

An Intelligent Situation Awareness Support System for Safety-Critical Environments

Mohsen Naderpour¹, 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
Mohsen.Naderpour@student.uts.edu.au, Jie.Lu@uts.edu.au, Guangquan.Zhang@uts.edu.au*

Abstract:

Operators handling abnormal situations in safety-critical environments need to be supported from a cognitive perspective to reduce their workload, stress, and 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 error. However, existing system safety researches focus mainly on technical issues and often neglect SA. This study presents an innovative cognition-driven decision support system called the situation awareness support system (SASS) to manage abnormal situations in safety-critical environments in which the effect of situational complexity on human decision-makers is a concern. To achieve this objective, a situational network modeling process and a situation assessment model that exploits the specific capabilities of dynamic Bayesian networks and risk indicators are first proposed. The SASS is then developed and consists of four major elements: 1) a situation data collection component that provides the current state of the observable variables based on online conditions and monitoring systems, 2) a situation assessment component based on dynamic Bayesian networks (DBN) to model the hazardous situations in a situational network and a fuzzy risk estimation method to generate the assessment result, 3) a situation recovery component that provides a basis for decision-making to reduce the risk level of situations to an acceptable level, and 4) a human-computer interface. The SASS is partially evaluated by a sensitivity analysis, which is carried out to validate DBN-based situational networks, and SA measurements are suggested for a full evaluation of the proposed system. The performance of the SASS is demonstrated by a case taken from US Chemical Safety Board reports, and the results demonstrate that the SASS provides a useful graphical, mathematically consistent system for dealing with incomplete and uncertain information to help operators maintain the risk of dynamic situations at an acceptable level.

Keywords: Decision support systems, Cognition-driven decision support, Situation awareness, Situation assessment, Risk assessment, Bayesian networks.

1. Introduction

Safety-critical environments are those domains in which hardware failure or poor or late decision-making by operators could result in loss of life, significant property damage, or environmental pollution. In many safety-critical environments today, the role of the operator shifts from a person who controls a process manually to a supervisor or decision-maker, and includes extensive cognitive tasks [15] including information gathering, planning, decision-making, demonstrating that the facility is fit for its intended purpose, and ensuring that the risks associated with its operation are sufficiently low

¹ Corresponding author, Tel: +61 2 9514 4520

[34]. In abnormal situations, a well-trained operator should comprehend a malfunction in real time by analyzing alarms, assessing values, and recognizing unusual trends associated with multiple instruments. When confronted with a complex abnormal situation, many alarms from different systems may sound at the same time, making it difficult for operators to judge within a short period of time which situation should be given priority. To return operational units to normal conditions, operators must respond quickly and make rapid decisions, but the mental workload of operators under these circumstances rises sharply, and a mental workload that is too high may increase the rate of error [17]. Paradoxically, several researches show that the focus of most human-system studies is on the technical elements, and human factors are often neglected [39]. This is due to well understood hardware reliability techniques, whereas the handling of human factors, by contrast, is difficult. These problems highlight the urgent need to discover cognitive decision support systems to manage abnormal situations that will lower operator workload and stress and consequently reduce the rate of errors made by operators.

Decision support systems (DSSs) are envisioned as “executive mind-support systems” that are expected to support decision-making from a human cognition perspective [4]. Over the years, some types of DSS, such as model-driven and data-driven DSSs, have achieved increased popularity in various domains. Model-driven DSSs emphasize the creation and manipulation of statistical, financial, optimization, or simulation models that require decision makers to specify model parameters according to their decision problems. The functionality of data-driven DSSs results from access to, and manipulation of, a large database of structured data, and their outputs are based on perceiving and comprehending the integrated information [41]. Unlike model-driven and data-driven DSSs, cognitive DSSs have not been researched, albeit they have long been recognized as being worthy of consideration [4]. Just as a cognitive process refers to an act of human information processing, so a cognition-driven decision support system refers to assisting operators in their decision-making from a human cognition perspective, using such attributes as sensing, comprehending and projecting [39]. Of these cognitive aspects, an operator’s situation awareness (SA) is considered to be the most important prerequisite for decision-making. Situation awareness comprises the perception of elements in the environment, the understanding of their meaning, and the projection of the status of that environment in the near future [10]. Situation awareness is likely to be at the root of many accidents in safety-

critical environments where multiple goals must be pursued simultaneously, multiple tasks require the operator's attention, operator performance is under high time stress, and negative consequences associated with poor performance are anticipated [22]. To give an example: On 14 June 2006 in an explosion at a chemical plant, one person was killed and two employees were injured when the operator could not maintain accurate SA and the vapor overflowed from the tank [5]. This case will be investigated in this paper as an example of poor operator SA which led to a severe accident.

Based on these issues, the main objective of this study is to develop a cognition-driven DSS, called the situation awareness support system (SASS), with the purpose of developing a comprehensive and practical operator support system for use in abnormal situations. The proposed SASS consists of four major components: 1) situation data collection (e.g. observable variables such as sensors), 2) situation assessment, which includes a dynamic Bayesian network-based situational network to model situations of interest and a risk estimation method to generate the assessment result, 3) situation recovery, and 4) a human-computer interface. The proposed system has the following advantages:

- 1) In most human-system studies, safety has been considered from a technical perspective. Only hazards that arise through hardware failure have been considered, despite the fact that human failure is a more common factor in safety-critical systems. To develop the system in this study, two important aspects, namely addressing hazards that result from hardware failure and reducing human error through decision-making, have been considered. A situation modeling process based on hardware and human failure is proposed to model hazardous situations, and a situation assessment model is developed to support operators to achieve and maintain SA, and to make correct decisions.
- 2) The proposed SASS does not control the manner of implementing actions and allows individual discretion in the choice of human action for the specific context. It has been shown that increased automation does not necessarily result in improved capability, because approaches that focus solely on automated features disconnect the operator from the system and alienate them from the production process [2]. Therefore, the SASS keeps operators in the loop of decision-making and action-taking.

- 3) The proposed SASS assists operators to avoid unforeseen risks in the operation system and to determine appropriate ways to eliminate or control hazards until their risk level falls As Low as Reasonably Practicable (ALARP), thus ensuring that the proposed system conforms to ALARP.
- 4) The proposed SASS includes a situation assessment component that uses dynamic Bayesian networks, which has certain advantages over other situation assessment methods that use artificial intelligence tools such as expert systems [36] and neural networks [37]. First, it includes nodes and directed arcs to express the knowledge, and new information can be transmitted by directed arcs between nodes. Second, knowledge in the component can be updated, whereas updating knowledge in expert systems is difficult. Third, it already has expert knowledge encoded in its construction, while neural networks must learn knowledge via datasets, assuming training data are available. Lastly, the cumulative effect of situations based on new evidence is very suitable for SA continuity, whereas this feature does not exist in other artificial intelligence tools [46].

This study makes three important contributions. First, it proposes a situational network modeling process which is used to model abnormal situations in one or more networks. Second, it presents a situation assessment model that exploits the specific capabilities of dynamic Bayesian networks and fuzzy risk analysis. The proposed situation assessment model can be applied to other related domains if the risk indicators for any measurement are appropriate. Third, it develops, for the first time, a SASS for managing abnormal situations in safety-critical environments in which the degree of automation and complexity continues to increase and the number of operators decreases, and where each operator must be able to comprehend and respond to a growing amount of risky status and alert information.

The paper is organized as follows. Section 2 presents the background of this study. A literature review of SA and related areas is given in Section 3. The methodology for this study is provided in Section 4, and the requirements, model, and components of the SASS are explained in Section 5. A case from US Chemical Safety Board investigation reports (www.csb.gov) is presented in Section 6 to demonstrate the performance of the SASS. Section 7 compares our model with an existing situation assessment model and discusses the limitations of this study. The conclusion and future work are summarized in Section 8.

2. Background

This section describes the background to this study, including situation awareness, Bayesian network theory and the preliminary concepts of fuzzy sets and fuzzy logic systems.

2.1. Situation Awareness

A situation is a set of circumstances in which a number of objects may have relationships with one another and the environment. Situation awareness can be described 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” [10]. This SA model follows an information processing chain from perception, through comprehension, to projection. Figure 1 enables a clear understanding of the definition of both ‘situation’ and ‘SA’. It shows four planes, each of which refers to a different level of abstraction. The bottom layer shows the World, which includes physical or conceptual things, or both. To the right of the World plane, a human head depicts the fact that SA is a state of knowledge which takes place in the human brain. The human is unable to observe all aspects of the World, and therefore has to obtain inputs from the computer for better appreciation (i.e. the arrow between the computer and the human head). The dots on the next layer (i.e. Perception) represent the objects from the World that are observed through sensors and represented in computer memory. The arrow pointing from the World plane to the radar icon represents the sensory process, which then feeds the computer. The emphasis in situation definition is on relationships which are described from the point of view of a thing (i.e. focal object), and how other things in the surroundings are related to it. This plane represents Comprehension. The top layer illustrates the Projection, and this layer is defined as the ability to anticipate future events and their implications [28].

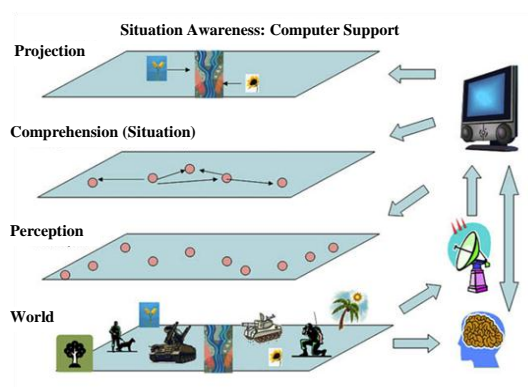


Figure 1: The situation and SA [28].

2.2. Bayesian Networks

A Bayesian network (BN) is a mathematical graphical representation method that provides an opportunity to model a causal process with uncertainty. Each node represents a variable and the arcs show direct probabilistic relations between the connected nodes. Dynamic BNs (DBNs) allow time to be taken into account by defining different variables at different time slices.

2.2.1. The Bayesian Network Notations

A BN usually involves a directed acyclic graph (DAG) that represents the network structure, and a set of conditional probability tables (CPTs), which are the network parameters [18]. Three common ways to construct a BN are to: (1) manually specify the DAG and CPTs by expert opinion; (2) automatically learn the DAG and CPTs using various algorithms based on observational data; and (3) manually construct the DAG by expert opinion or automatically learn the DAG using expert opinions as structural constraints/restrictions, and then to learn the CPTs from observational data [18]. In this paper, a conventional BN can be considered as a representation of static cause–effect relations between objects in a situation. Based on the conditional independence resulting from the d -separation concept, and the chain rule, BN represents the joint probability distribution $P(X)$ of variables $X = \{X_1, \dots, X_n\}$, included in the network as [23]:

$$P(X) = \prod_{i=1}^n P(X_i | Pa(X_i)) \quad (1)$$

where $Pa(X_i)$ is the parent set of X_i for any $i = 1, \dots, n$. If $Pa(X_i)$ is an empty set, then X_i is a root node and $P(X_i | Pa(X_i)) = P(X_i)$ denotes its prior probability. Bayesian networks use Bayes' theorem to update the prior occurrence probability of objects given new information. This new information, called evidence E , is usually obtained during system operation, including the occurrence or non-occurrence of the objects:

$$P(X|E) = \frac{P(X, E)}{P(E)} = \frac{P(X, E)}{\sum_x P(X, E)} \quad (2)$$

This equation will be used for probability prediction or probability updating in a given network. In predictive analysis, the conditional probabilities of the form $P(\text{situation}/\text{object})$ are calculated which show the occurrence probability of a particular situation given the occurrence or non-occurrence of a certain primary object. In updating analysis, the conditional probabilities of the form

$P(object/situation)$ are assessed, indicating the occurrence probability of a particular object given the occurrence of a certain situation.

