Intelligent Situation Awareness Support System for Safety-Critical Environments

Mohsen Naderpour

Ph.D. Thesis
This thesis is submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy.

University of Technology Sydney
Faculty of Engineering and Information Technology
March 2015

CERTIFICATE OF ORIGINAL AUTHORSHIP

I certify that the work in this thesis has not previously been submitted for a degree nor has it been submitted as part of requirements for a degree except as fully acknowledged within the text.

I also certify that the thesis has been written by me. Any help that I have received in my research work and the preparation of the thesis itself has been acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis.

Signature of Student: Production Note: Signature removed prior to publication.

Date: 27.03.2015

DEDICATION

To my darling wife for her passion and patience and to my beloved parents for their encouragement, that let my dreams came true.

ACKNOWLEDGEMENT

I would like to express my appreciation to Professor Jie Lu, who supervised this Ph.D. program, for all of her knowledgeable comments, precious support, right guidance at hard times, and great suggestions along the way. I want to thank Jie for her willingness that let my research follow my interests. I am also grateful to Associate Professor Guangquan Zhang, my co-supervisor, for his knowledgeable suggestions and valuable advice through my PhD study.

Looking back at my Ph.D., I see my wife, Fahimeh, truly shoulder to my shoulder during this journey. Thank you very much for being so supportive in all circumstances throughout the four years of this Ph.D., for understanding the stress I was subject to, for having sacrificed your time for me while you were doing your Ph.D., and for giving me the freedom to follow my scientific interests unconditionally. I could not have accomplished this without your constant love and support.

I would like to thank my parents, the first ones who taught me, for their encouragement and support despite the geographical distance. Pursuing my PhD was not possible without their love and assistance. I express my gratitude to all my friends and colleagues in the Decision Systems & e-Service Intelligence (DeSI) Laboratory for their help and valuable comments during my study.

I also appreciate the Faculty of Engineering and Information Technology and the Centre for Quantum Computation and Intelligent Systems (QCIS) at the University of Technology Sydney for conference registration and travel funds provided during this research. This research was also supported by the International Postgraduate Research Scholarship (IPRS) funded by the Australian government.

Last, but absolutely not least, a special thank you goes to Ms. Sue Felix and Ms. Barbara Munday for helping me to identify and correct grammar and syntax problems in my publications.

ABSTRACT

In today's safety-critical systems such as process and manufacturing plants, operators are often moved to a control room far away from the physical environment, and increasing amounts of information are passed to them via automated systems, they therefore need a greater level of support to control and maintain the facilities in a safe condition. This is especially important when operators confront abnormal situations in which the information flow is quite high and poor decisions may lead to serious consequences. Therefore, they 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, that is situation awareness (SA), has been found to be a crucial factor in improving performance and reducing error. However, existing system safety researches focus mainly on technical issues and often neglect SA.

This research reviews the role of SA in accidents of safety-critical environments and introduces a clear definition for abnormal situations based on risk indicators. It then relies on mental models that embody stored long-term knowledge about the systems, and develops an abnormal situations modelling (ASM) method, that exploits the specific capabilities of Bayesian networks (BNs). In this sense, it is assumed that the operator's mental model can be modelled using BNs as a representation of static cause–effect relationships between objects in the situation. Following this, the research 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. The SASS consists of five major components: (1) a knowledge–base that contains the abnormal situation models of the intended environment developed by the ASM method, (2) a situation data collection component that provides the current state of the observable variables based on online conditions and monitoring systems, (3) a situation assessment component that uses risk indicators and a fuzzy logic system to generate the assessment result, (4) a situation

recovery component that provides a basis for decision-making to reduce the risk level of situations to an acceptable level, and (5) a human-computer interface. The performance of the SASS is demonstrated by three cases investigated by the US Chemical Safety Board in which poor operators' SA has created industrial disasters in recent US history. The results of performance 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.

