The Explosion at Institute: Modeling and Analyzing the Situation Awareness Factor

Mohsen Naderpour[1], 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:

In 2008 a runaway chemical reaction caused an explosion at a methomyl unit in West Virginia, USA, killing two employees, injuring eight people, evacuating more than 40,000 residents adjacent to the facility, disrupting traffic on a nearby highway and causing significant business loss and interruption. Although the accident was formally investigated, the role of the situation awareness (SA) factor, i.e. a correct understanding of the situation, and appropriate models to maintain SA, remain unexplained. This paper extracts details of abnormal situations within the methomyl unit and models them into a situational network using dynamic Bayesian networks. A fuzzy logic system is used to resemble the operator's thinking when confronted with these abnormal situations. The combined situational network and fuzzy logic system make it possible for the operator to assess such situations dynamically to achieve accurate SA. The findings show that the proposed structure provides a useful graphical model that facilitates the inclusion of prior background knowledge and the updating of this knowledge when new information is available from monitoring systems.

Keywords: Situation awareness, Situation assessment, Abnormal situations, Methomyl unit, Accident analysis.

1. Introduction

On Thursday 28 August 2008 a runaway chemical reaction occurred at a methomyl production facility in Institute, West Virginia, USA. Highly flammable solvent sprayed from a 4,500 gallon pressure vessel known as a residue treater and immediately ignited, killing two employees and injuring eight firefighters and contractors. The intense fire burned for more than four hours, more than 40,000 residents were evacuated to shelter-in-place for over three hours, and the highway was closed for hours because of smoke disruption to traffic. The Chemical Safety Board (CSB) investigation team determined that the runaway chemical reaction and loss of containment of the flammable and toxic chemicals was the result

[1] Corresponding author, Tel: +61 2 9514 4520

of deviation from the written start-up procedures and included the bypassing of critical safety devices intended to prevent such a condition occurring. A poor process mimic screen, which could not provide adequate situation awareness (SA) for the board operator, was another important contributing factor (CSB 2011). The tragic event at Institute is an example of the difficulties experienced with regard to loss of SA, poor SA or lack of SA, all of which are now popular terms in accident investigation reports. However, SA itself is not the only cause of accidents (Dekker 2013). In the case of the Texas City, TX BP Amoco Refinery explosion on 23 March 2005, in which 15 workers were killed and 170 injured, several failed control instrumentation and alarms caused an overfilled and over-pressurized tower to discharge a large quantity of flammable liquid into the atmosphere, while the control room operator could not maintain accurate SA when monitoring this complex, fast moving environment, and an ignition created one of the worst industrial disasters in recent US history (Pridmore 2007).

A situation is a set of circumstances in which a number of objects may have relationships with one another and the environment, and situation awareness (SA) is knowing and understanding what is going on around you and predicting how things will change (Vincenzi *et al.* 2004). To date, several SA models, such as Endsley (1995), Bendy and Meister (1999), and Adams et al. (1995) have been developed; however, Endsley's model has undoubtedly received the most attention. This three-level 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" (Endsley 1995). 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 (Endsley 1995). In fact, situation assessment models explain the main features and general principles about how people process information and interact with the environment to maintain their SA. The primary research into SA came from the aviation industry, when a review of aircraft accidents showed that poor SA was the main causal factor. It was also found that most of the errors occurred when data were unavailable or difficult to discriminate or detect (level 1). About 20% of errors involved lack of, or an incomplete mental model, use of an incorrect mental model, over-reliance on default values, and miscellaneous other factors (level 2). In addition, around 3.5% of errors involved over-projection of current trends or miscellaneous other factors (level3). Another review in offshore drilling accidents by Sneddon et al. (2013) showed that 40% of such accidents are related to SA, and the

majority of those SA errors (67%) occurred at the perceptual level, 20% concerned comprehension, and 13% arose during projection. Therefore, this is not a problem limited to aviation, but one faced by many complex systems when combining and presenting the vast amounts of data available from many technological systems in order to provide true SA is a challenge.

In complex systems, SA level 1 is highly supported through the various heterogeneous sensors and appropriate signal-processing methods to extract as much information as possible about the dynamic environment and its elements, but regarding SA levels 2 and 3, there is still a need for appropriate and effective methods to support operators to infer real situations and to project their status in the near future (Fischer *et al.* 2011, Jones *et al.* 2011). In maritime security, an automated system has been developed that has the ability to recognize any deviance from normal behavior (Van den Broek *et al.* 2011). In military services, there are several SA systems, such as (Ghanea-Hercock *et al.* 2007) and (Smart *et al.* 2007), 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 have to integrate information by themselves to assess and project a future situation, so a system architecture has been developed by Baader et al. (2009) that focuses on using formal logic and an automated theorem to build an SA system in a more useful way. In the force protection domain, Brannon et al. (2009) used machine learning techniques to project a threat index. They took into account various inputs such as binary, categorical, and real-valued data to generate attributes including confidence levels, as well as evidence in support of, or against the assessment. In the aviation domain, an SA system called the tactile situation awareness system (TSAS) has been developed by Kim and Hoffmann (2003) 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. In the domain of nuclear power plants, Kim and Seong (2006) proposed a computational model of situation assessment that projects the states of the environment probabilistically when receiving information from indicators. Fischer and Beyerer (2012) also applied automated projection in surveillance systems where situations of interest in the maritime domain are recognized by calculating probabilities for the situations, given evidence obtained from observable characteristics. Although the application of SA systems is not

limited to the above domains, its application in safety-critical environments such as process control 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 support systems, 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 (Qian *et al.* 2008) or the prediction of process variables (Juricek *et al.* 2001) that will violate an emergency limit in the future; however, further research showed 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 (Klashner and Sabet 2007). When an abnormal situation occurs in a safety-critical system, operators firstly recognize it by receiving an alarm, and secondly need to understand what is happening in the plant by situation assessment. During the situation assessment process, operators receive information from observable variables or other operators and process the information to establish situation models based on their mental models (Kim and Seong 2006).

This study aims to introduce a methodology to model and analyze the SA factor in abnormal situations that can be utilized in the development of operator support systems. To identify abnormal situations, this paper uses risk indicators. Therefore, when a hazardous situation is defined as a possible circumstance immediately before harm is produced by the hazard, an abnormal situation is defined as a hazardous situation if its risk is not acceptable. This definition can also 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 uses Bayesian networks to model situation models based on a control room operator's mental models, and it also relies on risk level projections to show whether the situation is abnormal or not, and provides the priorities. A human-system interface based on the proposed approach is designed for the methomyl unit environment and the performance of the system is investigated through real data collected from the unit.

The paper is organized as follows. Section 2 presents our methodology for modeling and analyzing the SA factor. The process of the residue treater and timeline of events are explained in Section 3. The performance and results of the proposed methodology in the residue treater environment are presented in Section 4. The conclusion and future work are summarized in Section 5.

2. Modeling and analyzing situation awareness

The use of Bayesian networks (BNs) in situation assessment configuration of dynamic and complex domains has several advantages in comparison with other situation assessment methods that use other artificial intelligence tools such as expert systems (Naderpour and Lu 2012a) and neural networks (Naderpour and Lu 2012b). 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 (Naderpour *et al.* 2014a).

In the following sections, general information about BNs, and how a situational network can be developed and analyzed, are explained.

2.1. Bayesian networks

A situation is a set of circumstances in which a number of objects may have relationships with one another and the environment. Therefore, conventional BNs can be considered as a representation of static cause–effect relations between objects in a situation. From this point of view, a BN is a directed acyclic graph whose nodes correspond to objects and the arcs between nodes represent dependencies or direct causal influences between objects. The parameters of a BN determine the strength of the probabilistic relations between its nodes. Each node in the BN has a set of mutually exclusive and collectively exhaustive states with a probability distribution conditional on the states of its parent nodes, or an unconditional distribution if the node does not have any parents. The conditional and unconditional probabilities can be learned from available data or elicited from domain experts (Yet *et al.* 2013). 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 $X = \{X_1, X_2, \dots, X_n\}$, included in the network as:

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

where $Pa(X_i)$ is the parent set of X_i for any *i=1,…,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. BN takes advantage of Bayes theorem to update the prior occurrence probability of objects given new information, called evidence *E*, thus yielding the posteriors. This new information usually becomes available during the operational life of a system, including the occurrence or non-occurrence of objects (Khakzad *et al.* 2012):

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

This equation can be used for either prediction or diagnostic analysis. In predictive analysis, conditional probabilities of the form *P(situation|object)* are calculated, indicating the occurrence probability of a particular situation given the occurrence or non-occurrence of a certain primary object. On the other hand, in diagnostic analysis, those of the form *P(object|situation)* are evaluated, showing the occurrence probability of a particular object given the occurrence of a certain situation (Naderpour *et al.* 2013).