2.2.2. Dynamic Bayesian Network

A DBN model can be obtained from a static BN by introducing relevant temporal dependencies among variables to describe the behavior of a particular system at different times. A DBN usually has two types of dependency: non-contemporaneous and contemporaneous. Non-contemporaneous dependencies are arcs between nodes that represent variables at different times. Contemporaneous dependencies are arcs between nodes that represent variables within the same time period [35]. A DBN is defined as a pair $(B_1, 2TBN)$ where B_1 is a BN that defines the prior distribution $P(X_1)$ and $2TBN$ is a two-slice temporal BN with

$$P(X_t|X_{t-1}) = \prod_{i=1}^n P(X_t^i | Pa(X_t^i)) \quad (3)$$

where X_t^i is a node at time slice t and $Pa(X_t^i)$ is the set of parent nodes that can be in time slice t or in time slice $t-1$. In the first slice of a $2TBN$, the nodes have no parameters, but in the second slice each node has an associated CPT for discrete variables or conditional probability distribution (CPD) for continuous variables, which defines $P(X_t^i | Pa(X_t^i))$ for all $t > 1$. The arcs between slices reflect the causal flow of time. The node X_t^i is called persistent if there is an arc from X_{t-1}^i to X_t^i . The arcs within a slice are arbitrary, and directed arcs represent “instantaneous” causation. The semantics of a DBN can be defined by “unrolling” the $2TBN$ until there are T time-slices. The resulting joint distribution is then given by [35]:

$$P(X_{1:T}) = \prod_{t=1}^T \prod_{i=1}^n P(X_t^i | Pa(X_t^i)) \quad (4)$$

As exact inference is NP-hard, approximation algorithms can be used, such as clustering, unrolled junction tree, and the forward-backward algorithm.

2.3. Fuzzy Sets and Fuzzy Logic Systems

Fuzzy logic is a concept for dealing with uncertainty, vagueness, or imprecise problems that uses membership functions with values between 0 and 1. Unlike conventional set theory based on Boolean logic, a particular object or variable in fuzzy set theory based on fuzzy logic has a degree of

membership in a given set that may be anywhere in the range of 0 (completely not in the set) to 1 (completely in the set).

Definition 1 (Fuzzy set) [44]: Fuzzy set A is defined in terms of a universal set X by a membership function that assigns to each element $x \in X$ a value $\mu_A(x)$ in the interval $[0,1]$, i.e. $A: X \rightarrow [0,1]$.

Definition 2 (α -cut) [44]: Let A be a fuzzy set in the universe X , $\alpha \in (0,1]$. The α -cut or α -level set of the fuzzy set A is the crisp set A_α defined by:

$$A_\alpha = \{x \in X | \mu_A(x) \geq \alpha\} \quad (5)$$

Definition 3 (Fuzzy number) [44]: A fuzzy set A in \mathbb{R} satisfies the following conditions:

- A is normal,
- A_α is a closed interval for every $\alpha \in (0,1]$,
- the support of A is bounded.

Definition 4 (Fuzzy logic system) [33]: A fuzzy logic system (FLS) as shown in Figure 2 includes three parts: fuzzification, fuzzy inference engine and defuzzification. In the fuzzification process, the fuzzy sets are formed for all input variables. The fuzzy inference engine takes into account the input variables and the logic relations between them, and uses fuzzy logic operations to generate the output. In the defuzzification process, the output fuzzy set is converted into a crisp value.

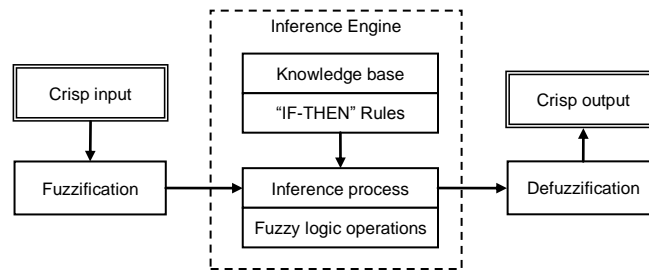


Figure 2: A fuzzy logic system [33].

3. Literature Review

There is a rich literature on SA, ranging from SA system modeling to cognitive workload assessment and support. The majority of researches to date have focused on the development of situation assessment models which underlie the achievement of SA, rather than the implementation of SA systems. In the literature review in this paper, the related concepts of situation assessment methods and SA systems modeling are considered.

3.1. Situation Assessment Methods

Situation assessment models explain the main features and general principles of how people process information and interact with the environment to maintain their SA; indeed, awareness of a situation is achieved as a result of situation assessment [10]. Since SA is a dynamic and collaborative process, 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 SA model, effective situation assessment approaches and the right tools are needed to conduct the prediction.

Many studies have reported that machine learning techniques can provide an effective method of intelligent prediction by extracting rules from previous data to generate new assessment results. For instance, Lu et al. developed a support vector machine-based assessment approach which has the ability to learn the rules from previous assessment results and generate the necessary warnings for a situation. They used a synthesized, artificially generated dataset to illustrate the effectiveness of their proposed situation assessment approach [30]. In another study, Lu et al. proposed a fuzzy least squares support vector machine technique for situation assessment using the integration of information obtained from related data sources. Again, they used an artificially generated dataset to show the accuracy of their technique [31]. A neural network-based situation assessment module was developed by Brannon et al. to provide a high level of SA for decision makers in force protection [2]. Despite the usefulness of machine learning techniques for situation assessment, their use in real environments is very limited because of the lack of appropriate SA training data [2].

Kim and Seong developed an analytic mathematical model for situation assessment based on BNs for the operators of a nuclear power plant (NPP). In their proposed model, operator knowledge (i.e. mental models) is elicited to assign to the CPTs of a network, and when operators receive information from indicators, the probabilities of the states of the environment (i.e. multiple accidents) are updated [24]. They extended their proposed approach by considering the interdependency of instrumentation and control systems and the operators in the NPP [25]. Other than in NPPs, Bayesian theory has been widely considered in the situation assessment configuration of command and control domains. For instance, a hierarchical BN-based situation assessment model developed in [3] includes two layers: the top layer, which serves as a fusion center, and the bottom layer, which provides the discretization of continuous data. A distributed approach to battlefield situation assessment based on level 2 of JDL

fusion processing was presented by [8] to enhance inference efficiency and allow computation at various levels of abstraction suitable for hierarchical military organizations. In the field of process safety, Naderpour and Lu developed an expert system-based situation assessment method for a chemical plant [36] and extended it to incorporate the ability of neural networks to project the state of the environment in the near future [37]; however, because of the lack of appropriate data for abnormal situations, it could not be implemented in the real world.

3.2. Situation Awareness Support Systems

The three-level model of SA has been used in a number of studies as the justification for structuring a computer-supported SA process in different domains. Two SASSs for maritime security have been developed. In the first, a system was developed to improve maritime threat detection capability by combining sensor-based information, context information, and intelligence from various sources based on domain ontologies. The system has the ability to recognize any deviance from normal behavior [47]. In the second, a model-driven situation analysis decision support system was developed based on abstract state machine modeling and CoreASM tool support for the purpose of infrastructure protection and emergency response [12]. In military services, there are several SA systems, such as [13] and [45], that are able to collect, filter and present different sources of data, and also support some form of low-level data fusion and analysis. However, these systems are not able to provide a deep, semantic modeling of the domain and are consequently unable to generate conclusions. Their users therefore have to integrate information by themselves to assess and predict a future situations, so a system architecture has been developed in [1] that focuses on using formal logic and an automated theorem to build a SA system in a more useful way. A SA system for force protection that combines humans and neural networks was proposed in [2] and includes a calculation engine for operation in three learning modes: supervised for initial training and known updating, reinforcement for online operational improvement, and unsupervised in the absence of all external signaling. The system can switch between the three learning types using an architecture based on adaptive resonance theory. In the aviation domain, a SA system called the tactile situation awareness system (TSAS) has been developed in [26] to improve the SA of pilots in simulated rotorcraft under high-load working conditions. Rather than presenting visual or aural information for the efficient

delivery of SA, this system relies on a wearable suit equipped with a tactile device that provides an intuitive human computer interface with three-dimensional space [26].

Although the majority of SA systems modeling studies are related to command and control fields, they are not limited to them. In business intelligence systems, for instance, a cognitive decision support system called FACETS was developed and evaluated based on a situation retrieval model [39]. The goal of FACETS is to assist managers in ill-structured decision situations to develop and enrich their SA for decision-making. The system allows managers to describe their SA in the form of English; it parses a manager's SA and constructs data warehouse queries that allow the retrieved situation information to be presented according to the navigation knowledge extracted from the manager's experience.

Although the application of SASSs is not limited to the above domains, its application in safety-critical environments is very rare. Most prior system safety studies in these environments focus on the deviation of the process from an acceptable range of operation. Therefore, in the development of operator DSSs, the use of quantitative knowledge and hardware failures has been relied on significantly. Most of these research studies focus on the identification of operation faults [42] or the prediction of process variables [21] that will violate an emergency limit in the future; however, some research shows that 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. Designing and integrating appropriate approaches to develop DSSs for complex domains is therefore highly recommended [27].

4. Methodology

The methodology of this study is planned according to the practice of design research [38], which has been proposed and applied in information systems, and is based on an SA-oriented design process [11], which has been established to guide the development of systems that support SA. The SA-oriented design process (Figure 3) incorporates SA considerations, including the determination of SA requirements, design principles for SA enhancement, and the measurement of SA in design evaluation. This methodology consists of the following steps:

Step 1: Determine SA requirements: To identify the aspects of a situation that are important for an operator's SA, Goal-Directed Task Analysis (GDTA) methodology, which is a form of

cognitive task analysis, is used. GDTA focuses on determining the operator's data and information needs (Level 1), combining the information to provide understanding (Level 2) and projecting future events (Level 3) [20]. In this analysis, the major goals and sub-goals of a particular job are initially identified, after which important decisions that need to be made are determined. The SA requirements for making these decisions and achieving each sub-goal are then identified. GDTA is not task-based analysis because in many environments the goals, not the tasks, form the basis for decision-making [11].

