use external resources in times of emergency. Currently, RAMIRES does not consider the communication of risks with external entities or the management of agreements with external organizations for emergency management.

5) *Organizational connectivity* refers to ability of the organizations to actively manage their links with external organizations they have to work with in time of crisis. RAMIRES does not offer the ability for management of links with external organizations.

6) *Robust processes for identifying and analyzing hazards* evaluates organizations in their ability in timely detection, reporting and analysis of hazards. This is one of the strengths of the methodology introduced in this paper that enables the proactive monitoring of hazards and automated analysis. In this way, the organizations do not need to rely on individuals to detect and report the hazards.

7) *Staff engagement and involvement* refers to staff involvement in effective risk management processes. RAMIRES introduces a dashboard to communicate the risks to the actors and to assist in decision making. This facilitates the cooperation among actors by providing them with relevant information and strategies via the dashboard.

The last category that is considered by Lee et al. (2013) is *adaptive capacity*, which focuses on the ability of organizations to adapt and manage the balance between stability and change. The following indicators are analyzed in this category:

1) *Silo mentality* focuses on the sense of teamwork and the facilitation of cooperation of the staff. In (Fugini et al., 2016), we discuss how RAMIRES as a risk management system with adaptive security can be used in cooperative risk treatment by enabling the clear indications of responsibilities and roles for the actors.

2) *Communications and relationships* refers to organization's ability to recover their relationships with external entities such as suppliers and customers. RAMIRES does not offer the possibility to manage the relations with external entities.

3) *Strategic vision and outcome expectancy* refers to organizations mission and visions and re-evaluation of decisions for achieving the overall goals. Evaluation of past decisions and learning from them is a limitation that should be considered in future works.

4) *Information and knowledge* refers to the availability of information and knowledge for decision making. The ontology proposed in this work can capture the safety knowledge and RAMIRES can be used to communicate relevant information in a secured way.

5) *Leadership and creativity* focuses on the role of organizations for encouraging innovation and creativity, e.g., by rewarding creative staff. RAMIRES considers hierarchies of actors' organizational roles as shown in this paper. Specifically, based on the security rules, RAMIRES lets the leader actor to view the preventive strategies assigned to other actors to assist decision making and the organization of the teams. However, RAMIRES does not consider rewarding the creative actors.

6) *Developed and responsive decision making* refers to accessibility of persons in authority when important decisions need their confirmation and the utilization of qualified persons in decision making. RAMIRES provides the actors with relevant information for decision making. However, it does not yet consider the qualifications of decision makers and the communication of the decisions to people in authority for confirmations.

Another important aspect that should be considered is the treatment of uncertainty in decision making for risk management, specially for high-consequence risks with large uncertainties (Aven et al., 2013). Uncertainty should be considered at various levels (Aven et al., 2013; Flage et al., 2014), starting from the uncertainty caused by unavailability or inaccuracies in the monitored data and experts knowledge that is used in the methodology; the uncertainty resulted from the inaccuracies of risk assessment models; and finally the uncertainty of the resulted estimations and information that is going to be used for the final decision making.

6. Implementation of RAMIRES

This section describes the details of implementation and development of RAMIRES. Firstly, we start with the development and design of the ontology. Then we continue with the implementation details of RAMIRES dashboard and ACS. Finally, we discuss the integration of the modules.

6.1. Designing the Ontology

The Web Ontology Language (OWL) is used to specify safety ontology concepts. For implementation, Protégé 5.0 beta is employed to define the OWL-based safety ontology. To implement the SWRL rules a plugin for Protégé is used which is called SWRLTab which provides SWRL rule editor to implement the constraints on the ontology that reflect the safety regulations of a specific industry (e.g., the temperature of a specific machinery should be below a values).

The development of ontology can be a challenging task as the knowledge, information and resources are not always well defined and found in one specific source. Various OSHA directives had to be reviewed to extract the relevant concepts, and the design of the ontology is recursively updated to best fit the concepts. Yet, the ontology must be further reviewed by experts in the domain to verify its correctness and completeness, which, in our case, is left for future works.

