Safety Science 79 (2015) 126–138

Contents lists available at ScienceDirect

Safety Science

journal homepage: www.elsevier.com/locate/ssci

The concept of risk situation awareness provision: Towards a new approach for assessing the DSA about the threats and vulnerabilities of complex socio-technical systems

Maria Mikela Chatzimichailidou [a,*], Neville A. Stanton [b], Ioannis M. Dokas [a]

[a] Department of Civil Engineering, Vasssilissis Sofias 12, Democritus University of Thrace, Xanthi 67100, Greece
[b] Transportation Research Group, Civil, Maritime and Environmental Engineering and Science Unit, Faculty of Engineering and the Environment, University Road, University of Southampton, Highfield, Southampton SO17 1BJ, UK

ARTICLE INFO

Article history:
Received 20 June 2014
Received in revised form 11 February 2015
Accepted 27 May 2015
Available online 18 June 2015

Keywords:
Situation awareness
Distributed situation awareness
Risk situation awareness provision
Socio-technical systems
Hazard analysis techniques

ABSTRACT

Situation Awareness (SA) is a widely cited and extensively reviewed concept. The context in which SA is examined herein is the complex socio-technical. Hence, the main focus is on Distributed Situation Awareness (DSA) and more precisely on the enhancement and degradation of the awareness regarding the threats and vulnerabilities that the system may possibly encounter. Specifically, by adopting the notion that safety and awareness are inherent and emergent properties of complex socio-technical systems, this paper introduces the novel concept of "risk SA provision". It is also discussed that the risk SA provision capability is dynamic by nature. Lastly, the Überlingen mid-air collision accident is used to demonstrate that hazard analysis techniques can be employed to create a more detailed image of what constitutes the 'ideal' socio-technical system in terms of risk SA provision capabilities. Resting on safety science and control theory, this work suggests a list of system elements and characteristics, which enhance information flow, retrieval, and dissemination and contribute to maintaining the system in an 'aware' and safe state. It is also argued that since those system elements are tangible, it seems possible to found a new DSA assessment approach on the measurement of the risk SA provision capabilities of the system.

© 2015 Elsevier Ltd. All rights reserved.

1. Introduction

In the literature, there are over thirty definitions of Situation Awareness (SA) (Salmon et al., 2009b). One widely cited definition proposes SA as a state of working knowledge of an individual; it is how much and how accurately he/she is aware of the current situation and concerns (1) the perception of the elements within a system, (2) the comprehension of their meaning, and (3) the projection of their future state (Endsley, 1995a). Another definition (Jeannot et al., 2003) argues that SA is what someone needs to know in order not to be surprised. According to Salmon et al. (2008) and Stanton et al. (2010), SA is an emergent property of a collaborative system itself rather than an individual endeavour.

The plethora of SA definitions is analogous to the models which explain the different types of SA, including: the individual SA model (Endsley, 1988; Sarter and Woods, 1991), the team and shared SA models (Salas et al., 1995; Salmon et al., 2008, 2009a,b), the meta (Salmon et al., 2008), compatible (Salmon et al., 2009b), and collective (Smart et al., 2007) SA models, and the most recent and complex one, the Distributed Situation Awareness (DSA) model (Stanton et al., 2006; Smart et al., 2007).

DSA is an approach that sets the foundations for a systemic framework explaining the emergence of SA in collaborative systems. It also implies that no one system agent, namely humans and automated controllers that possess reasoning mechanisms and demonstrate a capability to influence other agents or situations, has a complete picture of the situation in which the system finds itself, but just a facet of the corresponding situation at any point in time (Salmon et al., 2008). That accords with Salas et al. (1995) who claim that DSA is "something more" than the sum of individual or team SA, roughly meaning that in case of calculating the algebraic sum of individual SA and/or team SA of the system's parts, the outcome is not a value representing the system's DSA, but a partial image of it, from which the 'quantification' of emergence is the missing 'portion'. Thus, the DSA model appears to 'best

* Corresponding author at: Dionysiou Solomou 3, 67100 Xanthi, Greece. Tel.: +30 6942 413 863.
E-mail addresses: mikechat@civil.duth.gr, mikelachatzimichailidou@gmail.com (M.M. Chatzimichailidou), N.Stanton@soton.ac.uk (N.A. Stanton), idokas@civil.duth.gr (I.M. Dokas).

http://dx.doi.org/10.1016/j.ssci.2015.05.012
0925-7535/© 2015 Elsevier Ltd. All rights reserved.

fit' what really happens to a complex socio-technical system, while it, as an entity, strives to become aware of a potential harmful or unwanted situation in a timely manner.

To complement the SA models, there are a number of SA measurement approaches based either on individual SA models (e.g. Endsley's three-level model), or on team SA models (e.g. Salas et al., 1995; Salmon et al., 2009b). Stanton et al. (2005), having reviewed more than thirty different SA measurement approaches, categorised eighteen of them into six general categories for individual and three for team SA, based on their popularity and their potentiality to be applied in collaborative systems. The group of team SA measurement techniques integrates three of the individual SA measurement categories extended to the team level.