Step 2: Develop the SASS model: Situation awareness as a product of situation assessment provides input to the decision-making process, and situation assessment is therefore an important part of the SASS model. The SASS also requires a knowledge base that includes situation models which, in this paper, consist of DBN-based situation models. In addition, the related data of a situation (e.g. sensors) must be collected from the operation area, so the SASS needs a component that provides updated values of observable variables. If the risk level of a situation is not acceptable (i.e. the situation is abnormal), appropriate actions will be suggested to the operator through a recovery component. Ultimately, following appropriate decision-making by the operator, the abnormal situation will be rectified and the system will be updated in line with the new data collected from the environment. Useful information related to situations, objects, and observable variables will be presented in a human-computer interface, and all these issues will be taken into consideration in the development of the SASS model.

Step 3: Design and implement the proposed SASS: The SASS prototype system will be designed and implemented in this step according to the proposed model and SA-oriented design principles. The latter include several guidelines to address automation, complexity, and information uncertainty, and also incorporate general guidelines for the design of alarm systems and SA support in team operations [11]. This step includes the following sub-steps to create the prototype [38]: a) planning, b) analysis, c) design, d) development, e) testing, f) implementation, and g) maintenance.

Step 4: Evaluate the proposed SASS: This step considers the evaluation of the implemented prototype according to several criteria. The evaluation results, which might or might not meet expectations, will be fed back to the two previous steps to revise and improve the system. SA

measurement or sensitivity analysis are the criteria for evaluation of the SASS. DBNs are utilized to develop the situation models, and sensitivity analysis can therefore be used for the partial evaluation of SASS performance. The full validation of the proposed system will be carried out by evaluation of the prototype based on an appropriate SA measurement method.

Step 5: Demonstrate the performance of the proposed SASS through a case study: The literature provides many examples of incidents and accidents that could have been avoided if operators had recognized the situation in time. Therefore, an investigated case related to SA is chosen to demonstrate the performance of the SASS.

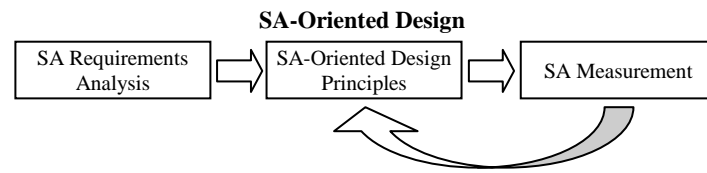


Figure 3: SA-oriented design process [11].

5. An Intelligent Situation Awareness Support System

Maintaining a complex and dynamic system in safe conditions, i.e. keeping the risks below accepted criteria, is a critical challenge because situations change dynamically and every decision has a significant social, economic and environmental impact. According to the methodology of this study, a situation awareness support system (SASS) is developed. The requirements, the proposed model, and the components of SASS are presented in the following sections.

5.1. The SASS Requirements

The SASS requirements are determined by GDTA. According to ALARP, it is necessary for operators of a potentially hazardous facility to demonstrate that: a) the facility is fit for its intended purpose, b) the risks associated with its functioning are sufficiently low, and c) sufficient safety and emergency measures have been instituted (or are proposed) [34]. The main goal of the system is to eliminate the risk or reduce it to an acceptable level. The other elements of GDTA are as shown in Table 1. The main goal is supported by two sub-goals: risk determination and risk reduction. The major decisions that need to be made in association with each sub-goal are identified, and the SA requirements for making these decisions and fulfilling each sub-goal are determined.

Table 1: Safety goals, decisions and SA requirement**Goal: Eliminate or reduce the risks to a level that is as low as reasonably practicable**

Subgoal 1: Determine the risks

Decision 1-1: Hazardous situation identification

- L1: Objects and relationships which contribute to creating a hazardous situation
- L1: Situations and relationships which contribute to creating a hazardous situation
- L2: Hazardous situations that threaten the system

Decision 1-2: Probability determination

- L1: Objects which are relevant to contributors to the hazardous situation
- L1: Observable variables which are relevant to the hazardous situation
- L2: Prior probability of the hazardous situation
- L3: Posterior probability of the hazardous situation

Decision 1-3: Severity determination

- L2: Possible consequences of the hazardous situation
- L3: Degree of loss

Decision 1-4: Risk level estimation

- L2: Probability of the hazardous situation (Decision 1-2)
- L2: Severity of the hazardous situation (Decision 1-3)
- L3: Current level of risk

Subgoal 2: Reduce the risks

Decision 2-1: Choosing practical options

- L2: Available reduction and containment options

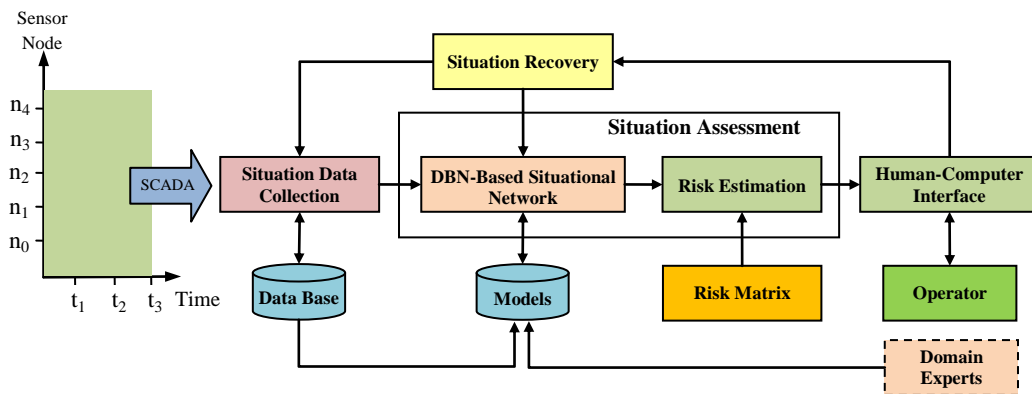
Decision 2-2: Options impact prediction

- L2: The severity of the hazardous situation
- L3: Projecting the new probability of the hazardous situation
- L3: New level of risk

L3= Projection of SA; L2= Comprehension of SA; L1= Perception of SA.

5.2. The Proposed SASS Model

Based on the SA requirements, the proposed SASS considers how situations and objects interact with one another based on BN models, how to update the states of a situation based on the SCADA¹ monitoring system, and how the risk of situations can be reduced to an acceptable level. The system's proposed model is shown in Figure 4. In the following sections, the components will be explained in detail and the means of addressing the identified decisions to achieve the sub-goals, and subsequently the main goal based on identified requirements, will be clarified.

**Figure 4: The proposed model of the situation awareness support system.**¹ Supervisory Control and Data Acquisition

5.2.1. The Situation Data Collection Component

The situation data collection component provides the current state of the observable variables, which are related to BN models according to the online condition and monitoring system. The component stores the data in a database, conducts a discretization process for continuous variables and transfers the result to the next component. The observable variables will be used as evidence in the situation assessment component. According to the condition and process monitoring, each observable variable value may be obtained from field sensors based on SCADA systems. As the observable variables extracted from sensors are continuous, a discretization process is required to use them in BNs. In general, mapping a continuous variable to a discrete variable can be achieved with a crisp set or a fuzzy set.

Consider a variable such as outside temperature defined on the frame $[-10,39]$ °C, which is inherently continuous but has to be represented as discrete when included in a discrete BN. It can be discrete to a scheme of three states: Cold, Normal, and Warm corresponding to the intervals $[-10,10)$ °C, $[10,25)$ °C, and $[25,39]$ °C, respectively. A thermometer reading of 9.9 °C would fall under the discrete state ‘cold’, whereas 10 °C would be labeled as ‘normal’. As can be seen, determining a crisp boundary between these states is not meaningful, hence the concept of fuzzy sets provides a more structured and smoother way. Figure 5 shows a fuzzy partition, but non-symmetric fuzzy sets or sets with a different shape can be used.

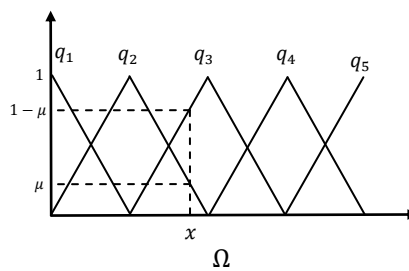


Figure 5: A fuzzy partition.

If x is a value of a variable X occurring on a domain partitioned as in Figure 5, then point semantic unification is applied to evaluate the probabilities $P(q_1/x), \dots, P(q_5/x)$ that constitute the distribution corresponding to the value x on the sets q_1, q_2, \dots, q_5 .

Definition 5 (Fuzzy partition): A fuzzy partition on the universe Ω is a set of fuzzy sets $\{q_1, q_2, \dots, q_m\}$ such that:

$$\forall x \in \Omega, \sum_{i=1}^m \mu_{q_i}(x) = 1 \quad (6)$$

where $\mu_{q_i}(x)$ is the membership function of q_i , i.e. $\mu_{q_i}: \Omega \rightarrow [0,1]$.

Definition 6 (Fuzzy state): Let $\{q_1, q_2, \dots, q_m\}$ be a fuzzy partition on the universe Ω , then every fuzzy set $q_i, i = 1, \dots, m$ is defined as a fuzzy state such that:

$$q_i = \{\mu_{q_i}(x) | x \in \Omega\} \quad (7)$$

For a particular BN, there are two types of evidence for every node: hard and soft. If a node is observed as one of its states, it is called hard evidence, and if the evidence is observed with uncertainty, it is called soft evidence. If a node does not have any parents, soft evidence is equivalent to modifying its prior probability; otherwise, soft evidence on a variable X_i is represented by a conditional probability vector $P(X_i=x/H_i)$ for $i=1,2,\dots,n$, where H_i denotes the hypothesis that the true state is the i -th state. To simplify the inference process for a continuous variable X_i , consider the fuzzy partition $\{q_1, q_2, \dots, q_m\}$. Define $H_j (j=1,2,\dots,m)$ as hypotheses that X_i is in fuzzy state q_j . The results of membership functions $\mu_{q_j}(x) j=1,2,\dots,m$ form the soft evidence vector:

$$e = \{\mu_{q_1}(x), \mu_{q_2}(x), \dots, \mu_{q_m}(x)\} \quad (8)$$

The $\mu_{q_j}(x)$ is considered to be approximately equivalent to the condition probability $P(q_j|X_i = x)$.

5.2.2. The Situation Assessment Component

This section describes how situations are defined and how they can be modeled by BNs. A DBN-based situational network is developed to model the situations of interest in a network, while every situation is modeled by a simple BN based on constitutive objects. Every environment may have one or more situational networks. In addition to generating the assessment result, the component enjoys a fuzzy risk estimation method.

5.2.2.1. Situations of Interest

Two types of hazardous situation are considered: 1) first level situations: the objects of a situation and their interactions may create a hazard; 2) higher level situations: relationships between situations may produce a hazard. To find the situations of interest, hazard identification methods and expert knowledge should be used. In many areas, hazardous situations have been found during the design and implementation phases, and various models have been developed to identify them. For example, HAZOP is a powerful method that has been well described in the literature; fault tree, event tree, and bow-tie can be adopted as the knowledge acquisition techniques [36]. The results form a model-base

which provides the requirements for making the first decision, i.e. hazardous situation identification (Decision 1-1 in Table 1).