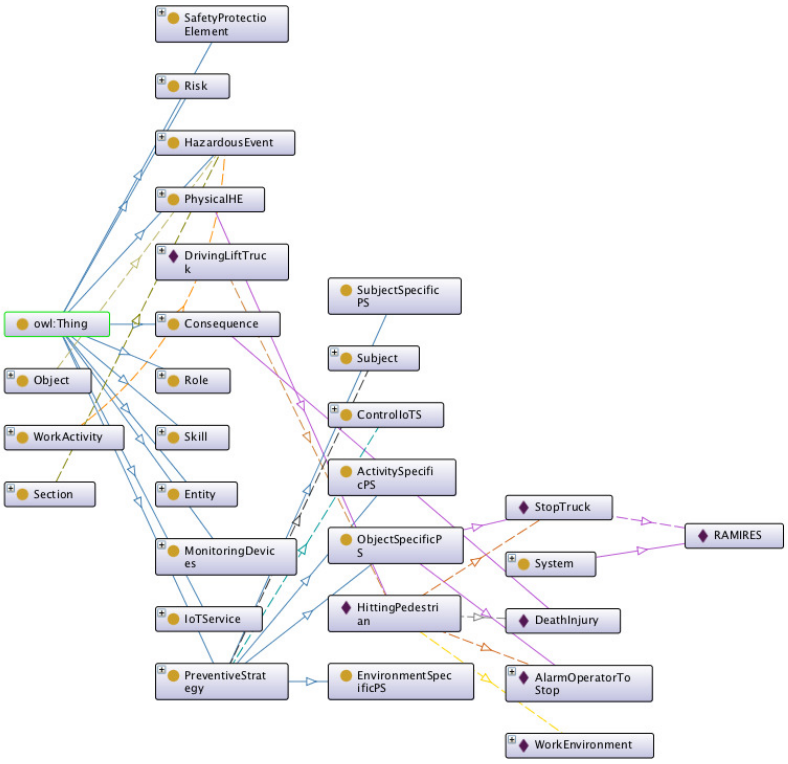

Figure 13: Screen shot, showing the developed ontology classes and the instances of the illustrated example in Protégé

Another challenge that we faced during the development process of the ontology was that in various resources it is not possible to find unique definitions and use of concepts. Different sources use different vocabularies or use the same concepts for representing different meanings. We referred to OSHA directives and ISO 31000:2009 to extract the concepts. As future works, we consider defining mappings between synonym concepts to provide a more general ontology.

For designing SWRL rules as constraints on the ontology, Drools-based rule engine is selected since it provides a convenient interface with Java that was used in implementation of a prototype of RAMIRES. Moreover, Protégé 5.0 beta automatically provides graphical user interfaces as forms that can be used to create the instance of the classes for designing the abstract model of a scenario or use cases for safety management.

To check the consistency of the designed ontology, a Description Logic reasoner called HermiT (version 1.3.8.418) is used to automatically check the formal consistency of the ontology and verify that it is minimally redundant. Figure 13 shows the ontology classes (circles) and their instances (diamonds) created in Protégé. The plus sign indicates that the classes can be expanded to view their subclasses and instances. Not all classes and their instances are expanded for sake of readability.

6.2. *Implementation of RAMIRES dashboard*

This work extends the risk management system proposed by Fugini et al. (2012b). In (Fugini et al., 2012a,b) the architecture of the web-based risk management tool based on MAPE methodology is described and it is implemented as a web-based application using Java. We extend this tool to incorporate knowledge provided by the ontology (considering the MAKE-K loop). RAMIRES only supports predefined instantiations of the ontology, while the real-time instantiations of concepts is not implemented yet. One of the main challenges here is the evaluation and validation of this tool while real-world data and use cases are not yet openly available for smart work environments. This is one of the main challenges in risk management in general as organizations either do not gather and save data on risks or they do not tend to make this data publicly available to be used in studies.

6.3. *Implementation of Adaptive Access Control*

In this work, we adopted risk-adaptive security to control the access of actors to represented information on the dashboard of RAMIRES. The risk-adaptive security model is explained in more details in (Fugini et al., 2016) and is developed on top of Balana (WSO2, accessed: 2016) which is an implementation of ABAC access control model. Balana is extended to incorporate adaptiveness to risks using Event-Condition-Action (ECA) rules (see Fugini et al. (2016) for more details).

The security rules are defined using XACML 3.0 policy language (Parducci et al., 2011). To facilitate the definition and analysis of ECA rules by security experts, a XML-based structure similar to XACML 3.0 is introduced (see Teimourikia et al. (2016)).

6.4. *The Integration of Implemented Modules*

Integration of various modules that are developed separately and on top of diverse frameworks is very challenging. In the

methodology introduced based on MAPE-K loop, the inputs and outputs of each step are clearly defined to facilitate adoption of various methods for monitoring, risk analysis and assessment, planning and execution of preventive strategies. Java is used as the main programming language for implementation of modules introduced in this work. Protégé automatically generates the Java code related to the defined ontology, its instances and the rules that are used to integrate the ontology in the previously developed risk management tool. Balana is also an open source framework developed using Java. We develop an interface to Balana where the access requests are sent as an input and authorization decisions are generated and returned as the result.