The static BN can be extended to a dynamic BN (DBN) model by introducing relevant temporal dependencies that capture the dynamic behaviors of the domain variables between representations of the static network at different times. Two types of dependencies can be distinguished in a DBN: contemporaneous and non-contemporaneous. Contemporaneous dependencies refer to arcs among nodes that represent variables within the same time period. Non-contemporaneous dependencies refer to arcs between nodes which represent variables at different times. A DBN is defined as a pair $(B_1, 2TBN)$ where B_1 is a BN which defines the prior distribution $P(X_1)$ and *2TBN* is a two-slice temporal BN with

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

where X_t^i is a node at time slice *t* and $Pa(X_t^i)$ is the set of parent nodes which can be in time slice *t* or in time slice *t-1*. The nodes in the first slice of a *2TBN* do not have any parameters associated with them, but each node in the second slice has an associated conditional probability distribution (CPD) for continuous variables or conditional probability table (CPT) for discrete variables, which defines $P\left(X_t^i|Pa(X_t^i)\right)$ for all $t > 1$. The arcs between slices are from left to right, reflecting the causal flow of time. If there is an arc from X_{t-1}^i to X_t^i, this node is called persistent. The arcs within a slice are arbitrary. Directed arcs

within a slice 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 (Murphy 2002):

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

2.2. Situational network development

Figure 1 shows our proposed method to develop a network of abnormal situations using BNs. To identify hazardous situations, an analysis is carried out using a combination of cognitive engineering procedures and hazard identification methods. Observation of operator performance, analysis of written materials and documentation, expert elicitation and formal questionnaires may be used to conduct the analysis (Endsley 2006). Previous hazard identification documents may help with this analysis. For example, HAZOP, one of the most powerful methods available, has been well-described in the literature and can help to determine the basic objects that contribute to the occurrence of situations. The situation model usually begins with root nodes, which are the basic objects, followed by intermediate nodes, a pivot node and leaf nodes. The pivot node is the focal object that delegates the situation, and relations among the root nodes and the pivot node define the relationships among the objects. The leaf nodes may be safety barriers which are physical objects of the environment and will connect to one another if there is relation between their performances. Also, one of the leaf nodes may be a consequence node that shows the possible accidents in the situation. If the situation is inferred by one or more observable variables, the focal object is connected to the observable variables.

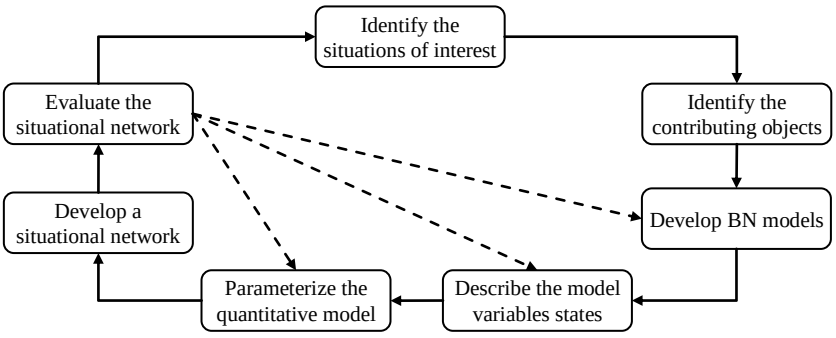

Figure 1: A cycle to build a situational network using BNs.

The states of basic and intermediate objects and safety barriers are defined as Boolean (i.e. success and failure), which refers to the objects working well (success) or not working (failure). The focal object

has two states, i.e. safe and hazardous. The states of consequence nodes are usually determined by consequence analysis, which concerns what may follow the occurrence of an abnormal situation. The states of observables are determined in terms of operation, six sigma quality and safety set-points. 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. Because the concept of fuzzy set theory can provide a method that is more smoothly structured, the states of observable variables are determined using a fuzzy partitioning method and fuzzy states definition (Naderpour *et al.* 2014b).

The prior probability of basic objects (nodes without parents) can be obtained through failure probability datasets such as the Center for Chemical Process Safety (CCPS 1989), and the Offshore Reliability Data Handbook (OREDA 2002), and if the failure probability is not available, expert judgment can be used. The CPTs of intermediate and pivot nodes are set based on "OR gate" or "AND gate" definitions. The CPTs of observable variables are determined by domain experts with recursive techniques (e.g. Delphi method) to guarantee the convergence of the results. The CPTs of consequence nodes are determined by 0 and 1 value corresponding to appropriate states.

Based on the above description, a situation may depend on the existence of other situations, or the existence of one situation can exclude the existence of another situation. The complete modeling of the dependencies results in a network of situations. As a result of this modeling, the existence of a situation is inferred based on information in the World, i.e. the observable variables and objects of configuration space. This also includes temporal dependencies, i.e. that the existence probability of an inferred situation in future can be supported by the earlier existence of the situation itself (Naderpour *et al.* 2014a).

Evaluation of the situational network requires the assessment of model behavior to ensure that the model demonstrates acceptable behavior. Sensitivity analysis is a technique for the systematic investigation of the influence of variation in the model inputs on this model's outcome, where inputs can be the parameters (i.e. values of conditional probabilities) or real inputs (i.e. values of observable nodes) (Bednarski *et al.* 2004). Sensitivity to findings based on a *d*-separation concept determines whether evidence about one variable may influence belief in a query variable. Using sensitivity to findings, it is possible to rank evidence nodes that allow the expert to identify whether a variable is sensitive or insensitive to other variables in particular contexts. This helps to identify errors in either the network

structure or the CPTs. In this regard, entropy is a common measure that assesses the average information required, in addition to the current knowledge, to specify a particular alternative. The entropy of a distribution over variable *X* is defined as follows:

$$H(X) = -\sum_{x \in X} P(x)\ log\ P(x) \tag{5}$$

and mutual information is used to measure the effect of one variable (*X*) on another (*Y*):

$$I(X,Y) = H(X) - H(X|Y) \tag{6}$$

where $I(X,Y)$ is the mutual information between variables. This measure reports the expected degree to which the joint probability of *X* and *Y* diverges from what it would be if *X* were independent of *Y* (Pollino *et al.* 2007). Sensitivity to parameters considers altering each of the parameters of query nodes and observing the related changes in the posterior probabilities of the query node. Most such sensitivity analyses are one-dimensional and, therefore, they only vary one parameter at a time. If models are unaffected by the precision of either the model or the input numbers, they may still be sensitive to changes in combinations of parameters. However, testing all possible combinations of parameters is exponentially complex (Korb and Nicholson 2003). The one-dimensional sensitivity analysis can be conducted by a sensitivity function for the output probability $f(x)$ when *x* is being varied. This sensitivity function is defined as follows (Laskey 1995):

$$f(x) = \frac{\alpha x + \beta}{\gamma x + \delta} \tag{7}$$

where $\alpha, \beta, \gamma, \delta \in \mathbb{R}$ and they are constants built from parameters that are fixed. The sensitivity value of the parameter *x* and the target probability can be obtained by taking the first derivative from the sensitivity as follows (Laskey 1995):

$$f'(x) = \frac{\alpha\delta - \beta\gamma}{(\gamma x + \delta)^2} \tag{8}$$

2.3. Situational network analysis

Usually, well-trained operators are able to form rules for every situation to assess their risks dynamically, and those rules are an important part of their mental models. For instance, if an operator has this rule: ‘when the probability of the situation of accumulated vapor in the production unit is likely and this situation has catastrophic severity, the risk level of this situation is not acceptable’. The rule helps the operator to understand that ‘when the risk level of the situation of accumulated vapor is increasing, the occurrence of an explosion is possible’. In this sense, it is assumed that the operator’s mental model can

be modeled using the rules for hazardous situations in that environment. Based on these rules, an operator tries to keep the situational risk to as low a level as reasonably practicable. Therefore, to resemble and analyze situational behavior based on the thought processes of operators, the methodology needs to generate an assessment level of risk for every situation over time. Figure 2 shows our proposed cycle for analyzing the situational network.

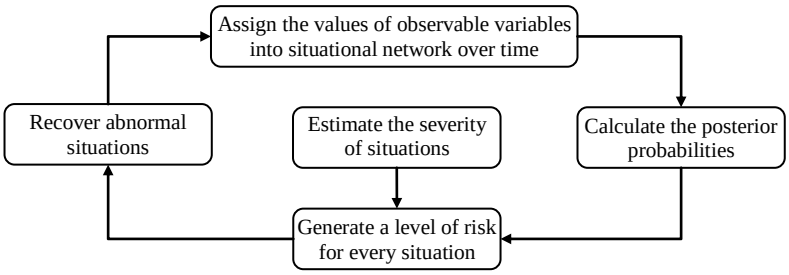

Figure 2: A cycle to analyze the situational network over time.

Suppose the configuration space σ is defined by all possible physical and conceptual objects. The current risk level of a situation at time t is defined as $R(S_t) = P(S_t) * S(S_t)$ where $P(S_t)$ is the probability and $S(S_t)$ is the severity of the situation. $P(S_t)$ depends on the objects of the subset space $\tilde{\sigma}$: $P(S_t) \coloneqq P(S_t|o_1, o_2, \dots, o_m)$ with $o_1, o_2, \dots, o_m \in \tilde{\sigma}$ and $S(S_t)$ is estimated through a loss analysis in which the adverse outcomes (human loss, asset loss, and environmental loss) associated with accidents, i.e. the states of consequence node, are converted and expressed in a common currency, such as monetary value, to provide a coherent view of the totality of loss associated with the situation (Naderpour and Lu 2012a). It is also assumed that the severity of situations remains constant during the study. Twenty five rules in terms of linguistic variables elicited form operators are showed in Table 1. Fuzzy logic is used to mathematically emulate human reasoning and allow an operator to express his/her knowledge in the form of related imprecise inputs and outputs in terms of linguistic variables. The results are obtained by using a fuzzy logic system where the membership functions illustrated in Figure 3 and Mamdani's fuzzy logic operations are utilized to generate the output.

Table 1: Operators' rules for assessing the risk of situations.

