Reliability Engineering and System Safety 133 (2015) 33–47

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

An abnormal situation modeling method to assist operators in safety-critical systems

Mohsen Naderpour *, Jie Lu, Guangquan Zhang

Decision Systems and e-Service Intelligence Laboratory, Centre for Quantum Computation & Intelligent Systems, School of Software, Faculty of Engineering and IT, University of Technology Sydney, PO Box 123, Broadway, NSW 2007, Australia

ARTICLE INFO

Article history:
Received 19 November 2013
Received in revised form
26 June 2014
Accepted 16 August 2014
Available online 27 August 2014

Keywords:
Situation awareness
Situation assessment
Safety-critical systems
Bayesian networks
Fuzzy logic systems
Risk assessment

ABSTRACT

One of the main causes of accidents in safety-critical systems is human error. In order to reduce human errors in the process of handling abnormal situations that are highly complex and mentally taxing activities, operators need to be supported, from a cognitive perspective, in order to reduce their workload, stress, and the consequent error rate. Of the various cognitive activities, a correct understanding of the situation, i.e. situation awareness (SA), is a crucial factor in improving performance and reducing errors. Despite the importance of SA in decision-making in time- and safety-critical situations, the difficulty of SA modeling and assessment means that very few methods have as yet been developed. This study confronts this challenge, and develops an innovative abnormal situation modeling (ASM) method that exploits the capabilities of risk indicators, Bayesian networks and fuzzy logic systems. The risk indicators are used to identify abnormal situations, Bayesian networks are utilized to model them and a fuzzy logic system is developed to assess them. The ASM method can be used in the development of situation assessment decision support systems that underlie the achievement of SA. The performance of the ASM method is tested through a real case study at a chemical plant.

1. Introduction

Today, in many safety-critical systems the role of operators has shifted from manual controllers to supervisors or decision-makers who are responsible for extensive cognitive tasks [1]. Operators are often moved to a control room far away from the physical process and have to rely on human computer interaction (HCI) principles to observe and comprehend the overwhelming amount of rapidly changing data for processing. In the presence of all this data, complex interfaces, and dynamic situations, human error could be a serious cause of accidents in these environments. It has been found that in most industries, 70–90 percent of accidents are attributed to human error [2]. Traditionally, there are two approaches to prevent human error during operation of safety-critical systems. The first approach aims for the provision of better training programs for operators, and the second aims to improve operator support systems [3]. However, it has been shown that in abnormal time pressure situations, ordinary training does not improve the quality of decision making [4], and therefore, the role of cognitive support systems to assist operators in such situations is highlighted [5].

In abnormal situations, a well-trained operator should comprehend a malfunction in real time by analyzing alarms, assessing values, and recognizing unusual trends indicated by multiple instruments. In such a situation, many alarms from different systems are frequently triggered at the same time, making it difficult for the operator to make a decision within a very short time frame. If several abnormal situations occur at once, decisions have to be made in even less time. Operators are usually unable to judge what situation should be given priority when confronted with complex abnormal situations such as these [6,7]. To return operational units to normal conditions, operators must respond quickly and make rapid decisions, but under these circumstances, the mental workload of operators rises sharply, and a mental workload that is too high may increase the rate of error.

Despite the importance of human factors, most of the operator support systems focus on the deviation of the process from an acceptable range of operation, the identification of operation faults [8] or the prediction of process variables [9] that will violate an emergency limit in the future. Therefore, quantitative knowledge and hardware failures have been relied on significantly; however, when faults occur, human operators have to rely on their experience under working pressure to understand what is going on and to contribute a solution [10]. These problems highlight the urgency

* Corresponding author. Tel.: +61 2 9514 4520.
E-mail addresses: Mohsen.Naderpour@student.uts.edu.au (M. Naderpour), Jie.Lu@uts.edu.au (J. Lu), Guangquan.Zhang@uts.edu.au (G. Zhang).

http://dx.doi.org/10.1016/j.ress.2014.08.003
0951-8320/

of cognitive human factors in the development of operator support systems to lower workload, stress and consequent error rates of operators. Of the various cognitive features, operators' situation awareness (SA) is considered to be the most important prerequisite for decision-making [11,12]. To date, several SA models have been developed; however, Endsley's three-level model has undoubtedly received the most attention. This model describes SA as "the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future" [11]. The three-level model describes SA as an internally held product, comprising three hierarchical levels (i.e. perception, comprehension, and projection), that is separate from the processes called situation assessment, used to achieve it [11]. Usually, assessing a situation requires data integration with the support of computer-based intelligent techniques. Because SA aims to predict the status of a situation in the near future, which is the third level of the three-level model, proper and effective situation assessment approaches and tools to conduct the prediction are required.