To provide data for simulations a database is designed based on PostGIS 9.3 that enables spatial queries. The architecture of this database is detailed in (Fugini et al., 2016). To communicate the results of spatial queries on PostGIS to RAMIRES, we adopt GeoJSON, an open standard format for representing and communicating spatial data based on JavaScript Open Notation (JSON).

7. Conclusions and Future Works

This paper has made a step towards introducing a methodology for run-time safety management of Smart Work Environments (SWEs), based on existing risk management standards (i.e., ISO 31000:2009) and proposing a dashboard as a tool to assist the safety management team. RAMIRES is proposed as a dashboard that implements the proposed methodology where risk can be communicated to actors to help them understand its consequences and make decisions, and where risk managers are guided in performing risk mitigation strategies. Moreover, to capture the safety expertise, and to facilitate automated and semi-automated risk management, we proposed a generic safety ontology based on OSHA and EU-OSHA. We showed the concepts that are the building blocks of this ontology used as the knowledge base for the Monitor, Analyze, Plan, and Execute steps of the MAPE-K loop. We also showed that the instances of the generic classes of the safety ontology can be created to design an abstract model of a specific SWE for safety management. And we also provided an illustrated example of applying constraints on the designed abstract model.

In this paper, RAMIRES is presented as a dashboard able to request/receive more information from the environment to decide the best preventive strategies for risk treatment. We have presented the overall architecture of RAMIRES and have illustrated its interactions with the SWE, actors and access control system along the phases of a safety management and decision making in risk treatment.

As future works, we plan to conduct interviews with occupational safety experts to further evaluate the ontology content. We will also continue with the defined objectives to propose a methodology to instantiate the ontology classes at run-time to be able to create an abstract model of the current state of the environment on the fly. And, we will work on a methodology to analyze the proposed ontology for run-time safety management. Moreover, other extensions will be considered to resolve the limitations of the methodology and of the tool with respect to resilience of the environment as discussed in this paper. More importantly, uncertainty is an important concept that should be considered in decision making and in the risk management process.

References

Ahmad, A., Paul, A., Rathore, M. M., Chang, H., 2016. Smart cyber society: Integration of capillary devices with high usability based on cyber–physical system. Future Generation Computer Systems 56, 493–503.

Almada-Lobo, F., 2016. The industry 4.0 revolution and the future of manufacturing execution systems (mes). Journal of Innovation Management 3 (4), 16–21.

Aven, T., Zio, E., Baraldi, P., Flage, R., 2013. Uncertainty in risk assessment: the representation and treatment of uncertainties by probabilistic and non-probabilistic methods. John Wiley & Sons.

Bahr, N. J., 2014. System safety engineering and risk assessment: a practical approach. CRC Press.

Bergström, J., van Winsen, R., Henriqson, E., 2015. On the rationale of resilience in the domain of safety: A literature review. Reliability Engineering & System Safety 141, 131–141.

Bertino, E., Ghinita, G., Kantarcioglu, M., Nguyen, D., Park, J., Sandhu, R., Sultana, S., Thuraisingham, B., Xu, S., 2014. A roadmap for privacy-enhanced secure data provenance. Journal of Intelligent Information Systems 43 (3), 481–501.

Bessis, N., Xhafa, F., Varvarigou, D., Hill, R., Li, M., 2013. Internet of Things and Inter-cooperative Computational Technologies for Collective Intelligence. Springer.

Colombo, A. W., Karnouskos, S., Bangemann, T., 2014. Towards the next generation of industrial cyber-physical systems. In: Industrial cloud-based cyber-physical systems. Springer, pp. 1–22.

De, S., Barnaghi, P., Bauer, M., Meissner, S., 2011. Service modelling for the internet of things. In: Computer Science and Information Systems (FedCSIS), 2011 Federated Conference on. IEEE, pp. 949–955.

EU-OSHA, accessed: 2016. European Agency for Safety and Health at Work. `https://osha.europa.eu/en`, [Online; accessed 25-January-2016].

Flage, R., Aven, T., Zio, E., Baraldi, P., 2014. Concerns, challenges, and directions of development for the issue of representing uncertainty in risk assessment. Risk Analysis 34 (7), 1196–1207.

Fugini, M., Raibulet, C., Ramoni, F., 2012a. Strategies for risk facing in work environments. In: Computer and Information Sciences II. Springer, pp. 425–431.

Fugini, M., Raibulet, C., Ubezio, L., 2012b. Risk assessment in work environments: modeling and simulation. Concurrency and Computation: Practice and Experience 24 (18), 2381–2403.

Fugini, M., Teimourikia, M., 2015. Ramires: Risk adaptive management in resilient environments with security. In: WETICE Conference (WETICE), 2015 IEEE 24th International. IEEE.