	Severity				
Probability	Negligible	Minor	Medium	Major	Catastrophic
Very likely	Tolerable not acceptable	Tolerable not acceptable	Not acceptable	Not acceptable	Not acceptable
Likely	Tolerable acceptable	Tolerable not acceptable	Tolerable not acceptable	Not acceptable	Not acceptable
Even	Acceptable	Tolerable acceptable	Tolerable not acceptable	Not acceptable	Not acceptable
Unlikely	Acceptable	Acceptable	Acceptable	Tolerable not acceptable	Tolerable not acceptable
Very Unlikely	Acceptable	Acceptable	Acceptable	Tolerable not acceptable	Tolerable not acceptable

By assigning the values of observable variables to the situational network, the posterior probabilities of objects and situations given this evidence, can be calculated. Consequently, the risk level of a situation will be updated. If the estimated risk of a situation is unacceptable, it is necessary to recover the situation. The situational network makes it possible to simulate the impact of recovery decisions on a situation.

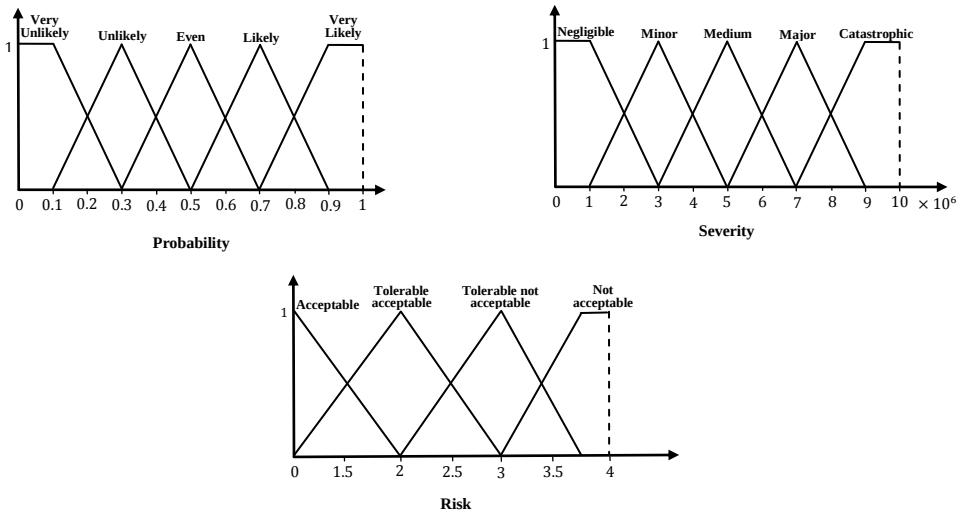

Figure 3: Membership functions of probability, severity, and risk.

3. Residue treater and timeline of events

A description of the residue treater process and the timeline of events are presented in the following sections.

3.1. Residue treater

Methomyl is a white, crystalline solid insecticide with a slight sulfurous odor. Methomyl dust is combustible and can form an explosive mixture when dispersed in air, and can also disrupt the functions of the central and peripheral nervous system. Methyl isocyanate, or MIC, is one of the key chemicals used to make methomyl. It is highly reactive with water and must be stored in stainless steel or glass containers

at temperatures below 40°C to prevent a highly exothermic reaction. The methomyl production process begins by reacting aldoxime with chlorine to make chloroacetaldoxime, which reacts with sodium methyl mercaptide to produce methylthioacetaldoxime (MSAO). MSAO reacts with methyl isocyanate to produce methomyl (Figure 4). Excess MIC is removed from the methomyl-solvent solution and the solution is then pumped to the crystallizers where an anti-solvent is added to cause the methomyl to crystallize. Finally, the crystallized methomyl is separated from the solvents in the centrifuges and the methomyl cake is removed, dried, cooled, packaged in drums, and moved to the warehouse. The residual liquid from the centrifuges contains very small quantities of methomyl and other impurities (CSB 2011).

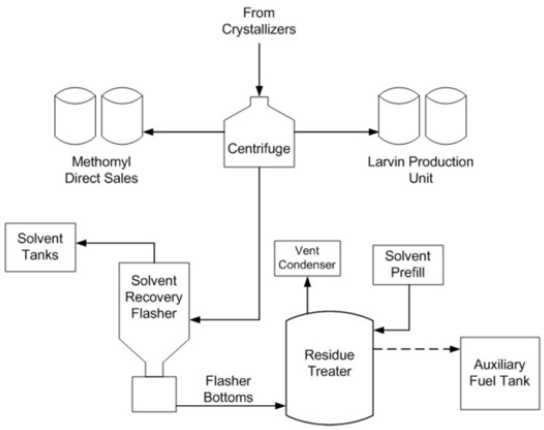

Figure 4: Methomyl synthesis process flow (CSB 2011).

Distillation separates the solvents in solvent recovery flashers and recycles the solvents to the start of the process (Figure 5). The unvaporized solvents and impurities, including up to 22 percent methomyl, accumulate in the bottom of the flasher. The flammable liquids can be used as fuel in the facility steam boilers, but before this flammable waste liquid (called "flasher bottoms") can be pumped to an auxiliary fuel tank, the methomyl concentration has to be reduced to not more than 0.5 percent by weight for environmental and processing considerations (CSB 2011).

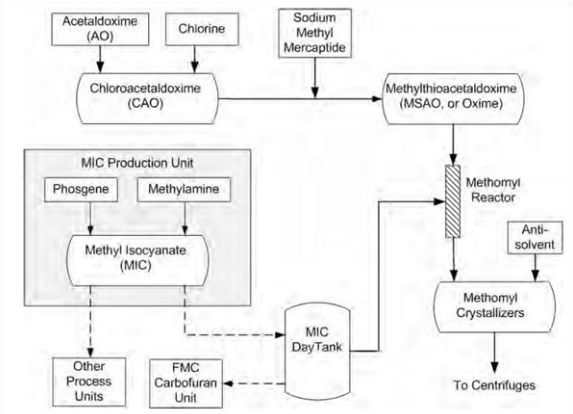

Figure 5: Methomyl centrifuge and solvent recovery process flow (CSB 2011).

The residue treater, which is a 4500-gallon pressure vessel with a maximum allowable operating pressure of 50 psig, is used to dilute the incoming flasher bottoms, and is designed to operate at a high sufficiently high temperature, and with sufficient residence time, to decompose the methomyl in the flasher bottoms stream to below 0.5 percent by weight (Figure 6). The solvent and residual waste material is transferred to the auxiliary fuel tank for use as a fuel in the facility steam boiler. Vapor generated in the methomyl decomposition reaction exits through the vent condenser to the process vent system where toxic and flammable vapor is removed (CSB 2011).

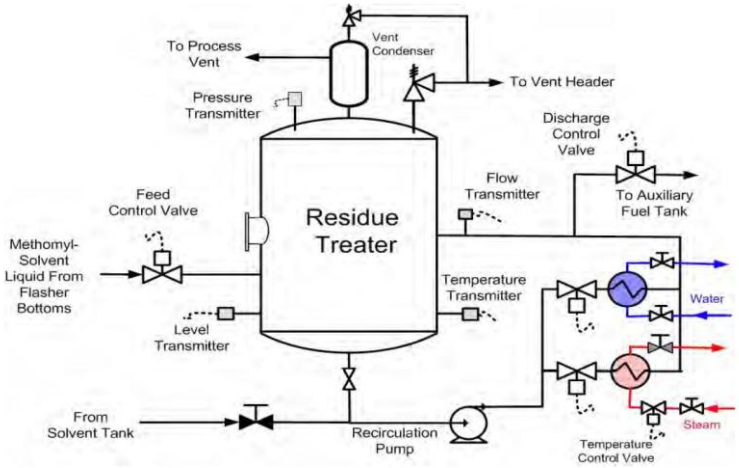

Figure 6: Residue treater piping system layout (CSB 2011).

3.2. Events timeline

At approximately 23:33 on 28 August 2008, a runaway chemical reaction caused a violent explosion at a manufacturing facility located in Institute, West Virginia. The accident occurred during the first methomyl restart after an extended outage to install a new process control system and a stainless steel

pressure vessel. During normal operations, dissolved methomyl and other waste chemicals are fed into the preheated residue treater, which is partially filled with solvent. The methomyl safely decomposes inside the residue treater to a concentration of less than 0.5 percent by weight. On the night of the incident, methomyl-containing solvent was pumped into the residue treater before the vessel was pre-filled with clean solvent and heated to the required minimum operating temperature specified in the operating procedure. The emergency vent system was overwhelmed by the evolving gas from the runaway decomposition reaction of the methomyl, and the residue treater exploded violently (CSB 2011).

On the day of the accident at approximately 4:00, the outside operator manually opened the residue treater feed control valve and began feeding flasher bottoms into the almost empty vessel. With a low flow rate of about 1.5 gallons per minute, more than 24 hours would be required to fill the residue treater to 50 percent, the normal operating level. The outside operator started the recirculation pump at 18:15, as directed by the board operator. The residue treater liquid level was approximately 30 percent (1,300 gallons), the temperature ranged between 60°C and 65°C, still significantly below the critical decomposition temperature of 135°C, and the pressure remained constant at 22 psig. At 18:38, the temperature began to steadily rise at a rate of about 0.6 degrees per minute (Figure 7). At 22:21, the level was 51 percent when the recirculation flow suddenly dropped to zero. In less than three minutes, the temperature reached 141°C, rapidly approaching the safe operating limit of 155°C, and was climbing at the rate of more than two degrees per minute. At approximately 22:25, the residue treater high pressure alarm sounded at the work station. The board operator immediately observed that the residue treater pressure was above the maximum operating pressure and climbing rapidly but did not understand what was wrong. He therefore asked two outside operators to investigate why the pressure in the residue treater was unexpectedly increasing. About 10 minutes later, as the two operators approached the newly installed residue treater, it suddenly and violently ruptured (CSB 2011).

