Accepted Manuscript

Ontology development for run-time safety management methodology in Smart Work Environments using ambient knowledge

Mahsa Teimourikia, Mariagrazia Fugini

PII: S0167-739X(16)30233-3
DOI: http://dx.doi.org/10.1016/j.future.2016.07.003
Reference: FUTURE 3105

To appear in: *Future Generation Computer Systems*

Received date: 29 February 2016
Revised date: 11 July 2016
Accepted date: 14 July 2016

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-