The SASS is partially evaluated by a sensitivity analysis, which is carried out to validate the BN-based situation models, and a multi-perspective evaluation approach is proposed based on SA measures to determine the degree to which the SASS improves not degrades the operator's SA. The approach consists of three SA metrics: the Situation Awareness Global Assessment Technique, the Situation Awareness Rating Technique, and the NASA Task Load Index. The first two metrics are used for direct objective and subjective measurement of SA, while the third is used to estimate the workload of operators. The approach is applied in a safety-critical environment, and ten operators participate in two 40-minute simulation trials using a virtual plant user interface, both with and without the support of the SASS. The results indicate that the SASS improves operators' SA, and specifically has benefits for SA levels 2 and 3. No significant correlations between the participants' SA scores have been found. In addition, it is concluded that the SASS reduces the workload of operators, although further investigations in different environments with a larger number of participants have been suggested.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

Chapter 1:

INTRODUCTION

1.1 BACKGROUND

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 (Ha & Seong 2009) 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 (Melchers 2001). 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 (Hsieh et al. 2012). Paradoxically, several researches show that the focus of most human-system studies is on the technical elements, and human factors are often neglected (Niu et al. 2013). 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 (Chen & Lee 2003). 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 (Power & Sharda 2007). Unlike model-driven and data-driven DSSs, cognitive DSSs have not been researched, albeit they have long been recognized as being worthy of consideration (Chen & Lee 2003). 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 (Niu et al. 2013). 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 (Endsley 1995b). 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 (Kaber & Endsley 1998).

For example, on 23 March 2005, at the Texas City, TX BP Amoco Refinery explosion, 15 workers were killed and 170 injured when a column was overfilled, overheated, and over-pressurized on start-up. A key problem identified in this catastrophic event was the difficulty experienced by the operator in maintaining an accurate awareness of the situation while monitoring a complex, fast moving environment (Pridmore 2007). Several other studies of accidents throughout many industries have found that loss of, or poor operator SA, was related to accidents classified as human error. For instance, loss of SA has been associated with 88% of major air carrier accidents that involved pilot errors and 58.6% of operational error in air traffic control operations (Endsley 1995a).

Based on above mentioned issues, the main objective of this research is to develop a cognition-driven DSS, called the situation awareness support system (SASS), to assist operators when they when they are confronted with abnormal situations in safety-critical environments.

1.2 RESEARCH PROBLEMS

This section explains main issues which significantly motivates this study and presents the research questions:

(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 (Endsley 2006; Endsley & Connors 2008; Papadopoulos & McDermid 2001). Therefore, to develop any new support system, two important aspects, namely addressing hazards that result from hardware failure and reducing human error through decision–making should be considered.

(2) Safety supervisory is one of those domains that the information flow is quite high, and poor decisions may lead to serious consequences. Therefore, operators are usually

stressed by quick and proper decision making in a short time. Most of operator support systems focus on the deviation of the process from an acceptable range of operation, the identification of operation faults (Qian et al. 2008) or the prediction of process variables (Juricek, Seborg & Larimore 2001) that will violate an emergency limit in the future. Therefore quantitative knowledge and hardware failures have been relied on significantly; however, when faults occur, human operators have to rely on their experience under working pressure to understand what is going on and to contribute a solution (Klashner & Sabet 2007). These problems also highlight the urgency of cognitive human factors in the development of operator support systems to lower workload, stress and consequent error rates of operators.

(3) Situation awareness, among human factors, has been found to be the most important prerequisite for decision-making (Endsley 1995b; Niu et al. 2013). Despite having its roots in aviation, it has been suggested that the concept is equally applicable to human supervisory control for land based industries. Several other studies of accidents throughout many industries have found that loss of, or poor operators' SA, was related to accidents classified as human error (Endsley 1995a). Due to the severity of the accidents that have occurred over the last ten years, SA has become the focus of research that aims to understand operator performance in critical, dynamic environments (Garland, Wise & Hopkin 1999). It is also argued that problems in human supervisory control may be due to poor SA (Stanton, Chambers & Piggott 2001), such as: 1) failure to detect critical cues regarding the state of the system; 2) failure to interpret the meaning of information perceived via Supervisory Control and Data Acquisition (SCADA) technology; 3) failure to understand individual task responsibilities and the responsibilities of others; 4) failure to communicate with other operators in the team; and 5) failure to communicate with other teams.