Approximately 2,200 gallons of flammable solvents and toxic insecticide residues sprayed onto the road and into the unit and immediately erupted in flames as severed electrical cables, or sparks from steel debris striking the concrete, ignited the solvent vapor. Debris was thrown in all directions, to a distance of some hundreds of feet. The blast over-pressure moderately damaged the unit control building and other nearby structures. Fortunately, a steel blanket protected a 6,700-gallon methyl isocyanate storage tank from flying debris and from the radiant heat generated by the nearby fires that burned for more than four

hours. One employee died at the scene from blunt force trauma and thermal burn injuries, and the second employee died 41 days later. Residences, businesses, and vehicles as far as seven miles from the explosion epicenter sustained over-pressure damage that included minor structural and exterior damage, and broken windows. Acrid, dense smoke billowed from the fire into the calm night air for many hours. Smoke drifted over nearby roads, forcing many road closures and disrupting highway traffic. Methomyl and solvents were released from the residue treater, and solvents and other toxic chemicals, including flammable and toxic MIC, were released from ruptured unit piping. The released chemicals rapidly ignited, producing undetermined combustion products (CSB 2011).

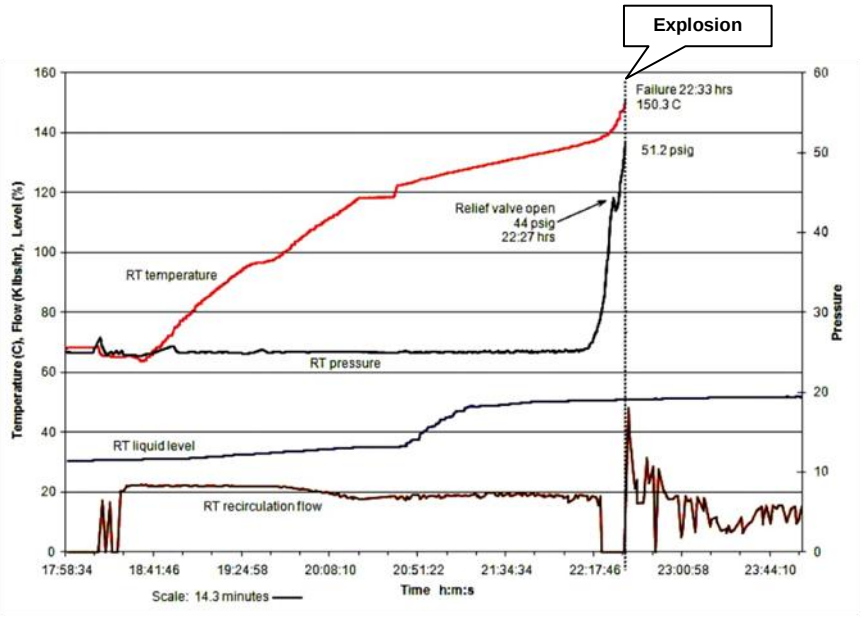

Figure 7: Residue treater process variables before the explosion (CSB 2011).

4. Application

The explosion happened during startup; therefore the startup operation is considered for modeling.

4.1. Situational network development

By consulting a chemical expert who has eight years' experience in the oil industry and analyzing the accident investigation report, several possible abnormal situations in the residue treater environment are determined, as follows:

- Situation of vent condenser failure (SVC)
- Situation of abnormal liquid level (SAL)
- Situation of abnormal recirculation (SAR)

- Situation of high pressure (SHP)
- Situation of abnormal temperature (SAT)
- Situation of high concentration of methomyl (SHC)
- Situation of runaway reaction (SRR)

In the following sections, the situations are modeled based on the proposed methodology. The CPTs of focal objects, which delegate the situations are presented, and the CPTs of other objects are omitted. The majority of failure probabilities are determined based on data recorded by OREDA (2002), and the use of expert judgment in a limited number of places. The focal objects are colored blue, other objects are shown in yellow and observable variables are colored green. It is worth noting that the states of observable variables are determined by using a fuzzy portioning method to improve traditional discretization methods (Naderpour *et al.* 2013).

4.1.1. Situation of vent condenser failure (SVC)

A vent condenser is a plume abatement device which cools and condenses the vented steam by cold plant water. At the residue treater, vapor generated in the methomyl decomposition reaction exits through the vent condenser to the process vent system where toxic and flammable vapor are removed. Any problem at the vent condenser will lead to an imbalance in the crystallizer solvent ratios and excess MSAO in the flasher bottoms. The objects, model, and CPT of SVC are presented in Table 2, Figure 8, and Table 3, respectively.

Table 2: SVC objects and symbols.

Objects	Symbol	Failure Probability
Loss of chilled cooling water supply	LCW	3.66E-05
Cooling water isolation valve is inadvertently closed	CWC	2.00E-02
Cooling water isolation valve is plugged	CWP	6.91E-03

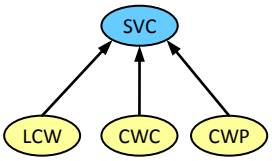

Figure 8: SVC model.

Table 3: CPT of P(SVC| LCW, CWC, CWP).

Variables	States and probabilities							
LCW	Failure				Success			
CWC	Failure		Success		Failure		Success	
CWP	Failure	Success	Failure	Success	Failure	Success	Failure	Success
Hazardous	1	1	1	1	1	1	1	0
Safe	0	0	0	0	0	0	0	1

4.1.2. Situation of abnormal liquid level (SAL)

The startup sequence requires the board operator, with the assistance of an outside operator, to manually pre-fill the residue treater with solvent to the minimum level of about 30 percent and to start the pump and achieve steady state recirculation. This is essential for safe, controlled methomyl decomposition, and starting routine operation, i.e. incoming flasher bottoms in the solvent at a lower level will increase the methomyl concentrate. The objects, model, and CPT of SAL are presented in Table 4, Figure 9, and Table 5, respectively. A level transmitter provides the residue treater liquid level (L), so SAL can be inferred by this variable. The value range of the liquid level variable is divided into three fuzzy states: Low, Normal and High. The membership function of L is determined and illustrated as follows:

$$\mu_{L(L)}(x) = \begin{cases} 1 & x \le 25 \\ (30 - x)/5 & 25 < x \le 30 \end{cases} \quad (9)$$

$$\mu_{L(N)}(x) = \begin{cases} (x - 25)/5 & 25 \le x < 30 \\ (35 - x)/5 & 30 \le x < 35 \end{cases} \quad (10)$$

$$\mu_{L(H)}(x) = \begin{cases} (x - 30)/5 & 30 \le x < 35 \\ 1 & x \ge 35 \end{cases} \quad (11)$$

Table 4: SAL objects and symbols.

Objects	Symbol	Failure Probability
Level transmitter	LT	1.40E-04
Manual level control	MLC	OR gate
Manual feed valve	MFV	1.40E-01
Manual discharge valve	MDV	1.40E-01
Failure of outside operator in operating manual valves	FOL	2.70E-01

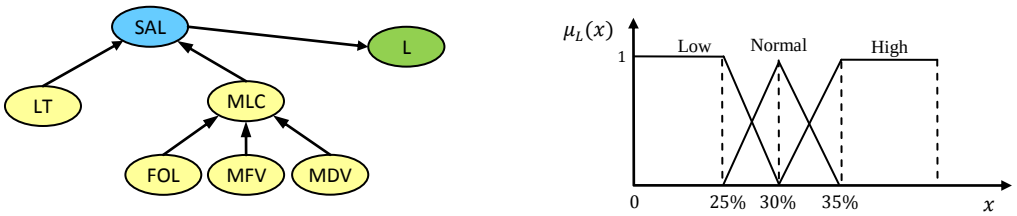

Figure 9: SAL model and membership function of liquid level.

Table 5: CPT of P(SAL| MLC, LT).

Variables	States and probabilities			
MLC	Failure		Success	
LT	Failure	Success	Failure	Success
Hazardous	1	1	1	0
Safe	0	0	0	1

4.1.3. Situation of abnormal recirculation (SAR)

The residue treater recirculation system is used to heat the solvent at the beginning of a new production run, mix the incoming flasher bottoms in the partially filled vessel, and remove excess heat generated by the exothermic decomposition of the methomyl inside the vessel. During startup, the control system modulates the recirculation and steam flows through the heater. When the liquid temperature increases to the set-point limit, the control system closes the steam flow valve, and changes the position of the circulation valves to redirect the recirculation flow from the heater to the cooler. The objects, model, and CPT of SHL are presented in Table 6, Figure 10, and Table 7, respectively. A pump provides a steady state recirculation, and a flow transmitter measures the flow of liquid through the recirculation pipeline. The measurement is converted from electrical signals and sent to the DCS by the flow transmitter. This allows operators to visualize the amount of liquid being transferred through the heating cycle during startup. The value range of the recirculation flow (F) is divided into three fuzzy states, Very Low, Low, and Normal, as shown in Figure 10, and the membership function of F is determined as follows:

$$\mu_{F(VL)}(x) = \begin{cases} 1 & x \leq 10 \\ (20 - x)/10 & 10 < x \leq 20 \end{cases} \quad (12)$$

$$\mu_{F(L)}(x) = \begin{cases} (x - 10)/10 & 10 \leq x < 20 \\ 1 & 20 \leq x < 40 \\ (60 - x)/20 & 40 \leq x < 60 \end{cases} \quad (13)$$

$$\mu_{F(N)}(x) = \begin{cases} (x - 40)/20 & 40 \leq x < 60 \\ 1 & x \geq 60 \end{cases} \quad (14)$$

Table 6: SAR objects and symbols.