Many researchers (e.g. Stanton et al., 2001; Smart et al., 2007; Salmon et al., 2009b; Fioratou et al., 2010; Naderpour et al., 2014) have pointed out that SA is a key factor for systems safety. Indeed, any kind of SA degradation (Sorathia, 2008) may lead to safety issues; loss of SA, poor SA, and lack of SA are included in technical accident reports (e.g. BFU, 2002), conveying that SA is a concept that plays an important role in systems safety and resilience engineering. Hence, what we call in this paper risk SA, which is the individual SA of an agent of the system and refers to the presence of threats and vulnerabilities that may lead to system accidents, is one of the fundamental factors that determine the degree of safety that the controlled, by that agent, part of the system holds. According to this view, it is essential to make an estimate of how and to what degree various elements of the system affect the risk SA of all individual agents, because this in turn will contribute to estimate, what we call in this paper, risk DSA (i.e. the DSA about the presence of threats and vulnerabilities and how these may affect the safety of the entire system) and, through that, evaluate the safety level of complex socio-technical systems.

Based on the existing individual- or team-focused models and measurement techniques, it seems impractical, if not impossible, to 'measure' DSA in complex socio-technical systems. To be more specific, Salas et al. (1995), Stanton and Young (2003), Salmon et al. (2009a,b) have stated that the existing (and exhausted) individual and team SA models and measurement techniques are proven not to be adequate in the context of complex socio-technical systems. In particular, they argue that there is little evidence that these measurement techniques actually work (Salmon et al., 2009a), and they also raise concerns about their reliability and validity in cases where the objective is to measure SA in complex socio-technical systems. Thus, considering the existing individual and team SA models, the corresponding measurement techniques, as well as the current technological basis (e.g. we cannot constantly monitor human brain functions and reactions to stimuli), it is the cognitive and distributed 'character' of SA that possibly renders the direct measurement of risk DSA quite a challenging task.

The paper in hand acknowledges that all SA approaches have a unique form and function in their particular territory, however, it identifies a gap in the literature; *a measurable quantity, indicating how much the system as it is designed to function augments the awareness of its threats and vulnerabilities, seems to be absent in the literature.* Specifically, this paper is intended to map the road towards a means[1] that will make it possible for engineers and designers to choose the system or the system's alternative design requirements that maximise the awareness of safety-related issues and thus the risk DSA.

Setting as a higher research goal to bridge this gap, this paper introduces the concept of '*risk SA provision*', which reflects the inherent, according to the system design and development, capability of each system part to provide its agent with SA about the presence of system threats and vulnerabilities, possibly leading to accidents.

Using the Überlingen mid-air collision accident, this paper illustrates that these capabilities are dynamic by nature in a manner that they vary according to the design specifications of each complex socio-technical system. As a result, all or some parts of the complex socio-technical system can be designed and developed with more or less enhanced risk SA provision capabilities, integrating or leaving out elements, such as sensors, capable of detecting more threats and vulnerabilities, as well as agents whose mental or process models sufficiently represent possible accident scenarios, etc. In short, *the risk SA provision capability stems from the number, type, and characteristics of each one of the system elements that together shape the different parts of it, laying thus the foundation for the emergence of risk DSA on a system level.*

This paper demonstrates that hazard analysis techniques can be used to create a more detailed image of what constitutes the 'ideal' socio-technical system in terms of risk SA provision capabilities. In view of this, we apply a hazard analysis and an early warning sign identification approach, which both adhere to the principles of a system-theoretic accident model, to the control structure of the two aircraft involved in the Überlingen mid-air collision accident. Along these lines, a list of 12 guidelines that complement the newly introduced concept is offered and backed up by the hazard analysis.

2. The risk SA provision concept in complex socio-technical systems

2.1. Complex socio-technical systems

Socio-technical systems are comprised by both 'socio', i.e. people and society, and 'technical', i.e. machines and technology, elements (Walker et al., 2008). In order for such systems to achieve their purposes, they involve complex interactions between human and nonhuman agents, and other elements as well.

A graphical model of a complex socio-technical system is depicted in Fig. 1. The human-like figures express humans that control various processes of the complex socio-technical system, whether they are individuals or teams. The technical components of that system are the elements marked as 'C', 'A', and 'S', standing for automated controllers, actuators, and sensors[2], whilst the 'CP' element denotes a controlled process within the socio-technical system. A control loop, formed by the elements with the letters 'C', 'A', 'S', and 'CP' on them, depicts a fully automated part of the socio-technical system. The parts of the system where humans exercise indirect control over the controlled process, with an automated controller in the middle, are denoted by the bidirectional arrows between the human-like figures and the elements with the 'C' letter, together with the rest of the control loop which includes the controlled process. Finally, the parts of the system where humans have direct control over a controlled process are denoted by the bidirectional arrows between the human-like figures and the elements with the 'CP' label. In Fig. 1, agents are designated by the human-like figures, as well as by the elements with the label 'C'. The agents located at a specific hierarchical level enforce safety constraints/requirements (Leveson, 2011) on their controlled processes, which include other agents located at the lower hierarchical levels. In Fig. 1, for instance, there are three hierarchical levels: L0, L1, and L2.

As a didactic example of the model depicted in Fig. 1, consider a hypothetical incident taking place in a highway tunnel; the human

[1] The word 'means', as used in this paper, indicates "a method or way of doing something" (Cambridge Dictionaries Online), i.e. an instrument by which an act can be accomplished or an end achieved.

[2] In some cases it is possible for a human to play the role of a sensor. By 'sensor' we mean any instrument, mechanical or even human, that detects events or changes in quantities as well as qualities, and provides a corresponding signal.

Download English Version:

https://daneshyari.com/en/article/6975667

Download Persian Version:

https://daneshyari.com/article/6975667

Daneshyari.com