5.2.2.2. DBN-Based Situational Network

A situation is a collection of physical or conceptual objects, or both, that have relationships with one another and the environment. Suppose the configuration space σ is defined by all possible physical and conceptual objects. Mathematically, a situation at time t can be modeled using a subset $\tilde{\sigma}$ of the configuration space as a statement, which is either hazardous or safe:

$$S_t = \begin{cases} \text{Hazardous} & \text{if } R(S_t) > \text{Risk Criteria} \\ \text{Safe} & \text{if } R(S_t) \leq \text{Risk Criteria} \end{cases} \quad (9)$$

where the $R(S_t)$ is the current risk level of the situation and is defined as:

$$R(S_t) = P(S_t) * S(S_t) \quad (10)$$

where $P(S_t)$ is the probability of the situation at a time t and depends on the objects of the subset space $\tilde{\sigma}$:

$$P(S_t) := P(S_t | o_1, o_2, \dots, o_m) \text{ with } o_1, o_2, \dots, o_m \in \tilde{\sigma} \quad (11)$$

and $S(S_t)$ is the severity of the situation. As a result of this modeling, the existence of a situation is inferred on the basis of information in the world, i.e. the observable variables and objects of configuration space.

The first level situation can be illustrated by a BN, based on its objects. The BN usually begins with root nodes that include the basic objects, which are followed by intermediate nodes, then a pivot node and leaf nodes. The pivot node is the focal object that delegates the situation, and relations between the root nodes and the pivot node define the relationships between the objects. The leaf nodes are safety barriers that are physical objects of the situation and will connect to each other if there is a relation between their performances. Also, one of the leaf nodes may be a consequence node that has multiple states, and highlights potential accidents in this situation. Figure 6(a) shows a situation A in which node A is the focal object to which all other nodes relate. It may be that a number of situations can only be inferred by observing the operational life of a system over a period of time. Although all situations are characterized by information collected over a time-period, they only exist at a specific point in time, and their existence in the next time-point has to be verified again.

Higher level situations are inferred from other situations. Several higher level situations can exist in parallel, or the existence of one situation can preclude the existence of another situation. Figure 6(b) shows an example of a network of situations. As can be seen, there are four situations of interest, namely A, B, C and D, where A and B belong to the first level situations category. They can be inferred directly from objects O_1 , O_2 and O_3 , while situations C and D are higher level situations whose existence is dependent on the existence of lower level situations. The temporal dependencies are illustrated by dashed lines.

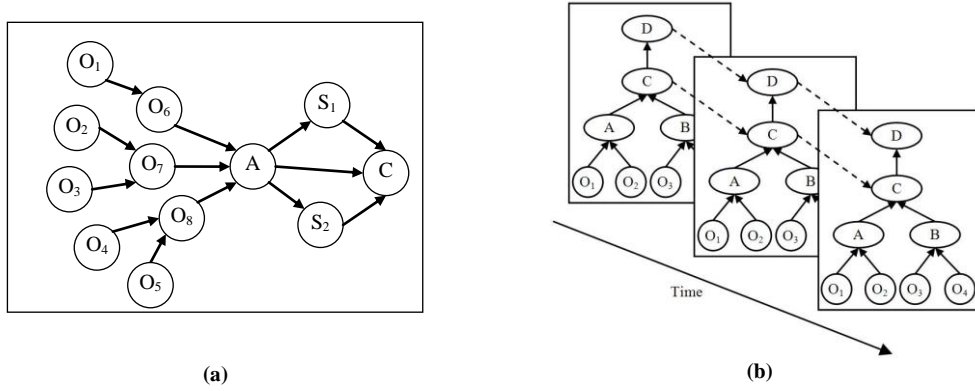


Figure 6: A simple BN and a dynamic BN.

The probability of the existence of the first level situation is inferred directly from the values of the configuration space, and the probability of a higher level situation is calculated based on the existence probability of other situations. This also includes temporal dependencies, i.e. where the existence probability of a future inferred situation is supported by the earlier existence of the situation itself. The complete modeling of the dependencies results in a network of situations.

The states of the system at time t depend only on the states at the previous time slice ($t-1$) and the current time instance. Furthermore, the situational network is a probability distribution function on the sequence of T variables $X=\{x_1, x_2, \dots, x_T\}$ and T observables $Y=\{y_1, y_2, \dots, y_T\}$ that satisfies the requirements for DBNs with the following factorization, where the state x_t depends only on state x_{t-1} :

$$P(X, Y) = \prod_{t=2}^T P(x_t | x_{t-1}) \cdot \prod_{t=1}^T P(y_t | x_t) \cdot P(x_1) \quad (12)$$

The DBN parameters include the state transition pdf $P(x_{t+1} | x_t)$, the observation pdf $P(y_t | x_t)$ and pdf $P(x_1)$ using historical data, and prior knowledge or CPTs according to an expert's judgment should be defined.

5.2.2.3. The Risk Estimation Method

While the DBN-based situational network provides the prior and posterior probabilities of situations and their objects, the situation assessment should generate an assessment level of risk for every situation and show whether or not the current risk level is acceptable. Well-trained operators are usually able to form rules for every situation to assess risk, and those rules are an important part of their mental model. For instance, if an operator has the rule, ‘when the probability of the situation of accumulated vapor in the production unit is likely, and this situation has a catastrophic severity, therefore the risk level of this situation is not acceptable’, this rule helps the operator to understand that ‘when the risk level of the situation of accumulated vapor increases, the occurrence of an explosion is possible’. It is assumed that the operator’s mental model can be tailored using the rules for the hazardous situations of the environment. The results of this assessment are necessary for the subsequent component, i.e. situation recovery, in which new actions will be conducted to reduce situational risk to a level as low as reasonably practicable.

Situational risk estimation is highly subjective and is related to inexact and vague information, so the application of fuzzy logic is appropriate. Fuzzy logic, which mathematically emulates human reasoning, provides an intuitive way of designing function blocks for intelligent systems. Fuzzy logic allows an operator to express his/her knowledge in the form of related imprecise inputs and outputs in terms of linguistic variables, which simplifies knowledge acquisition and representation, and the knowledge obtained is easy to understand and modify. Therefore, to estimate the situational risk level, a fuzzy logic system (FLS) is utilized in the following steps:

- Estimation of the situation probability
- Estimation of the situation severity
- Estimation of the situation risk

A. The Situation Probability Estimation

The DBN-based situational network provides the prior and posterior probabilities (Decision 1-2 in Table 1). The quantitative analysis can be achieved by two methods: the forward method (or predictive analysis) and the backward method (or diagnostic analysis). In the forward method, the probability of occurrence of any situation in the situational network is calculated on the basis of the prior

probabilities of the objects and the conditional dependence of each situation. The backward method computes the posterior probability distribution of any situation and object, given the observation of a set of evidence. It can also be conducted to find the most probable explanation (MPE) of the states of the objects leading to hazardous situations or specific consequences.

B. The Situation Severity Estimation

The consequence states of a hazardous situation are usually determined by consequence analysis, which concerns what may follow the occurrence of a hazardous situation. Such an occurrence may lead to a wide range of consequences, some of which will probably be undesirable events. To project the degree of loss, the adverse outcomes associated with accidents identified through consequence analysis are investigated. Consequences can essentially be grouped into three categories; human loss, asset loss, and environmental loss.

Human loss is measured in ‘fatalities’, ‘injuries with disabilities’, ‘major injuries’, and ‘minor injuries’. These measurements help experts to aggregate various degrees of harm to a given group of people into an equivalent fatality figure. The convention ratio might be 1: 0.5: 0.1: 0.005 to respectively aggregate fatality, injury with disability, serious injury and minor injury for the estimation of human loss in equivalent fatalities. The degree of loss to enterprises can be estimated by considering several potential events such as damage to infrastructure and equipment, loss of materials and products, delay in services, loss of customers and goodwill, and possible legal fines. To generate an estimate for asset loss, all the potentials for a specific circumstance predicted by consequence analysis are converted to money. Environmental loss mainly focuses on the release and dispersion of harmful substances in the environment, and these harmful substances typically consist of any combination of oils, liquefied gases, flammable substances, reactive or radio-active materials, and bio-toxins. As the dispersion of these substances into the atmosphere may contaminate the water table, land, or rivers over time, both the immediate effects and potential future damage must be investigated. The cost of clean-up operations and emergency services, claims by affected parties, and fines by government are considered in estimating environmental loss [16].

To provide a coherent view of the totality of loss associated with a hazardous situation, all categories must be converted to a common currency. Although asset and environmental losses are generally expressed in monetary terms, the human loss forecast in the form of equivalent fatalities is

converted to an equivalent monetary value by employing the concept of Value of Preventing a Fatality [16].

The above loss analysis is usually conducted through a systemic investigation process by a group of experts who are familiar with loss estimation and prevention. In addition, the consequence of a hazardous situation is considered to remain constant throughout the lifetime of the system. Table 2 shows the proposed severity matrix of this study, which includes an estimated dollar value of damage for each consequence category (Decision 1-3 in Table 1).

Table 2: Consequence severity matrix.

Severity class	Monetary Value	Human Loss	Asset Loss	Environmental Loss
Negligible	<10k	One minor injury	Minor repairs that can be done immediately by own crew	Around the area, easy recovery
Minor	10-100k	One or two minor injuries	Repairs that take several days to carry out	Within the plant, short term remediation effort
Medium	100k-1 million	Multiple major injuries	Damage that takes months to repair and causes serious consequences	Minor offsite impact, remediation cost will be less than 1 million
Major	1-10 million	One fatality or multiple injuries with disabilities	Very large material damage	Community advisory issued, remediation cost remains below 10 million
Catastrophic	>10 million	Multiple fatalities	Significant parts of the system destroyed	Community evacuation for longer period, remediation cost in excess of 10 million

C. The Situation Risk Estimation

To estimate the risk level of every situation, an FLS is used. The selection of a membership function for variables essentially depends on the variable characteristics, available information and expert knowledge. The shapes of the membership functions are defined as a combination of trapezoidal and triangular numbers to simplify the operation and increase the sensitivity in a number of bounds. The α level cuts “1” and “0” are used to describe the fuzzy sets for each variable. Tables 3-5 present the fuzzification of variables and Figure 7 illustrates the proposed fuzzy sets. The logic relations between variables, including the 25 rules (e.g. IF *probability is E* AND *severity is MA* THEN *risk is NA*) are shown in Table 6. To generate the output, Mamdani’s fuzzy inference method described in Table 7 is used to implicate each single rule and aggregate the outcome from all rules into a single output fuzzy set. In the defuzzification process, the output fuzzy set of risk is converted into a crisp value, which is used for the risk evaluation category (Decision 1-4 in Table 1).

Table 3: Fuzzification of probability.