Objects	Symbol	Failure Probability
Flow transmitter	FT	7.13E-06
Recirculation pump	RP	4.00E-02
Temperature sensor in recirculation	TS	4.00E-02
Automatic steam valve	ASV	8.68E-06
Automatic heater system	AHS	OR gate

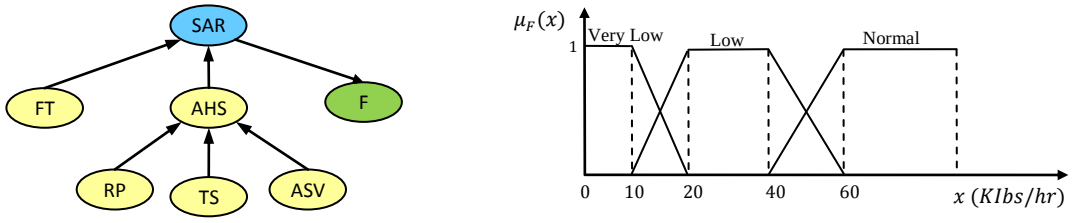

Figure 10: SAR model and membership function of recirculation flow.

Table 7: CPT of P(SAR| FT, AHS).

Variables	States and probabilities			
FT	Failure		Success	
AHS	Failure	Success	Failure	Success
Hazardous	1	1	1	0
Safe	0	0	0	1

4.1.4. Situation of high pressure (SHP)

The residue treater includes a pressure vessel with a maximum allowable operating pressure of 50 psig and an automatic pressure control. The vent condenser at the top of the residue treater, which is prone to blockages during unit operation, passes the gases produced by the methomyl decomposition reaction to the flare system. The gas flow carries trace amounts of solid material into the vent system, which are deposited on the surface of the pipe, and over time, accumulated deposits can choke the flow and cause the residue treater pressure to climb. The objects, model, and CPT of SHP are presented in Table 8, Figure 11, and Table 9 respectively. The situation is connected to node P because it can be inferred from the pressure variable (P). The residue treater is normally operated at 20 psig. The pressure value range is divided into three fuzzy states, Normal, High, and Very High, and the membership function of P is determined as follows, and as shown in Figure 11:

$$\mu_{P(N)}(x) = \begin{cases} 1 & x \leq 20 \\ (25 - x)/5 & 20 < x \leq 25 \end{cases} \quad (15)$$

$$\mu_{P(H)}(x) = \begin{cases} (x - 20)/5 & 20 \leq x < 25 \\ (30 - x)/5 & 25 \leq x \leq 30 \end{cases} \quad (16)$$

$$\mu_{P(VH)}(x) = \begin{cases} (x - 25)/5 & 25 \leq x < 30 \\ 1 & x \geq 30 \end{cases} \quad (17)$$

Table 8: SHP objects and symbols.

Objects	Symbol	Failure Probability
Pressure transmitter	PT	1.64E-01
Automatic relief valve (mechanical failure)	ARV	3.40E-01
Automatic pressure control	APC	OR gate
Failure of outside operator in operating manual valve	FOP	2.70E-01
Manual relief valve	MRV	1.39E-01
Manual pressure control	MPC	OR gate
High pressure protection system	HPP	AND gate
Accumulating deposits at vent condenser piping	AD	4.95E-06
Situation of vent condenser failure	SVC	NA
Inadequate ventilation	IV	OR gate

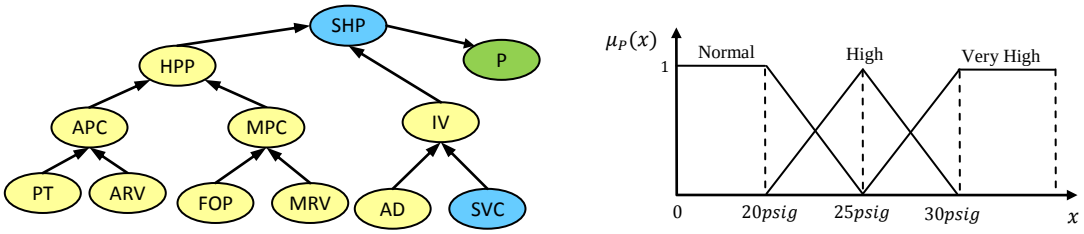

Figure 11: SHP model and membership function of pressure.

Table 9: CPT of P(SHP| HPP, IV).

Variables	**States and probabilities**			
HPP	Failure		Success	
IV	Failure	Success	Failure	Success
Hazardous	1	0	0	0
Safe	0	1	1	1

4.1.5. Situation of abnormal temperature (SAT)

A minimum temperature interlock prevents the feed control valve from opening until the minimum temperature of the residue treater contents are at, or above, the set-point. During startup, an automatic temperature control system monitors the bulk liquid temperature inside the vessel. Steam flows are used to heat the solvent. At normal operating conditions, the temperature of the flasher bottoms liquid is kept at about 80°C to prevent uncontrolled auto-decomposition of the more highly concentrated methomyl. The contents of the residue treater are maintained at approximately 135°C, a temperature that ensures that the incoming methomyl will quickly decompose to avoid accumulation to an unsafe concentration inside the residue treater. The objects, model, and CPT of SAT are presented in Table 10, Figure 12, and Table 11, respectively. A temperature transmitter provides the residue treater temperature (T) that is used for inferring SAT. The temperature value range is divided into three fuzzy states, Low, Normal, and High, as shown in Figure 12, and the membership function of T is determined as follows:

$$\mu_{T(L)}(x) = \begin{cases} 1 & x \leq 130 \\ (135 - x)/5 & 130 < x \leq 135 \end{cases} \quad (18)$$

$$\mu_{T(N)}(x) = \begin{cases} (x - 130)/5 & 130 < x \leq 135 \\ (140 - x)/5 & 135 < x \leq 140 \end{cases} \quad (19)$$

$$\mu_{T(H)}(x) = \begin{cases} (x - 135)/5 & 135 \leq x < 140 \\ 1 & x \geq 140 \end{cases} \quad (20)$$

Table 10: SAT objects and symbols.

Objects	Symbol	Failure Probability
Temperature transmitter	TT	6.84E-06
Situation of abnormal recirculation	SAR	NA
Automatic temperature control	ATC	OR gate
Failure of outside operator to operate steam valve	FOT	1.00E-01
Manual steam valve	MSV	1.39E-06
Manual temperature control	MTC	OR gate

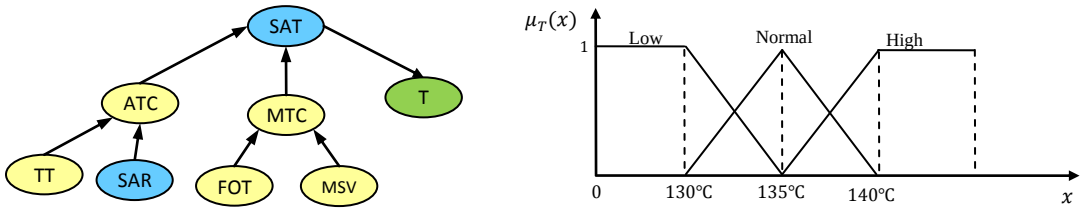

Figure 12: SAT model and membership function of temperature.

Table 11: CPT of P(SAT| ATC, MTC).

Variables	States and probabilities			
ATC	Failure		Success	
MTC	Failure	Success	Failure	Success
Hazardous	1	0	0	0
Safe	0	1	1	1

4.1.6. Situation of high concentration of methomyl (SHC)

The methomyl safely decomposes inside the residue treater to a concentration of less than 0.5 percent by weight. If the tank is allowed to cool below 130°C for any reason, it must be sampled before being heated up again. In addition, if the tank has a liquid level lower than 30 percent, the concentration of methomyl will increase when the flasher bottoms are introduced into residue treater. The objects, model, and CPT of SHC are presented in Table 12, Figure 13, and Table 13, respectively.

Table 12: SHC objects and symbols.

Objects	Symbol	Failure Probability
Situation of abnormal liquid level	SAL	NA
Failure of outside operator to understand liquid level	FON	1.00E-02
High concentration of methomyl because of low liquid level	HCL	AND gate
Situation of abnormal temperature	SAT	NA
Manual concentration control	MCC	OR gate
Failure of outside operator in sampling	FOS	2.00E-01
Failure of laboratory in testing the concentration of methomyl	FLN	1.00E-02
High concentration of methomyl because of low temperature	HCT	AND gate

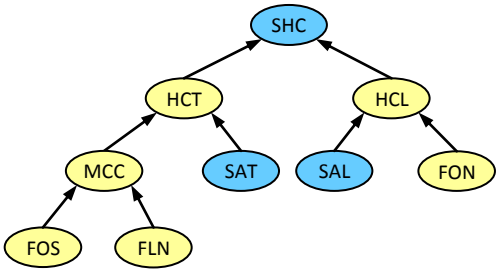

Figure 13: SHC model.

Table 13: CPT of P(SHC| HCT, HCL).