Many studies have reported that machine learning techniques could be effectively used for intelligent prediction by extracting rules from previous data to generate new assessment results [13]. Despite the usefulness of machine learning techniques for situation assessment, their use in real environments, especially in abnormal situations, are very limited because of the lack of appropriate training data [14]. Therefore, a number of quantitative situation assessment models based on probabilistic modeling techniques, such as Miao et al. [15] and Kim and Seong [16], have been proposed. In the former, Miao et al. proposed a computational model of situation assessment using belief networks. Their model consists of developing a structure to represent the SA mental model, and developing a belief update algorithm to reflect SA event propagation and projection [15]. In the latter, Kim and Seong developed a situation assessment model based on Bayesian networks (BNs) for operators of nuclear power plants (NPPs). In their proposed model, the knowledge of operators, i.e. mental models, is elicited for assignation to the CPTs of the network, and when operators receive information from indicators, the probabilities of the states of the environment, i.e. several accidents, are updated [16]. They assume that the occurrences of situations are mutually exclusive, and they therefore provided very finite states, including four accidents for the environment, to avoid a large BN in which the need for essential data increases exponentially, or proportionally.

This paper develops a new abnormal situation modeling (ASM) method that exploits specific capabilities of BNs, risk indicators and fuzzy logic systems to determine abnormal situations, model them in a situational network, and assess them dynamically. The paper defines the situation as a set of circumstance in which a number of objects may have relationships with one another and the environment, and a hazardous situation as a possible circumstance immediately before harm is produced by a hazard. Therefore, an abnormal situation is defined as a hazardous situation if its risk is not acceptable. Conventional BN is considered as a representation of static cause–effect relationships between objects in a situation, and it is assumed that operators use Bayesian inference to process incoming information. In addition, as operators are usually able to form rules for every situation to assess risks, and those rules are an important part of their mental model, then the ASM method needs to resemble their thinking when confronted with abnormal situations. Therefore, to estimate the situational risk level, a fuzzy logic system (FLS) is utilized. Finally, the prototype based on the ASM method can trigger an alarm for every situation that has an unacceptable risk; therefore, it is assumed that operators consider abnormal situations by considering observable variables and hearing alarms.

In comparison with previous research work, this study has advantages. First, situations in the ASM method might be inclusive, unlike previous studies in which situations are exclusive. Second, unlike previous networks that only include indicators and sensors that are unable to determine the cause of abnormal situations, the ASM method enables the most probable cause of abnormal situations to be obtained from the situation models, thus assisting operators to understand situations. Third, the ASM method is able to generate risk levels for every hazardous situation to show whether a situation is abnormal (i.e. its risk level is unacceptable), and to help operators to understand the hierarchy of investigations (i.e. a situation with a higher risk has priority over other situations to be investigated).

The paper is organized as follows. Section 2 presents the theory of BNs. The proposed ASM method is explained in Section 3. A case study from the US Chemical Safety Board investigation reports (www.csb.gov) is presented in Section 4 to demonstrate the performance of the ASM method. The conclusion and future work are summarized in Section 5.

2. Bayesian networks

A BN is defined as a couple: $\mathcal{G}=((N,A),\mathcal{P})$, where (N,A) represents the graph; N is a set of nodes; A is a set of arcs; $\mathcal{P}$ represents the set of probability distributions that are associated to each node. When a node is not a root node, the distribution is a conditional probability distribution that quantifies the probabilistic dependency between that node and its parents [17]. A discrete random variable X is represented by a node $n \in N$ with a finite number of mutually exclusive states. States are defined on $S_n : \{s_1^n, s_2^n, \dots, s_M^n\}$. The set $\mathcal{P}$ is represented with Conditional Probability Tables (CPT), and each node has an associated CPT. For instance, if n_i is a parent of n_j, and the nodes n_i and n_j are defined over the sets $S_{n_i} : \{s_1^{n_i}, s_2^{n_i}, \dots, s_M^{n_i}\}$ and $S_{n_j} : \{s_1^{n_j}, s_2^{n_j}, \dots, s_L^{n_j}\}$, the CPT of n_j is then defined as a matrix by the conditional probabilities $p(n_j|n_i)$ over each n_j state knowing its parents states (n_i):

$$P(n_j|pa(n_j)) = \begin{bmatrix} p\left(n_j = s_1^{n_j}|n_i = s_1^{n_i}\right) & \cdots & p\left(n_j = s_L^{n_j}|n_i = s_1^{n_i}\right) \\ \vdots & \vdots & \vdots \\ p\left(n_j = s_1^{n_j}|n_i = s_M^{n_i}\right) & \cdots & p\left(n_j = s_L^{n_j}|n_i = s_M^{n_i}\right) \end{bmatrix} \quad (1)$$

Various inference algorithms can be used to compute marginal probabilities for each unobserved node, given information on the states of a set of observed nodes, that the junction tree algorithm is the a classical one. Inference in BN then allows us to take into account any state variable observation (an event) so as to update the probabilities of the other variables. When observations are given, this knowledge is integrated into the network and all the probabilities are updated accordingly. A hard evidence of the random variable X indicates that the state of the node $n \in N$ is one of the states $S_n : \{s_1^n, s_2^n, \dots, s_M^n\}$. Nevertheless, when this knowledge is uncertain, soft evidence can be used. A soft evidence for a node n is defined as one that enables the updating of the prior probability values for the states of n [17].

2.1. Dynamic and object oriented Bayesian networks

A dynamic BN (DBN) is a BN that includes a temporal dimension. This new dimension is managed by time-indexed random variables X_i, which is represented at time step k by a node $n_{(i,k)} \in N$ with a finite number of states $S_{n_i} : \{s_1^{n_i}, s_2^{n_i}, \dots, s_M^{n_i}\}$. Several time stages are represented by several sets of nodes and an arc that