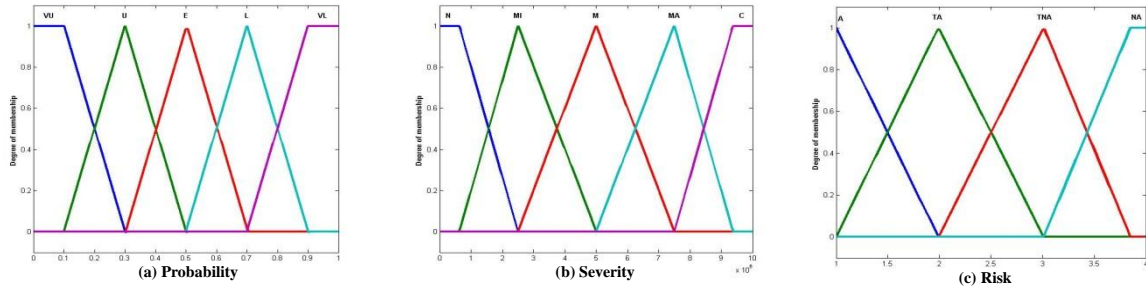
Set	Linguistic term	α level cuts	
		1-level cut	0-level cut
VL	Very likely	1e-007, 1	3e-007
L	Likely	3e-007	5e-007, 1e-007
E	Even	5e-007	7e-007, 3e-007
U	Unlikely	7e-007	9e-007, 5e-007
VU	Very Unlikely	1e-006, 9e-007	7e-007
Universe of discourse: $(10^{-6}-10^0)$			

Table 4: Fuzzification of severity.

Set	Linguistic term	α level cuts	
		1-level cut	0-level cut
N	Negligible	0, 6.25E+05	2.5E+06
MI	Minor	2.5E+06	6.25E+05, 5E+06
M	Medium	5E+06	2.5E+06, 7.5E+06
MA	Major	7.5E+06	5E+06, 9.375E+06
C	Catastrophic	9.375E+06, 1E+07	7.5E+06
Universe of discourse: (0-10 ⁷)			

Table 5: Fuzzification of risk.

Set	Linguistic term	α level cuts	
		1-level cut	0-level cut
A	Acceptable	1	2
TA	Tolerable acceptable	2	1, 3
TNA	Tolerable not acceptable	3	2, 3.85
NA	Not acceptable	3.85, 4	3
Universe of discourse: (1-4)			

**Figure 7:** Membership functions of probability, severity and risk variables.**Table 6:** Risk matrix.

		Severity				
		N	MI	M	MA	C
Probability	VL	TNA	TNA	NA	NA	NA
	L	TA	TNA	TNA	NA	NA
	E	A	TA	TNA	NA	NA
	U	A	A	TA	TNA	NA
	VU	A	A	TA	TNA	TNA

Table 7: Characteristics of the Mamdani model [32].

Operation	Operator	Formula
Union (OR)	MAX	$\mu_C(x) = \max(\mu_A(x), \mu_B(x)) = \mu_A(x) \vee \mu_B(x)$
Intersection (AND)	MIN	$\mu_C(x) = \min(\mu_A(x), \mu_B(x)) = \mu_A(x) \wedge \mu_B(x)$
Implication	MIN	$\max(\min(\mu_A(x), \mu_B(x)))$
Aggregation	MAX	
Defuzzification	CENTROID (center of gravity)	$COA = Z^* = \frac{\int z \mu_C(z) dz}{\int \mu_C(z) dz}$

$\mu_C(x)$ = value of the resultant membership function. $\mu_A(x)$ = value of the membership function where the input belongs to the fuzzy set A. z = abscissa value, $(\mu_C(z))$ is the ordinate).

5.2.3. The Situation Recovery Component

If the estimated risk of the situation is unacceptable, it is necessary to recover the situation.

Identifying the risk-reducing measures therefore contributes to decisions about risk control, mitigation,

transfer, elimination, or an appropriate combination thereof. However, the DBN does not provide the risk reduction measures; it helps to simulate the impact of risk recovery decisions on a situation. A list of available reduction and containment options can be presented as decision rules (i.e. IF *Antecedent*; THEN *Consequent*) where ‘antecedent’ is a situation, while ‘consequent’ is a suggested action to remove or eliminate the risk and recover the situation (Decision 2-1 in Table 1). Based on the operator’s response to choosing practical options, the situation assessment component has the ability to simulate the situation and estimate the new risk level (Decision 2-2 in Table 1). The aim is to eliminate or reduce the risk level of situations to an acceptable level.

5.2.4. The Human-Computer Interface

A graphical user interface (GUI) for the proposed system is developed based on SA-oriented design principles and using SMILE (Structural Modeling, Inference, and Learning Engine), which is a library of C++ classes for implementing BNs in intelligent systems [29]. The proposed system does not control the manner of actions and maintains the operator’s involvement in the decision-making process. The development of human-computer interactions indicates that, with insufficient automation, operators will have an excessive workload, whereas too much automation may disconnect operators from the system and alienate them from the production process [2]. Therefore, keeping operators in the loop of decision-making, taking action, and updating the related information are critical issues in designing support systems.

5.3. The Proposed SASS Evaluation

Evaluation is an important aspect of every methodology because it provides a reasonable amount of confidence in the results of the model. The SASS is based on DBNs, therefore the evaluation can be conducted in two ways: by SA measurement, or by sensitivity analysis. The SA measurement can be used for full validation of the human-computer interface and the sensitivity analysis is appropriate for the partial evaluation of BN models. The validation of the proposed system in this paper is demonstrated by sensitivity analysis through the case study, and a full evaluation will be conducted in a future study based on the SA measurement.

5.3.1. Situation Awareness Measurement

The enhancement of SA is a major goal in the design and development of human-computer interfaces, training programs, and automation concepts in a variety of systems. To evaluate the degree to which new technologies and design concepts improve an operator's SA, it is necessary to analyze these concepts systematically based on a measure of SA that can determine which ideas have merit and which may have negative effects [9]. A recent review identified several different SA measurement approaches, categorized into the following types: 1) Self-rating techniques, 2) Freeze probe techniques, 3) Observer rating techniques, 4) Real-time probe techniques, 5) Process indices, and 6) Performance measures.

The literature shows that the SAGAT¹, which is a freeze probe technique, and the SART², which is a self-rating approach, are the most common SA measurement techniques to be applied during individual and team SA assessments. However, many researchers argue that further investigation to develop the measurement of SA in complex and dynamic systems is required [14, 43].

5.3.2. Sensitivity Analysis

To develop the proposed system, this study relies on DBNs, permitting the investigation of a partial validation by sensitivity analysis, according to the following three axioms [19]:

- 1) A slight decrease/increase in the prior probabilities of each parent node should result in the effect of a relative decrease/increase of the posterior probabilities of the child node.
- 2) Given the variation of subjective probability distributions of each parent node, the magnitude of influence of the parent node on the child node values should remain consistent.
- 3) The magnitude of the total influence of the combination of probability variations from x attributes (evidence) on the values should be always greater than the probability variations from the set of x - y ($y \in x$) attributes (sub-evidence).

To validate the proposed DBNs, the parameters used need to be closely monitored for a long period of time. Therefore the above axioms are useful for partial validation.

6. A Case Study

To demonstrate and test the performance of the SASS, three case studies were used: a tank equipped with steam coils at a chemical plant [5], an ink vehicle insulated mix tank at a paint

¹ Situation Awareness Global Assessment Technique

² Situation Awareness Rating Technique

manufacturing company [6], and a residue treater at a methomyl production unit [7]. In this paper, the first case study is chosen because it is easier to understand than the other two; it also adds a sense of urgency or reality to the proposed system, and shows how the system works. In addition, it provides a real application of the proposed system and helps to validate its performance.

6.1. The Case Description

The case concerns the ignition of a vapor cloud in a 2,200-gallon open-top tank used for mixing a flammable liquid in the manufacture of a product called “Super Clean and Tilt”, a proprietary mixture that is applied to cured concrete surfaces to prevent bonding with wet concrete. According to the US Chemical Safety Board (CSB), an operator who was mixing and heating a flammable mixture of heptane and mineral spirits in the tank failed to maintain accurate SA and the vapor overflowed from the tank, resulting in the ignition of the vapor cloud. One person was killed and two employees were injured, causing significant business interruption [5].

The tank in this case is equipped with steam coils (Figure 8) that supply the heat required for the mixing process, a temperature controller that includes a temperature sensor and a pneumatic control unit, and steam valves, which are operated on the basis of the temperature of the mixture. Safety systems include a sprinkler system, an ignition barrier and an alarm system. The environment has local and area heating, and exhaust ventilation systems that are assumed to have sufficient capacity to collect a huge volume of vapor. The sprinkler system and fire alarm system have been designed to reduce damage if a fire occurs or vapor accumulates. An operator checks the temperature using an infrared thermometer, monitors the environment and conducts appropriate actions when necessary.

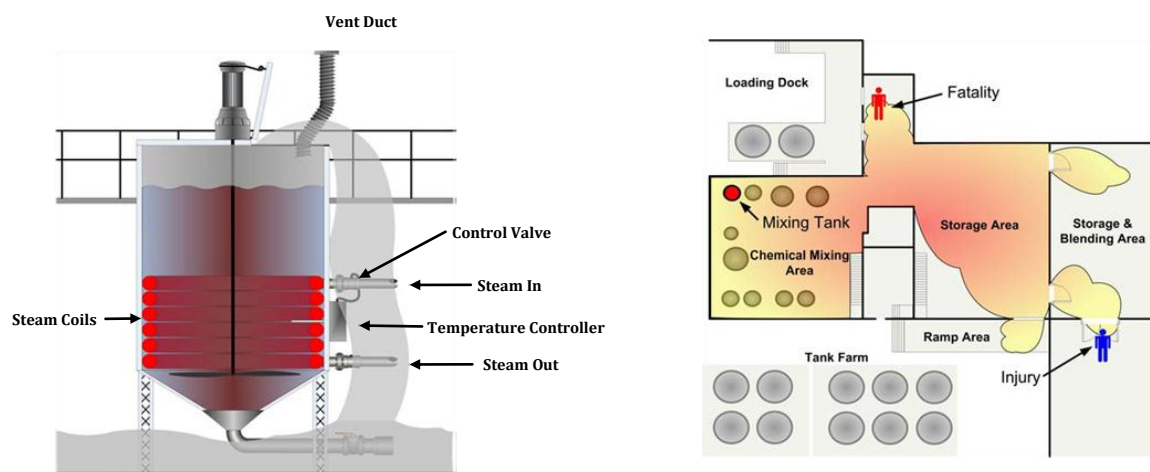


Figure 8: Mixing tank environment [5].

6.2. Situations of Interest

There are several possible hazardous situations in the environment that threaten the system. As the report shows, these hazardous situations are as follows:

- S^{AV} = Accumulated vapor in the production building
- S^{HT} = High temperature inside the tank
- S^{IV} = Inadequate building ventilation

The first situation is not directly inferrable from the objects, i.e. it is a “higher level situation” and has to be defined by the dependencies on first level situations. Table 8 shows the safety barriers and consequence node affected by S^{AV} . The second and third situations can be inferred from their contributor objects and observable variables, i.e. they are “first level situations”, and to assess them, a number of physical and conceptual objects are determined, as shown in Tables 9 and 10. The failure probabilities are determined based on data recorded by the Offshore Reliability Data Handbook [40].