Variables	**States and probabilities**			
HCT	Failure		Success	
HCL	Failure	Success	Failure	Success
Hazardous	1	1	1	0
Safe	0	0	0	1

4.1.7. Situation of runaway reaction (SRR)

A runaway reaction is a chemical reaction over which control has been lost. The reaction speed continues to accelerate until the reaction either runs out of reactants or the vessel containing it over-pressurizes and containment is lost. The temporal arcs point to the SRR situation because it is assumed that the situation is formed after a time interval. The interpretation is that the runaway reaction occurs when a high concentration of methomyl exists for a few minutes inside the vessel and a high pressure situation exists in the environment. The objects, model, and CPT of SRR are presented in Table 14, Figure 14, and Table 15, respectively.

Table 14: SRR objects and symbols.

Objects	**Symbol**
Situation of high pressure	SHP
Situation of high concentration of methomyl	SHC

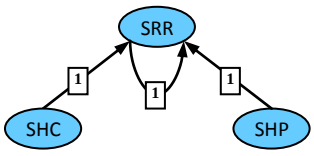

Figure 14: SRR model.

Table 15: CPT of P(SRR| SHC, SHP, SRR).

Variables	**States and probabilities**							
SHC	Hazardous				Safe			
SHP	Hazardous		Safe		Hazardous		Safe	
SRR	Hazardous	Safe	Hazardous	Safe	Hazardous	Safe	Hazardous	Safe
Hazardous	1	0.99	0.05	0.05	0.4	0.05	0.05	0
Safe	0	0.01	0.95	0.95	0.6	0.95	0.95	1

4.1.8. Situational network

The environment has a continuous air monitor system, which is located in and around the production unit, with 16 stationary sample points to detect fugitive leaks from process equipment. It detects concentrations of airborne chemical contaminants and alerts facility occupants if air concentration exceeds safe levels (1.0 ppm). In addition, a fire alarm and several fire cannons are located in the environment to reduce damage if a fire occurs. The air monitor system, alarm, and fire cannons are considered to be safety barriers, as shown in Table 16. The probability of the existence of spark is also estimated in this table.

Table 16: Safety barriers and chance of spark.

Objects	Symbol	Failure Probability
Air monitor system	AM	0.18E-06
Fire alarm	FA	1.30E-03
Fire cannon	FC	4.00E-01
Spark	SP	1.00E-01

The SRR can have results that range from the boiling over of the reaction mass to large increases in temperature and pressure that lead to an explosion. Such violent reactions can cause blast and missile damage. If flammable materials are released, fire or secondary explosion may result. Hot liquids and toxic materials may contaminate the workplace or generate a toxic cloud that may spread off-site. There can be serious risk of injury, even death, to plant operators, as well as the general public, and the local environment may be harmed. Therefore, SRR has a consequence node whose states are determined using consequence analysis, as described in the modeling process and presented in Table 17. The table contains the degree of loss corresponding to every state, which is evaluated by the expert.

Table 17: The states of SRR consequences node.

Consequence	Symbol	Loss ($)
Explosion with high death and high property damage	C1	1E+07
Fire with high death and moderate property damage	C2	7E+06
Fire with low death and high property damage	C3	5E+06
Fire with low death and moderate property damage	C4	4E+06
Ruptured vessel with vapor cloud with possibility of ignition	C5	3E+06
Safe evacuation	C6	1E+06
Safe state	C7	0E+00

Note: the safe state indicates the safe state of SRR.

For other situations, the resultant situation is considered to be a consequence of the occurrence. The degree of loss in these situations is also calculated and summarized in Table 18. A situational network for the residue treater is developed and illustrated in Figure 15.

Table 18: Loss of situations.

Situation	Consequence of occurrence	Loss ($)
SAR	SLT	1E+03
SLT	SHC	1E+04
SLL	SHC	1E+04
SHC	SRR	3E+06
SVC	SHP	1E+03
SHP	SRR	3E+06

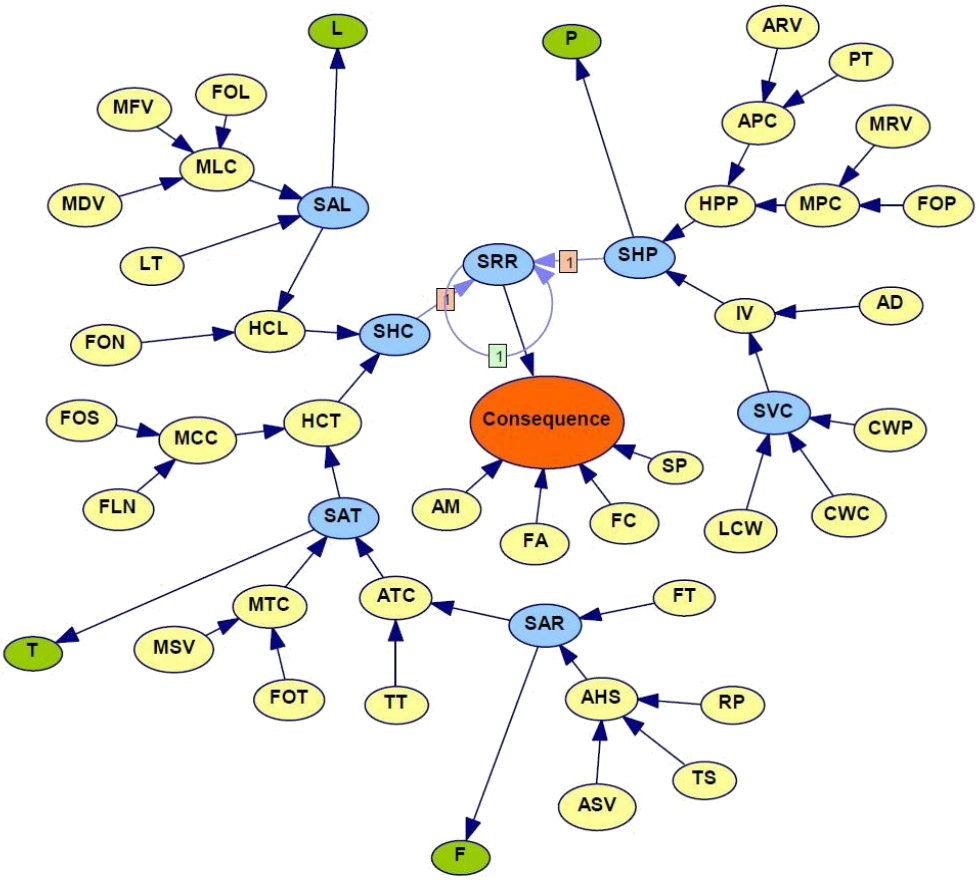

Figure 15: The situational network.

4.1.9. Situational network evaluation

Application of the sensitivity to findings shows that the query variable, SRR, in the absence of other evidence, is most sensitive to SHP, followed by observable variable P. This is what the experts expected because SRR results if methomyl is allowed to accumulate in the residue treater and the pressure relief system is not working properly. When findings for observable variable P (i.e. P=High) are entered into the network, the sensitivity measures and the ranking of variables are changed. With this evidence, SRR is most sensitive to SHC and SAL, followed by observable variable L. Alternatively, when P=High and L=High are entered into the network, some of the remaining variables become more influential. These observations agreed with the experts understanding of the situational network.

Sensitivity to parameters was analyzed in the CTPs of observable variables which were determined by the experts. For instance, scenario S=(SRR, Hazardous, E={SHP=Hazardous, T=High}) was investigated in which the hypothesis under consideration is SRR=Hazardous, while the parameter in focus is *P*(T=High| SAT=Hazardous). Therefore, the sensitivity function $f(t)$ was defined as follows:

$$f(t) = P(SRR = \ Hazardous \mid SHP = Hazardous, T = High) = \frac{\alpha t+\beta}{\gamma t+\delta} \quad (21)$$

The coefficients of denominator and numerator functions were determined separately. Both functions are linear in the parameter *t*. Thus, the coefficients of each function were determined by propagating evidence for two different parameter values. The sensitivity function resulted as follows when t_0=0.1 and t_1=0.2 were used to propagate evidence:

$$f(t) = \frac{6.31t+0.0001}{6.09t+1} \quad (22)$$

The graph of the sensitivity function $f(t)$ for all possible values of *t*, i.e. values between zero and one, is plotted in Figure 16. As can be seen, the minimum value of the probability of the hypothesis is 0.0001 for *t*=0, while the maximum value of the probability of the hypothesis is 0.887 for *t*=1. Clearly, the posterior probability of the hypothesis is more sensitive to variations in the parameter value when the initial parameter value is in the range from 0 to, say, 0.5 than when the initial parameter is in the range from 0.5 to 1.

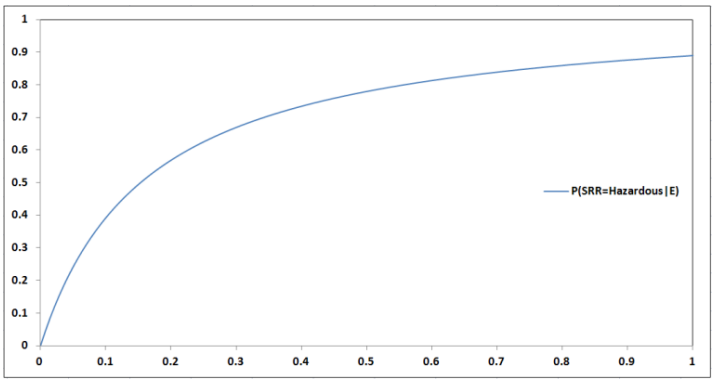

Figure 16: The graph of the sensitivity function *f*(*t*)= *P*(SRR= Hazardous| E).