Fugini, M., Teimourikia, M., Hadjichristofi, G., 2016. A web-based cooperative tool for risk management with adaptive security. Future Generation Computer Systems 54, 409–422.

Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M., 2013. Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems 29 (7), 1645–1660.

Hollnagel, E., 2014. Safety-I and safety–II: the past and future of safety management. Ashgate Publishing, Ltd.

Hossain, M., Fotouhi, M., Hasan, R., et al., 2015. Towards an analysis of security issues, challenges, and open problems in the internet of things. In: Services (SERVICES), 2015 IEEE World Congress on. IEEE, pp. 21–28.

Hoyos, C. G., Zimolong, B., 2014. Occupational safety and accident prevention: behavioral strategies and methods. Elsevier.

Hu, V. C., Ferraiolo, D., Kuhn, R., Schnitzer, A., Sandlin, K., Miller, R., Scarfone, K., 2014. Guide to attribute based access control (abac) definition and considerations. NIST Special Publication 800, 162.

Hu, V. C., Kuhn, D. R., Ferraiolo, D. F., 2015. Attribute-based access control. IEEE Computer 48 (2), 85–88.

Iglesia, D. G. D. L., Weyns, D., 2015. Mape-k formal templates to rigorously design behaviors for self-adaptive systems. ACM Transactions on Autonomous and Adaptive Systems (TAAS) 10 (3), 15.

Lee, A. V., Vargo, J., Seville, E., 2013. Developing a tool to measure and compare organizations resilience. Natural hazards review 14 (1), 29–41.

Lee, J., 2015. Smart factory systems. Informatik-Spektrum, 1–6.

Lu, Y., Li, Q., Zhou, Z., Deng, Y., 2015. Ontology-based knowledge modeling for automated construction safety checking. Safety Science 79, 11–18.

MIA, accessed: 2016.

OSHA, accessed: 2016. Occupational Safety and Health Administration. `https://www.osha.gov/`, [Online; accessed 25-January-2016].

Parducci, B., Lockhart, H., Rissanen, E., 2011. Extensible access control markup language (xacml) version 3.0. OASIS Std., August.

Power, D. J., Sharda, R., Burstein, F., 2015. Decision support systems. Wiley Online Library.

Purdy, G., 2010. Iso 31000: 2009-setting a new standard for risk management. Risk analysis 30 (6), 881–886.

Sadeghi, A.-R., Wachsmann, C., Waidner, M., 2015. Security and privacy challenges in industrial internet of things. In: Proceedings of the 52nd Annual Design Automation Conference. ACM, p. 54.

Sicari, S., Cappiello, C., De Pellegrini, F., Miorandi, D., Coen-Porisini, A., 2014. A security-and quality-aware system architecture for internet of things. Information Systems Frontiers, 1–13.

Sicari, S., Rizzardi, A., Grieco, L., Coen-Porisini, A., 2015. Security, privacy and trust in internet of things: The road ahead. Computer Networks 76, 146–164.

Smith, K., 2013. Environmental hazards: assessing risk and reducing disaster. Routledge.

Takahashi, T., Emura, K., Kanaoka, A., Matsuo, S., Minowa, T., 2013. Risk visualization and alerting system: Architecture and proof-of-concept implementation. In: Proceedings of the first international workshop on Security in embedded systems and smartphones. ACM, pp. 3–10.

Teimourikia, M., Marilli, G., Fugini, M., 2016. Context-based risk-adaptive security model and conflict management. In: 27th International Conference on Database and Expert Systems Applications (DEXA). Springer.

W3C, 2016. SWRL: A Semantic Web Rule Language Combining OWL and RuleML. `https://www.w3.org/Submission/SWRL/`, [Online; accessed 25-June-2016].

Wang, H.-H., Boukamp, F., 2011. Ontology-based representation and reasoning framework for supporting job hazard analysis. Journal of Computing in Civil Engineering 25 (6), 442–456.

Wang, S., Wan, J., Li, D., Zhang, C., 2016. Implementing smart factory of industry 4.0: an outlook. International Journal of Distributed Sensor Networks 2016.

Whitman, M. E., Mattord, H. J., 2011. Principles of information security. Cengage Learning.

WSO2, accessed: 2016. Balana repository. `https://github.com/wso2/balana`.

Zhang, S., Boukamp, F., Teizer, J., 2014. Ontology-based semantic modeling of safety management knowledge. In: Computing in Civil and Building Engineering Conference (2014). American Society of Civil Engineers, pp. 2254–2262.

Zhang, S., Boukamp, F., Teizer, J., 2015. Ontology-based semantic modeling of construction safety knowledge: Towards automated safety planning for job hazard analysis (jha). Automation in Construction 52, 29–41.