Table 8: S^{AV} objects and symbols.

Objects	Symbol	Failure Probability
Ignition Barrier	I	0.1000
Alarm System	A	0.0013, 0.2250
Sprinkler System	P	0.04000
Consequences	C	NA

Note: the failure probability of the alarm system is affected by the ignition barrier or accumulated vapor.

Table 9: S^{HT} objects and symbols.

Objects	Symbol	Failure Probability
Operator	O	0.0200
Infrared Thermometer	T	0.0468
Sensor	S	0.0400
Pneumatic Unit	PU	0.2015
Temperature Measurement System	TMS	0.0658 (OR gate)
Manual Steam Valve	MSV	0.0243
Automatic Steam Valve	ASV	0.0276
Temperature Control System	TCS	0.2334 (OR gate)
Manual Temperature Control	MTC	0.0885 (OR gate)
Automatic Temperature Control	ATC	0.2549 (OR gate)

Table 10: S^{IV} objects and symbols.

Objects	Symbol	Failure Probability
Belt	B	0.0500
Fan	F	0.0100
Duct Plugging	D	0.0010

6.3. The Situation Data Collection Component

A sensor reports the tank temperature every minute, as noted above. There is also an environment temperature sensor that shows the temperature of the production unit. The monitoring system provides update information about these observable variables to the situation data collection component, and

this information is stored in a database and fuzzily prepared as inference evidence for use in the situation assessment component.

The process for making Super Clean and Tilt involves several hours of mixing and heating, with the temperature controller being adjusted to maintain the temperature at 73 °C. The environmental temperature in normal operation is about 25 °C. The value ranges of temperature variables based on expert knowledge and considering the limits for the six-sigma quality are divided into two fuzzy states, Normal and High, and their membership functions are illustrated in Figure 9 and determined as follows:

- ◆ Inside tank temperature (ToI): {Normal, High}

$$\mu_{ToI(N)}(x) = \begin{cases} 1 & x \leq 73 \\ (77 - x)/4 & 73 < x \leq 77 \end{cases} \quad (13)$$

$$\mu_{ToI(H)}(x) = \begin{cases} (x - 73)/4 & 73 \leq x < 77 \\ 1 & x \geq 77 \end{cases} \quad (14)$$

- ◆ Temperature of the production building (ToB): {Normal, High}

$$\mu_{ToB(N)}(x) = \begin{cases} 1 & x \leq 25 \\ (40 - x)/5 & 25 < x \leq 30 \end{cases} \quad (15)$$

$$\mu_{ToB(H)}(x) = \begin{cases} (x - 35)/5 & 25 \leq x < 30 \\ 1 & x \geq 30 \end{cases} \quad (16)$$

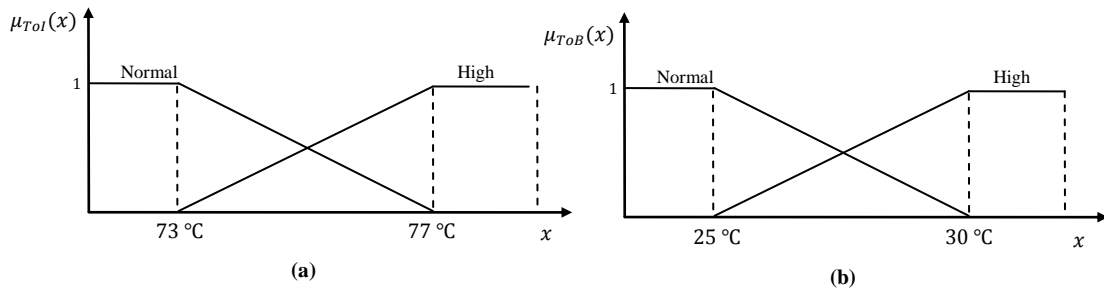


Figure 9: The membership functions of observable variables.

6.4. The Situation Assessment Component

A situational network for the case study is developed and illustrated in Figure 10. The figure shows three situations of interest in which the higher level situation is colored red, the first level situations are colored blue, and objects are shown in yellow. The time difference of one time step is set to one minute. The temporal arc points to the S^{AV} situation, as it is assumed that the situation is formed after a time interval that is longer than one minute. The interpretation is that the vapor accumulates when the

high temperature persists for a few minutes inside the tank and the ventilation system is unable to disperse it.

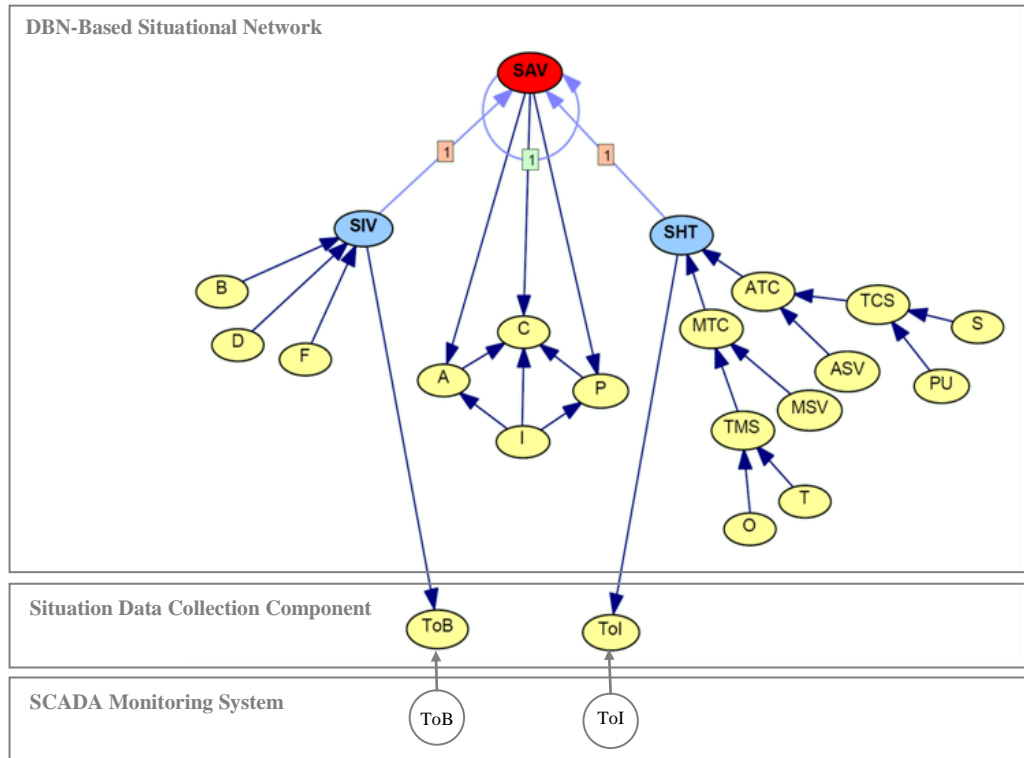


Figure 10: The situational network for three situations of interest.

The prior probability of the higher level situation, i.e. S^{AV} , is set to 1 for safe state and 0 for hazardous state, and it is assumed that the environment is initially safe. To establish other parameters, namely the conditional probabilities of the network, historical data and expert judgment are used. The CPTs of S^{AV} , S^{IV} and S^{HT} are shown in Tables 11-13, and other CPTs are omitted because they are set in a similar way.

Table 11: CPT of $P(S^{AV} | S^{AV}, S^{HT}, S^{IV})$.

S^{AV}	S^{HT}	S^{IV}	$S^{AV}=\text{Hazardous}$	$S^{AV}=\text{Safe}$
Hazardous	Hazardous	Hazardous	0.95	0.05
Hazardous	Hazardous	Safe	0.6	0.4
Hazardous	Safe	Hazardous	0.4	0.6
Hazardous	Safe	Safe	0.05	0.95
Safe	Hazardous	Hazardous	0.95	0.05
Safe	Hazardous	Safe	0.05	0.95
Safe	Safe	Hazardous	0.05	0.95
Safe	Safe	Safe	0.05	0.95

Table 12: CPT of $P(S^{HT} | \text{MTC}, \text{ATC})$.

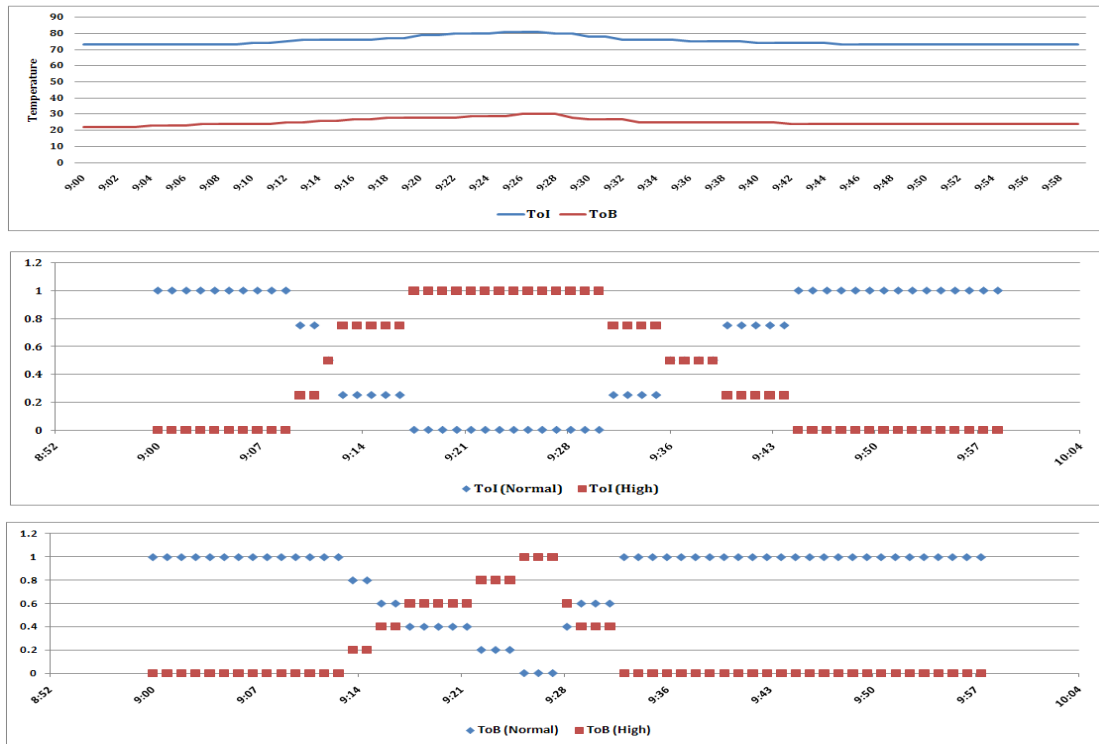
MTC	ATC	$S^{HT}=\text{Hazardous}$	$S^{HT}=\text{Safe}$
Failure	Failure	1	0
Failure	Success	0	1
Success	Failure	0	1
Success	Success	0	1

Table 13: CPT of $P(S^{IV} | D, F, B)$.