4.2. The Human-System Interface

A graphical user interface for the proposed situational network is developed that 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 (Brannon *et al.* 2009). Therefore, keeping operators in the loop of decision-making, taking action, and updating the related information are critical issues in designing support systems. This level corresponds to level 5 of automation, called decision support, proposed by Kaber and Endsley (2004). The human-system interface is shown in Figure 17. Because modeling of the situational network for the residue treater led to a complex model, object oriented BNs (OOBNs) were used in the development process. The system is set to trigger an alarm for every situation that has a risk level in excess of 2.5, i.e. tolerable not acceptable. In addition, mouse-clicking any situation in the interface opens a pop-up window that contains the related sub-network, including contributing objects, their failure probabilities, and the most probable explanation.

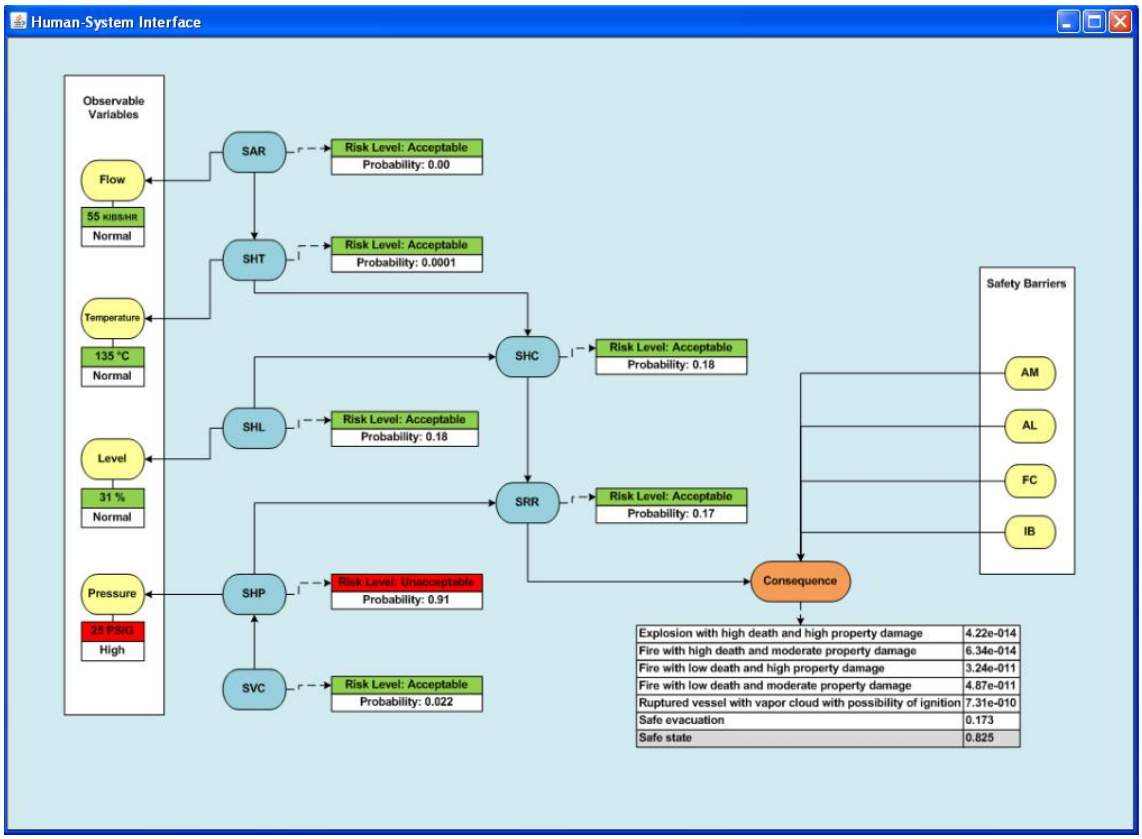

Figure 17: The human-system interface based on OOBNs.

4.3. Situational network analysis

The performance of the proposed methodology is investigated through the accident timeline events in the residue treater environment explained in Section 3.2, and by using the developed system.

4.3.1. Scenario

On the night of the accident, the critical startup safety prerequisites, pre-startup solvent fill and heat-up were omitted from the restart activities. Furthermore, the board operators bypassed the minimum operating temperature interlock that prevented adding methomyl into the residue treater, as some operators were accustomed to doing. At about 23:45 the board operator started to pre-fill the vessel with solvent and heat the content to achieve the required minimum operating temperature. At 04:00 on 28 August, the residue treater liquid level was approximately 15 percent, significantly below the critical required solvent level (30 percent), and the temperature was around 65°C, still significantly below 135°C, the critical decomposition temperature. The outside operator prematurely opened the residue treater feed control valve and began to feed flasher bottoms into the vessel to start a routine operation. To simplify the presentation of situational network performance, the last hour before the explosion is chosen, i.e. from 21:30 to 22:30 on 28 August. The trend of observable variables for the period of study is illustrated in Figure 18. At 21:30, the residue treater liquid level was approximately 50 percent, the temperature was 130°C raising steadily about 0.5 degree per minute, and the pressure was 22 psig. At 22:21, the level was 51 percent when the recirculation flow suddenly dropped to zero. In less than three minutes, the temperature reached 141°C, rapidly approaching 155°C, the safe operating limit, and climbed at the rate of more than two degrees per minute.

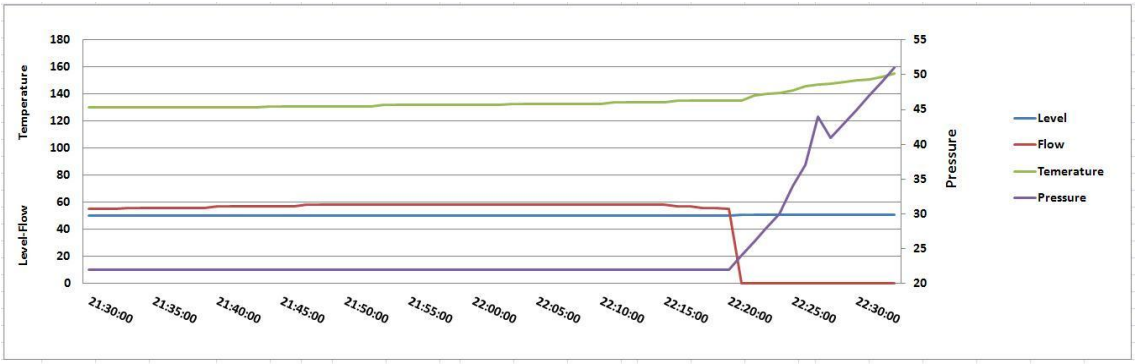

Figure 18: The trend of observable variables.

4.3.2. Results

The fuzzy partitioning values of observable variables based on the proposed membership functions are calculated and assigned to the situational network. The posterior probabilities of the situations are updated and the risk level of each situation is projected, as shown in Figure 19. As can be seen, the estimated risk level of SAT is 2.95 (tolerable not acceptable) at the beginning of the period because the temperature was

below the safety set-point. It then becomes tolerable not acceptable from 22:15 as the temperature deviates from the safety set-point. The risk level of SHP is acceptable, i.e. 1.65, during the period of study until 22:25 as the pressure increases and deviates the safety set-point. The risk level of SHC is unacceptable for the whole period under study because the liquid level of the solvent was below the safety set-point (30 percent), i.e. the risk level of SAL is unacceptable, and the operator opened the feed valve without considering this fact.

As can be seen, the risk level of SRR is acceptable, i.e. 1.35, until 22:24, when it increases to 3.03, which is unacceptable, immediately after appearing to be an SHP.

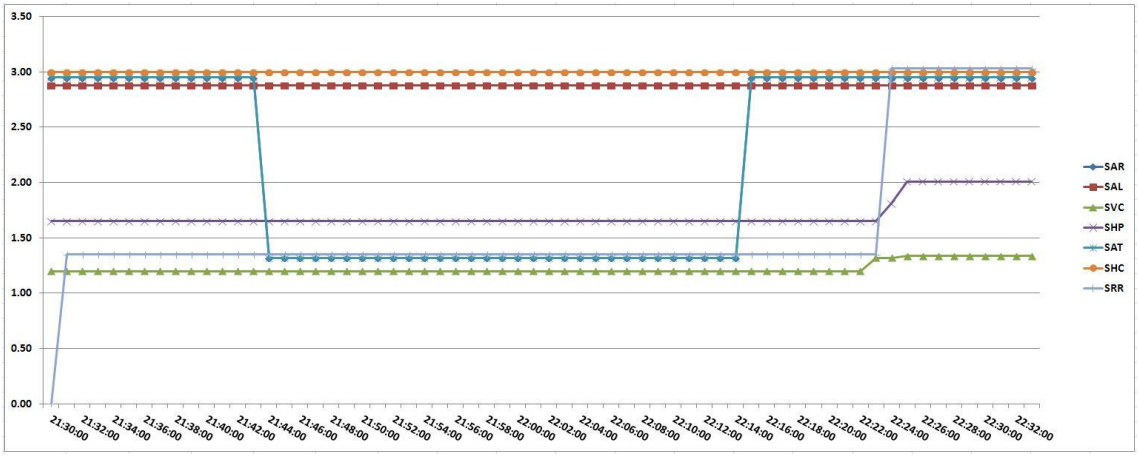

Figure 19: Projection of situation risk levels.