(4) 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, Bauer & Beyerer 2011; Jones, Connors & Endsley 2011).

Based on the above mentioned issues, the research questions of this study are determined as follows:

- **Research Question 1**: What should be the goal of a decision support system to assist operators in handling abnormal situations?
- **Research Question 2**: What are the requirements for such operator decision support system and how they can be achieved?
- **Research Question 3**: How could abnormal situations be defined and modelled in safety-critical environments?
- **Research Question 4**: How could a situation assessment method be developed and implemented in safety-critical environments?
- **Research Question 5**: What is a practical model of an operator decision support system to manage abnormal situations and what sub-systems should be included?
- **Research Question 6**: How could the proposed system be implemented in safety-critical environments?
- **Research Question 7**: How could the performance of the proposed system be evaluated in a dynamic and complex environment?

1.3 RESEARCH OBJECTIVES

This research has seven objectives based on the research problems, which are explained as follows:

Research Objective 1: The first research objective corresponding to research question 1 is to determine the goal of the decision support system that aims to assist operators in managing abnormal situations in safety-critical environments. Nowadays, maintaining complex and dynamic systems in safe conditions, i.e. keeping the risks below the acceptance criteria, is a critical challenge because situations change dynamically and every

decision has a significant social, economic and environmental impact on society. The key focus must be on keeping the human operator aware of the situation, showing the risk level of hazardous situations and providing a base to reduce risks until they reach a level that is As Low as Reasonably Practicable (ALARP). According to ALARP, it is necessary for operators and intending 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) (Melchers 2001).

Research Objective 2: The second research objective is to determine the requirements of the proposed operator DSS. This objective corresponds to research question 2. To determine the aspects of the situation that are important for an operator's SA, a cognitive methodology called the Goal-Directed Task Analysis (GDTA) is utilized. The elements of GDTA include goal, sub-goals, decisions, and the SA requirements. The GDTA hierarchy is not attached to a fixed timeline, and is thus able to represent the workflow experienced in many dynamic systems. The GDTA hierarchy is also independent of the technology being used to perform a task (i.e. it is not tied to how tasks are done with a given system, but to what information is really needed). The analysis is not only focused on what data people need, but on how the data is to be combined and integrated to support decision making and goal attainment.

Research Objective 3: Corresponding to research question 3, the third research objective is to define abnormal situations and propose a method for their modelling based on operators' mental models. Mental models refer to mechanisms whereby humans are able to generate descriptions of system purpose and explanations of system functioning (Endsley 2000b). Mental models embody stored long-term knowledge about the systems that can be called upon for interaction with the relevant system when needed. In this sense, the current research presents a novel abnormal situation definition and develops a new method that is able to model the operator's mental models using the capabilities of object oriented

Bayesian networks. Bayesian networks (BNs) are used as a representation of static cause–effect relationships between objects in abnormal situations.

Research Objective 4: The forth research objective corresponding to research question 4 is to develop a new situation assessment model. The research assumes that operators are able to form rules for every situation to assess risks, and those rules are an important part of their mental model. Therefore, the research develops a situation assessment model to resemble their thinking when confronting abnormal situations. Fuzzy logic and fuzzy logic systems, which 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, are used to resemble human thinking when they are confronted with abnormal situations.

Research Objective 5: The fifth research objective is to develop a novel DSS model corresponding to research question 5. Previous researches in the field of systems safety have only considered developing scenarios for specific undesirable events from an engineering perspective, whereas in today's safety-critical systems, operators face several hazards from different subsystems which dynamically threaten the system, and they have to comprehend both the current state and the near future state to make correct decisions. A human-centric system is therefore needed to support operators in understanding and assessing the current state of a situation and to assist them to take appropriate actions in abnormal situations. To this end, a new DSS model as shown in Figure 1.1 is proposed to support operators' SA.