D	F	B	$S^{IV}=\text{Hazardous}$	$S^{IV}=\text{Safe}$
Failure	Failure	Failure	1	0
Failure	Failure	Success	1	0
Failure	Success	Failure	1	0
Failure	Success	Success	1	0
Success	Failure	Failure	1	0
Success	Failure	Success	1	0
Success	Success	Failure	1	0
Success	Success	Success	0	1

6.5. Evaluation of the Proposed System

On the morning of 14 June 2006, the temperature of the mixing tank and the production unit started to increase, with the former deviating from normal value at 9:10 AM and the latter deviating from normal value at 9:14 AM. The trend of observable variables for 60 minutes is illustrated in Figure 11 together with the fuzzy partitioning values of the variables. This information can be interpreted as ground truth data to evaluate the proposed system's performance. A sensitivity analysis based on the conditions of Section 5.3.2 is also presented.

**Figure 11:** The observable variables and their fuzzy partitioning values.

6.5.1. System Performance

By assigning the primary probabilities to the situation assessment component one minute after the start of the period, i.e. 9:01 AM, the probability of S^{AV} is 0.05 and the probabilities of the consequence states are calculated as shown in Table 14. As can be seen, the safe state is the most probable consequence of S^{AV} . The total loss of S^{AV} , i.e. its severity, can be calculated by multiplication of the

probabilities and losses of consequences, which is about $\$2.56\text{E}+04$. Therefore, the estimated risk level is 1.3, which means that the current risk level of S^{AV} is acceptable. It is worth noting that, for situations S^{HT} and S^{IV} , the accumulated vapor can be considered as their consequence in which the degree of loss is about $\$1\text{E}+06$.

Table 14: The consequences of S^{AV} .

Consequence	Symbol	Loss (\$)	Probability
Explosion	C1	5E+06	2.60E-06
Fire with low death and high property damage	C2	3E+06	0.0020
Fire with high death and moderate property damage	C3	4E+06	3.90E-06
Fire with low death and moderate property damage	C4	2E+06	0.0030
Vapor cloud with possibility of ignition	C5	1E+06	0.0100
Safe evacuation (near miss)	C6	1E+05	0.0349
Safe state	C7	0	0.9500

By assigning the fuzzy soft evidence that the situation data collection component provides for the situation assessment component, the posterior probabilities of the situations are updated during the period, as shown in Figure 12. As can be seen, the S^{HT} situation is hazardous from minutes 16 to 31 and situation S^{IV} becomes hazardous from minutes 24 to 28, as is expected as a result of the observable variables. In parallel, the risk level of S^{HT} is 2.95, i.e. TNA from minutes 16 to 31, and the risk level of S^{IV} is TNA during minutes 24 to 28, as shown in Figure 12. It is assumed that the local and area ventilation systems have the ability to evacuate the vapor, thus the risk level of S^{AV} is A from minutes 17 to 25, immediately before ventilation system malfunction; its risk level rises from minutes 25 and reaches a peak at 3.1, which means it is NA.

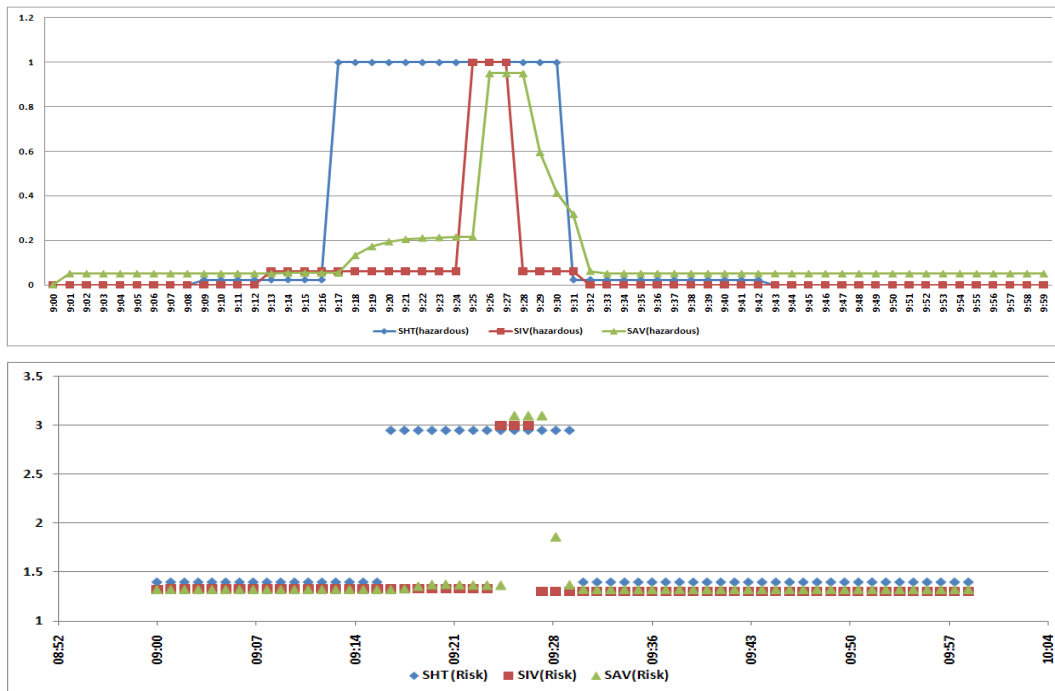


Figure 12: The posterior probabilities and risk levels of situations.

6.5.2. Sensitivity Analysis

Sensitivity analysis has been conducted to present a partial validation of the model. Examination of the model at time t reveals that, when the failure probability of “sensor” is set to 1 (i.e. Failure), this results in a revised failure probability of 1 from 0.23 and 0.25 for TCS and ATC respectively because of OR gate definition, and increases the failure probability of S^{HT} from 0.02 to 0.08. Likewise, at time t , when the failure probability of “infrared thermometer” is set to 1 (i.e. Failure), the failure probability of TMS and MTC is raised to 1 from 0.06 and 0.08, respectively, and the failure probability of S^{HT} is increased to 1 from 0.08. The evidence increases the failure probability 0.1 for S^{AV} from 0.05 at time $t+1$ (temporal dependency). Similarly, when at time t the failure probability of “fan” is set to 1 (i.e. Failure), this results in a revised failure probability of 1 from 0.06 for S^{IV} because of OR gate definition, and failure probability of 0.9 from 0.1 for S^{AV} at time $t+1$.

6.6. Situation Recovery Component

The system is set to trigger an alarm for every situation that has a risk level of more than 2.5 (i.e. tolerable not acceptable). At 9:16 AM when the risk level of S^{HT} rose, the system showed that the most probable explanation was the failure of the pneumatic unit (PU), but an inspection at 9:18 AM determined the valid performance of the temperature controller, i.e. the PU and the sensor (S). This evidence (success of PU and S) indicates that the failure of the automatic steam valve (ASV) was the most likely factor. Considering the result of the situation assessment, maintenance decisions to recover the situation were suggested in the situation recovery component. This demonstrates the system’s ability to support the operator in finding the most probable explanation for an abnormal situation and consequently assist in reducing the risk to an acceptable level. Additionally, the proposed system presents the factors that contribute to the creation of an accident or a specific consequence. For instance, if at 9:26 AM a fire with low death and moderate property damage (C4) is reported, the posterior probability of other nodes as a result of this evidence will show that failure of the ASV and belt caused the accumulated vapor, and failure of the ignition barrier caused the fire.

7. Discussion

This section compares the proposed situation assessment method in this paper and another existing BN-based model, and explains the limitations of this study.

7.1. Comparison with another Situation Assessment Model

To illustrate the key differences between different types of model, a BN-based situation assessment model proposed by Kim and Seong [24] is compared with this study's method in this section. The differences between the two models can be summarized as follows:

- The study by Kim and Seong (KS) does not provide a definition for the situation and assumes that the situation is equal to the nuclear power plant (NPP) environment in their study. In addition, the authors assume that the occurrences of various situations are mutually exclusive. Based on these assumptions, they 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. The situation in our study is clearly defined, and a situation modeling process proposed in which the situations might be inclusive.
- The KS model does not provide a situation model; it assumes that the situation model is the operator's understanding of the state of the plant. It also assumes that the situation can be modeled using the representative states of the plant, meaning that the operator only considers those representative states. The KS network therefore only includes indicators and sensors, based on which the KS model is unable to determine the cause of abnormal situations, nor can it support operators' understanding of such situations. In the KS model, therefore, operators have to rely on their knowledge to understand situations. In the study presented in this paper, the most probable causes of any abnormal situation can be obtained from the situation models that help operators to understand the situation.
- Learning, education, training, and other experiences enable operators to form mental models of plant dynamics in their long-term memory. The KS model uses deterministic rules to describe operators' mental models for the representative states of the environment. The authors incorporate the operators' mental models into the situation assessment model through the CPTs of the BN. In our paper's study, CPTs aside, the knowledge is used to encode the objects, relationships and observable variables that represent information sources and situations.

- The KS model only provides a set of probabilities for representative states that correspond to accidents or transitions, unlike the proposed system which 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 authors provide no evaluation method for the KS method. The study in this paper suggests two evaluation methods for the partial and full validation of the SASS. The partial evaluation is conducted by sensitivity analysis to validate the situation models and situational network, and SA measurement is suggested for the full evaluation of the SASS.

7.2. Limitations

The proposed SASS provides superior support for operators in safety-critical domains; however, there are several limitations and other important features related to human operators that should be taken into account:

- Human thinking is so complex that no computer program, however sophisticated, can ever replace it. This study makes two assumptions to simulate the situation assessment process conducted by human operators. First, it is assumed that operators use Bayesian inference to process incoming information. As operators do not perform mathematical calculations while performing a situation assessment, the proposed situation assessment model provides only approximations of operator behavior in the situation assessment process. The proposed model is expected to provide the most logical results and therefore can be considered to be optimistic. In the real world, the conclusions of a human operator will tend to be more conservative than the results of mathematical calculations based on Bayesian inference [24]. Second, this study assumes that the proposed FLS used to generate the assessment result for every situation is specially structured to resemble the human thinking process. Although well-skilled operators who have learned or acquired this knowledge by education and experience over a prolonged period of time are able to determine the risk level of situations, unskilled or semi-skilled operators need to consult the FLS.

- Since SASS is a dynamic system, it needs to have the ability to generate warnings when awareness is diminished due to uncertainty or lack of data. Operators may be confronted with an abnormal situation in which incorrect information is provided by failed sensors, or in which information is simply not available. Experienced operators are usually able to correctly recognize an abnormal situation, identify the failed sensors, and extract or deduce the correct information, but less experienced operators need to be supported by the proposed system to achieve SA.
- To develop the situation models, data are collected from domain experts. As the probability cannot be elicited perfectly, some uncertainty associated with the probability distributions will be unavoidable; therefore the data problem is also an important issue for the proposed system.