At 22:21 when the risk level of SAR rises, the situational network shows that the most probable explanation is the failure of the recirculation pump (RP) with a probability of 0.5. At 22:25 when the risk level of SAR increases, the situational network shows that the most probable explanation is the failure of the high pressure protection system (HPP) and the failure of the automatic relief valve. The system helps the operator to prevent accidents in abnormal situations, but it can also present the factors that contribute to the creation of an accident or a specific consequence. For instance, if at 22:33 a fire with low death and high property damage (C3) is reported, the posterior probability updating from this evidence shows that the closed cooling water isolation valve (CWC) causes inadequate ventilation, and consequently SHP in the residue treater which, with SHC, creates SRR.

5. Conclusion and future work

Situation awareness is likely to be at the root of many accidents in safety-critical systems where multiple goals must be pursued simultaneously, multiple tasks require the operator's attention, operator performance is under high stress, and negative consequences associated with poor performance are

anticipated. This paper has shown a methodology for developing and analyzing a situational network to support the SA for control room operators in the decision-making process when they are confronted by abnormal situations in safety-critical systems. The proposed methodology exploits the specific capabilities of Bayesian networks and fuzzy logic systems to simulate human thinking. In addition, the methodology uses risk indicators to determine when a situation is abnormal and also to show the investigation priority whenever it is necessary. As operators do not perform mathematical calculations while performing a situation assessment, the proposed methodology provides only an approximation of operator behavior in the situation assessment process. Therefore, the proposed methodology is expected to provide the most logical results and 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. The performance of the methodology was investigated in the residue treater environment, and an HSI considering the capabilities of OOBNs was also developed for the intended plant. As has been shown, it provides a useful graphical model that meets the requirements of a practical SA system. The Bayesian inference facilitates the inclusion of prior background knowledge and the updating of this knowledge when new information is available from the SCADA monitoring system.

In comparison with previous research works (Miao *et al.* 1997, Kim and Seong 2006), this study has some advantages. First, situations in our method might be inclusive, unlike previous studies where situations are exclusive. Second, unlike previous networks that only include indicators and sensors and are unable to determine the cause of abnormal situations, our method enables the most probable cause of abnormal situations to be obtained from the situation models, thus assisting operators to understand situations. Third, the 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 first direction for future study is to evaluate the performance of the proposed HSI based on a SA measurement. As in many safety-critical systems, the safety of the system is supervised by control room operators and outside operators who are members of a team, so 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 the Australian Research Council (ARC) under Discovery Project DP140101366.

References

Adams, M.J., Tenney, Y.J., Pew, R.W., 1995. Situation awareness and the cognitive management of complex systems. Human Factors 37 (1), 85-104.

Baader, F., Bauer, A., Baumgartner, P., Cregan, A., Gabaldon, A., Ji, K., Lee, K., Rajaratnam, D., Schwitter, R., 2009. A novel architecture for situation awareness systems. In: Proceedings of the 18th International Conference on Automated Reasoning with Analytic Tableaux and Related Methods, pp. 77-92.

Bednarski, M., Cholewa, W., Frid, W., 2004. Identification of sensitivities in Bayesian networks. Engineering Applications of Artificial Intelligence 17 (4), 327-335.

Bedny, G., Meister, D., 1999. Theory of activity and situation awareness. International Journal of Cognitive Ergonomics 3 (1), 63-72.

Brannon, N.G., Seiffertt, J.E., Draelos, T.J., Wunsch Ii, D.C., 2009. Coordinated machine learning and decision support for situation awareness. Neural Networks 22 (3), 316-325.

CCPS, 1989. Guidelines for process equipment reliability data with data tables Center for Chemical Process Safety of the American Institute of Chemical Engineers.

CSB, 2011. Pesticide chemical runaway reaction pressure vessel explosion. Washington, DC.

Dekker, S.W.A., 2013. On the epistemology and ethics of communicating a cartesian consciousness. Safety Science 56, 96-99.

Endsley, M.R., 1995. Toward a theory of situation awareness in dynamic systems. Human Factors: The Journal of the Human Factors and Ergonomics Society 37 (1), 32-64.

Endsley, M.R., 2006. Situation awareness. In: Salvendy, G. ed. Handbook of human factors and ergonomics. John Wiley and Sons, pp. 528-542.

Fischer, Y., Bauer, A., Beyerer, J., Year. A conceptual framework for automatic situation assessment. In: Proceedings of the 2011 IEEE First International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), pp. 234-239.

Fischer, Y., Beyerer, J., Year. Defining dynamic Bayesian networks for probabilistic situation assessment. In: Proceedings of the 15th International Conference on Information Fusion (FUSION), pp. 888-895.

Ghanea-Hercock, R., Gelenbe, E., Jennings, N.R., Smith, O., Allsopp, D.N., Healing, A., Duman, H., Sparks, S., Karunatillake, N.C., Vytelingum, P., 2007. Hyperion-next-generation battlespace information services. The Computer Journal 50 (6), 632-645.

Jones, R.E.T., Connors, E.S., Endsley, M.R., Year. A framework for representing agent and human situation awareness. In: Proceedings of the 2011 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), pp. 226-233.

Juricek, B.C., Seborg, D.E., Larimore, W.E., 2001. Predictive monitoring for abnormal situation management. Journal of Process Control 11 (2), 111-128.

Kaber, D.B., Endsley, M.R., 2004. The effects of level of automation and adaptive automation on human performance, situation awareness and workload in a dynamic control task. Theoretical Issues in Ergonomics Science 5 (2), 113-153.

Khakzad, N., Khan, F., Amyotte, P., 2012. Dynamic safety analysis of process systems by mapping bow-tie into Bayesian network. Process Safety and Environmental Protection 91 (1-2), 46-53.

Kim, M.C., Seong, P.H., 2006. An analytic model for situation assessment of nuclear power plant operators based on Bayesian inference. Reliability Engineering & System Safety 91 (3), 270-282.

Kim, Y.J., Hoffmann, C.M., 2003. Enhanced battlefield visualization for situation awareness. Computers & Graphics 27 (6), 873-885.

Klashner, R., Sabet, S., 2007. A dss design model for complex problems: Lessons from mission critical infrastructure. Decision Support Systems 43 (3), 990-1013.

675 Korb, K.B., Nicholson, A.E., 2003. Bayesian artificial intelligence Taylor & Francis.

676 Laskey, K.B., 1995. Sensitivity analysis for probability assessments in Bayesian networks. IEEE Transactions on Systems, Man and
677 Cybernetics 25 (6), 901-909.

678 Miao, A.X., Zacharias, G.L., Shih-Ping, K., 1997. A computational situation assessment model for nuclear power plant operations.
679 IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans 27 (6), 728-742.

680 Murphy, K.P., 2002. Dynamic Bayesian networks: Representation, inference and learning. PhD. University of California.

681 Naderpour, M., Lu, J., 2012a. A fuzzy dual expert system for managing situation awareness in a safety supervisory system. 21st
682 IEEE International Conference on Fuzzy Systems. Brisbane-Australia, pp. 715-721.

683 Naderpour, M., Lu, J., 2012b. Supporting situation awareness using neural network and expert system. 10th International FLINS
684 Conference on Uncertainty Modeling in Knowledge Engineering and Decision Making. Istanbul-Turkey, pp. 993-998.

685 Naderpour, M., Lu, J., Zhang, G., 2013. A fuzzy dynamic Bayesian network-based situation assessment approach. 22nd IEEE
686 International Conference on Fuzzy Systems (FUZZ-IEEE). Hyderabad, India.

687 Naderpour, M., Lu, J., Zhang, G., 2014a. An intelligent situation awareness support system for safety-critical environments.
688 Decision Support Systems 59, 325-340.

689 Naderpour, M., Lu, J., Zhang, G., 2014b. A situation risk awareness approach for process systems safety. Safety Science 64, 173-
690 189.

691 Oreda, 2002. Offshore reliability data handbook SINTEF Industrial Management.

692 Pollino, C.A., Woodberry, O., Nicholson, A., Korb, K., Hart, B.T., 2007. Parameterisation and evaluation of a Bayesian network for
693 use in an ecological risk assessment. Environmental Modelling & Software 22 (8), 1140-1152.

694 Pridmore, J.L., 2007. Designing for the improvement of operator situation awareness in automation systems. PhD Auburn
695 University.

696 Qian, Y., Xu, L., Li, X., Lin, L., Kraslawski, A., 2008. Lubres: An expert system development and implementation for real-time
697 fault diagnosis of a lubricating oil refining process. Expert Systems with Applications 35 (3), 1252-1266.

698 Smart, P.R., Russell, A., Shadbolt, N.R., Carr, L.A., 2007. AKTIVESA: A technical demonstrator system for enhanced situation
699 awareness. The Computer Journal 50 (6), 703-716.

700 Sneddon, A., Mearns, K., Flin, R., 2013. Stress, fatigue, situation awareness and safety in offshore drilling crews. Safety Science 56
701 (0), 80-88.

702 Van Den Broek, A.C., Neef, R.M., Hanckmann, P., Van Gosliga, S.P., Van Halsema, D., Year. Improving maritime situational
703 awareness by fusing sensor information and intelligence. In: Proceedings of the 14th International Conference on Information
704 Fusion (FUSION), pp. 1-8.

705 Vincenzi, D.A., Mouloua, M., Hancock, P.A., 2004. Human performance, situation awareness and automation: Current research and
706 trends : Hpsaa ii L. Erlbaum Associates.

707 Yet, B., Bastani, K., Raharjo, H., Lifvergren, S., Marsh, W., Bergman, B., 2013. Decision support system for warfarin therapy
708 management using Bayesian networks. Decision Support Systems 55 (2), 488-498.

709

710