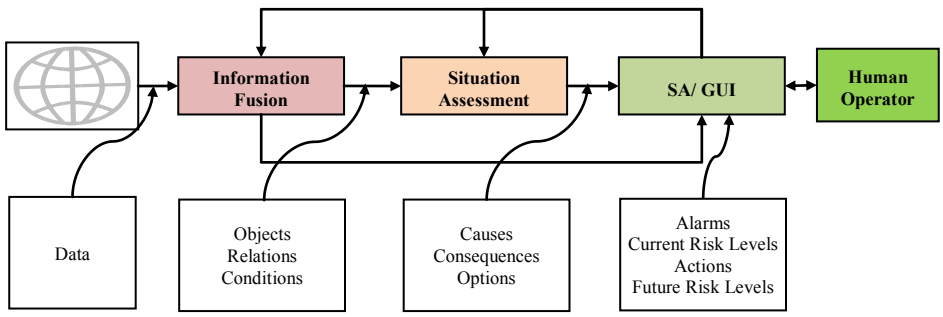


Figure 1.1: The DSS general model

Research Objective 6: The sixth research objective backs to research questions 1, 2, 3, 4 and 5 and aims to develop a system prototype based on the proposed models during this study. The prototype is developed based on the determined requirements, and models proposed in research objectives 3, 4, and 5. To demonstrate the performance of the DSS, three case studies taken from the US Chemical Safety Board investigation reports (www.csb.gov) are used: (1) a residue treater unit at a methomyl unit (CSB 2011), (2) a tank equipped with steam coils at a chemical plant (CSB 2007), and (3) an ink vehicle insulated mix tank at a paint manufacturing company (CSB 2008).

Research Objective 7: The seventh research objectives aims to evaluate the developed DSS. Evaluation is an important aspect of every methodology because it provides a reasonable amount of confidence in the results of the model. Two evaluation methods are relied in this research to validate the performance of the proposed DSS. First a sensitivity analysis is used to evaluate the BN-based situation models. Second a multi-perspective evaluation approach is proposed for full validation of the proposed system.

1.4 RESEARCH CONTRIBUTIONS

According to the research objectives, several research contributions of this study are summarized as follows:

(1) First and foremost among contributions is that this research considers safety in safety-critical environments resulting in human protection from harm and loss of life. 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 modelling 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) This research develops a cognitive DSS 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 proposed DSS 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, thus ensuring that the proposed system conforms to ALARP.

(3) The proposed situation assessment component employs BNs, which have certain advantages over other situation assessment methods that use artificial intelligence tools such as expert systems (Naderpour & Lu 2012a) and neural networks (Naderpour & 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 (Su et al. 2011). The proposed situation assessment model can be applied to other related domains if the risk indicators for any measurement are appropriate.

(4) There were too many alarms and they were poorly prioritized. The control room displays did not help the operators to understand what was happening. These two quotes from an HSE report on a major accident in a chemical process plant clearly indicate that at least not all process control systems represent the state of the art in ergonomics (Nachreiner, Nickel & Meyer 2006). The proposed DSS 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).

(5) The proposed human-centric DSS 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 (Brannon et al. 2009). Therefore, the DSS keeps operators in the loop of decision–making and action–taking.

1.5 RESEARCH METHODOLOGY

Research methodology is the "collections of problem solving methods governed by a set of principles and a common philosophy for solving targeted problems" (Gallupe 2007). Several research methodologies such as case study, field study, design research, field experiment, laboratory experiment, survey, and action research have been proposed and applied in the domain of information systems. The methodology of this research is planned according to the practice of design research (Niu, Lu & Zhang 2009), which has been proposed and applied in information systems, and is based on an SA-oriented design process (Endsley 2006), which has been established to guide the development of systems that support SA.

1.5.1 GENERAL METHODOLOGY

The design research methodology as presented in Figure 1.2 includes five basic stages (Niu, Lu & Zhang 2009):

(1) **Awareness of problem**: This is the first step where limitations of existing applications are analysed and significant research problems are acknowledged. The research problems reflect a gap between existing applications and the expected status. Research problems can be identified from different sources: industry experience, observations on practical applications and literature review. A clear definition of the

research problem provides a focus for the research throughout the development process. The output of this phase is a research proposal for new research effort.