8. Conclusion and Future Work

This paper has presented a set of requirements based on GDTA methodology for the development of a SA support system to help operators in abnormal situations. A situational network modeling process was developed by exploiting the specific capabilities of DBNs, and a situation assessment method based on risk indicators proposed. The SASS was developed according to the identified requirements, the situation assessment method, and the receipt of online real information from the environment. As has been shown, the DBN-based situation assessment component provides a framework that is mathematically consistent for dealing with uncertain and incomplete information. Its reasoning is carried out using a probabilistic technique that generates consistent answers derived from a single multi-dimensional distribution. In addition, the Bayesian theorem facilitates the inclusion and updating of prior background knowledge when new information is available from the SCADA monitoring system. The proposed system also includes a situation recovery component that helps operators to reduce the risk of a situation to an acceptable level. The performance and effectiveness of the proposed system has been demonstrated through a real case study and evaluated through sensitivity analysis.

The first direction for future study is to develop a system prototype based on the proposed theoretical material, and to conduct an evaluation of the prototype based on SA measurement. In many safety-critical systems, the safety of the system is supervised by operators and engineers from a range

of departments who are members of a team. These team members have a common goal and perform specific roles in their interaction with elements in the task environment. The second future direction of the research, therefore, is to extend the proposed system to a distributed system that applies a team situation awareness concept.

Acknowledgment

The work presented in this paper was supported by Australian Research Council (ARC) under Discovery Projects DP088739 and DP110103733.

References

- [1] F. Baader, A. Bauer, P. Baumgartner, A. Cregan, A. Gabaldon, K. Ji, K. Lee, D. Rajaratnam, R. Schwitter, A novel architecture for situation awareness systems in: 18th International Conference on Automated Reasoning with Analytic Tableaux and Related Methods, (Springer Berlin / Heidelberg, Oslo, Norway, 2009), pp. 77-92.
- [2] N.G. Brannon, J.E. Seiffert, T.J. Draelos, D.C. Wunsch II, Coordinated machine learning and decision support for situation awareness, *Neural Networks*, 22(3) (2009) 316-325.
- [3] H. Chai, B. Wang, A hierarchical situation assessment model based on fuzzy Bayesian network, in: H. Deng, D. Miao, J. Lei, F. Wang Eds. *Artificial Intelligence and Computational Intelligence*, (Springer-Verlag, Berlin Heidelberg, 2011), pp. 444-454.
- [4] J.Q. Chen, S.M. Lee, An exploratory cognitive DSS for strategic decision making, *Decision Support Systems*, 36(2) (2003) 147-160.
- [5] CSB, Mixing and heating a flammable liquid in an open top tank in, (Washington, DC, 2007).
- [6] CSB, Confined vapor cloud explosion, in, (Washington, DC, 2008).
- [7] CSB, Pesticide chemical runaway reaction pressure vessel explosion, in, (Washington, DC, 2011).
- [8] S. Das, R. Grey, P. Gonsalves, Situation assessment via Bayesian belief networks, in: *Fifth International Conference on Information Fusion*, (Maryland, USA, 2002), pp. 664-671 vol.661.
- [9] M. Endsley, Measurement of situation awareness in dynamic systems, *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 37(1) (1995) 65-84.
- [10] M.R. Endsley, Toward a theory of situation awareness in dynamic systems, *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 37(1) (1995) 32-64.
- [11] M.R. Endsley, Situation awareness, in: G. Salvendy Ed. *Handbook of Human Factors and Ergonomics*, (John Wiley and Sons, 2006), pp. 528-542.
- [12] R. Farahbod, V. Avram, U. Glasser, A. Guitouni, Engineering situation analysis decision support systems, in: *2011 European Intelligence and Security Informatics Conference (EISIC)*, (Athens, Greece, 2011), pp. 10-18.
- [13] R. Ghanea-Hercock, E. Gelenbe, N.R. Jennings, O. Smith, D.N. Allsopp, A. Healing, H. Duman, S. Sparks, N.C. Karunatilake, P. Vytelingum, Hyperion-next-generation battlespace information services, *The Computer Journal*, 50(6) (2007) 632-645.
- [14] J.C. Gorman, N.J. Cooke, J.L. Winner, Measuring team situation awareness in decentralized command and control environments, *Ergonomics*, 49(12-13) (2006) 1312-1325.
- [15] J.S. Ha, P.H. Seong, A human-machine interface evaluation method: A difficulty evaluation method in information searching (DEMIS), *Reliability Engineering & System Safety*, 94(10) (2009) 1557-1567.
- [16] A. Hessami, A systems framework for strategic approach to risk in e-business, *International Journal of Information Science and Management*, (Special) (2010) 89-121.
- [17] M.-H. Hsieh, S.-L. Hwang, K.-H. Liu, S.-F.M. Liang, C.-F. Chuang, A decision support system for identifying abnormal operating procedures in a nuclear power plant, *Nuclear Engineering and Design*, 249(0) (2012) 413-418.
- [18] Y. Hu, X. Zhang, E.W.T. Ngai, R. Cai, M. Liu, Software project risk analysis using Bayesian networks with causality constraints, *Decision Support Systems*, (2012) <http://dx.doi.org/10.1016/j.dss.2012.1011.1001>.
- [19] B. Jones, I. Jenkinson, Z. Yang, J. Wang, The use of Bayesian network modelling for maintenance planning in a manufacturing industry, *Reliability Engineering & System Safety*, 95(3) (2010) 267-277.
- [20] R. Jones, E. Connors, M. Mossey, J. Hyatt, N. Hansen, M. Endsley, Using fuzzy cognitive mapping techniques to model situation awareness for army infantry platoon leaders, *Computational & Mathematical Organization Theory*, 17(3) (2011) 272-295.

- [21] B.C. Juricek, D.E. Seborg, W.E. Larimore, Predictive monitoring for abnormal situation management, *Journal of Process Control*, 11(2) (2001) 111-128.
- [22] D.B. Kaber, M.R. Endsley, Team situation awareness for process control safety and performance, *Process Safety Progress*, 17(1) (1998) 43-48.
- [23] N. Khakzad, F. Khan, P. Amyotte, Dynamic safety analysis of process systems by mapping bow-tie into Bayesian network, *Process Safety and Environmental Protection*, 91(1-2) (2012) 46-53.
- [24] M.C. Kim, P.H. Seong, An analytic model for situation assessment of nuclear power plant operators based on Bayesian inference, *Reliability Engineering & System Safety*, 91(3) (2006) 270-282.
- [25] M.C. Kim, P.H. Seong, A computational method for probabilistic safety assessment of I&C systems and human operators in nuclear power plants, *Reliability Engineering & System Safety*, 91(5) (2006) 580-593.
- [26] Y.J. Kim, C.M. Hoffmann, Enhanced battlefield visualization for situation awareness, *Computers & Graphics*, 27(6) (2003) 873-885.
- [27] R. Klashner, S. Sabet, A DSS design model for complex problems: Lessons from mission critical infrastructure, *Decision Support Systems*, 43(3) (2007) 990-1013.
- [28] M.M. Kokar, C.J. Matheus, K. Baclawski, Ontology-based situation awareness, *Information Fusion*, 10(1) (2009) 83-98.
- [29] D.S. Laboratory, SMILE (structural modeling, inference, and learning engine), (University of Pittsburgh, 1998).
- [30] J. Lu, B. Liu, G. Zhang, Z. Hao, Y. Xiao, A situation assessment approach using support vector machines as a learning tool, *International Journal of Nuclear Knowledge Management*, 3(1) (2008) 82-97.
- [31] J. Lu, X. Yang, G. Zhang, Support vector machine-based multi-source multi-attribute information integration for situation assessment, *Expert Systems with Applications*, 34(2) (2008) 1333-1340.
- [32] E.H. Mamdani, Application of fuzzy logic to approximate reasoning using linguistic synthesis, *IEEE Transactions on Computers*, C-26(12) (1977) 1182-1191.
- [33] A.S. Markowski, M.S. Mannan, A. Kotynia, H. Pawlak, Application of fuzzy logic to explosion risk assessment, *Journal of Loss Prevention in the Process Industries*, 24(6) (2011) 780-790.
- [34] R.E. Melchers, On the ALARP approach to risk management, *Reliability Engineering & System Safety*, 71(2) (2001) 201-208.
- [35] K.P. Murphy, *Dynamic Bayesian networks: Representation, inference and learning*, (University of California, Berkeley, 2002).
- [36] M. Naderpour, J. Lu, A fuzzy dual expert system for managing situation awareness in a safety supervisory system, in: 21st IEEE International Conference on Fuzzy Systems, (Brisbane-Australia, 2012), pp. 715-721.
- [37] M. Naderpour, J. Lu, Supporting situation awareness using neural network and expert system, in: 10th International FLINS Conference on Uncertainty Modeling in Knowledge Engineering and Decision Making, (Istanbul-Turkey, 2012), pp. 993-998.
- [38] L. Niu, J. Lu, G. Zhang, *Cognition-driven decision support for business intelligence: Models, techniques, systems and applications*, (Springer-Verlag, Berlin Heidelberg, 2009).
- [39] L. Niu, J. Lu, G. Zhang, D. Wu, Facets: A cognitive business intelligence system, *Information Systems*, 38(2013) 835-862.
- [40] OREDA, *Offshore reliability data handbook*, (SINTEF Industrial Management, 2002).
- [41] D.J. Power, R. Sharda, Model-driven decision support systems: Concepts and research directions, *Decision Support Systems*, 43(3) (2007) 1044-1061.
- [42] Y. Qian, L. Xu, X. Li, L. Lin, A. Kraslawski, Lubres: An expert system development and implementation for real-time fault diagnosis of a lubricating oil refining process, *Expert Systems with Applications*, 35(3) (2008) 1252-1266.
- [43] P.M. Salmon, N.A. Stanton, G.H. Walker, D. Jenkins, D. Ladva, L. Rafferty, M. Young, Measuring situation awareness in complex systems: Comparison of measures study, *International Journal of Industrial Ergonomics*, 39(3) (2009) 490-500.
- [44] A.F. Shapiro, Fuzzy random variables, *Insurance: Mathematics and Economics*, 44(2) (2009) 307-314.
- [45] P.R. Smart, A. Russell, N.R. Shadbolt, L.A. Carr, Aktivesa: A technical demonstrator system for enhanced situation awareness, *The Computer Journal*, 50(6) (2007) 703-716.
- [46] X. Su, P. Bai, F. Du, Y. Feng, Application of Bayesian networks in situation assessment, in: R. Chen Ed. *Intelligent Computing and Information Science*, (Springer-Verlag Berlin Heidelberg, 2011), pp. 643-648.
- [47] A.C. Van den Broek, R.M. Neef, P. Hanckmann, S.P. Van Gosliga, D. Van Halsema, Improving maritime situational awareness by fusing sensor information and intelligence, in: 14th International Conference on Information Fusion (FUSION), (2011), pp. 1-8.