(2) **Suggestion**: This phase follows immediately behind the identification of research problems where a tentative design is suggested. The tentative design describes what the prospective artefacts will be and how they can be developed. Suggestion is a creative process during which new concepts, models and functions of artefacts are demonstrated. The resulting tentative design of this step is usually one part of the research proposal.

(3) **Development**: This phase considers the implementation of the suggested tentative design artefacts. The techniques for implementation will be based on the artefact to be constructed. The implementation itself can be simple and does not need to involve novelty; the novelty is primarily in the design not the construction of the artefact. The development process is often an iterative process in which an initial prototype is first built and then evolves as the researcher has deeper comprehension of research problems. Thus, the output of the suggestion step is also feedback of the first step, whereby the research proposal can be revised. This step includes the following sub-steps to create the prototype (Niu, Lu & Zhang 2009): a) planning, b) analysis, c) design, d) development, e) testing, f) implementation, and g) maintenance.

(4) **Evaluation**: This phase consider the evaluation of the implemented artefacts. The artefacts performance can be evaluated according to criteria defined in the research proposal and the suggested design. The evaluation results, which might or not meet the expectations, are fed back to the first two steps. Accordingly, the proposal and design might be revised and the artefacts might be improved.

(5) **Conclusion**: This is the final phase of a design research effort. Typically, it is the result of satisfaction with the evaluation results of the developed artefacts. However, there are still deviations in the behaviour between the suggested proposal and the artefacts that are actually developed. A design research effort concludes as long as the developed artefacts are considered as 'good enough' wherein the anomalous behaviour may well serve as the subject of further research.

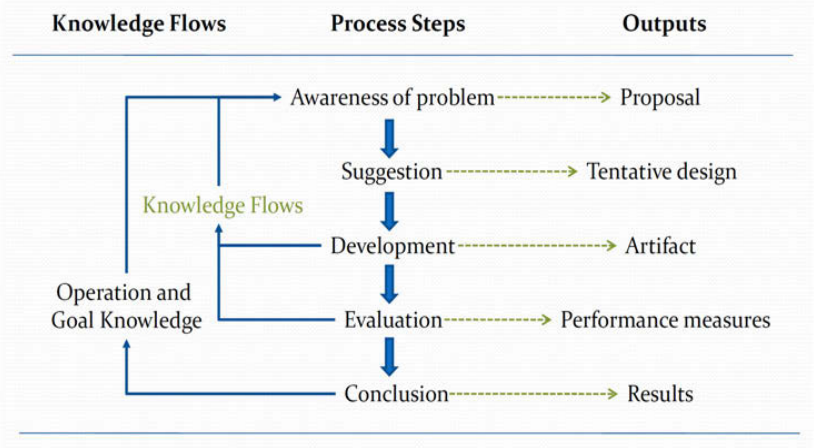


Figure 1.2: The general methodology of research

1.5.2 SA-Oriented Design Process

The SA-oriented design process as shown in Figure 1.3 incorporates SA considerations, including the determination of SA requirements, design principles for SA enhancement, and the measurement of SA in design evaluation. SA oriented design principles include (1) general guidelines for supporting SA, (2) guidelines for coping with automation and complexity, (3) guidelines for the design of alarm systems, and (4) guidelines for the presentation of information uncertainty. Some of the general principles include the following: (1) Direct presentation of higher-level SA needs (comprehension and projection) is recommended, rather than supplying only low-level data that operators must integrate and interpret manually; (2) goal-oriented information displays should be provided and organized so that the information needed for a particular goal is collected and answers directly the major decisions associated with the goal; (3) support for global SA is critical, providing an overview of the situation across the operator's goals at all times (with detailed

information for goals of current interest) and enabling efficient and timely goal switching and projection; (4) critical cues related to key features of schemata need to be determined and made salient in the interface design (in particular, those cues that will indicate the presence of prototypical situations will be of prime importance and will facilitate goal switching in critical conditions); (5) extraneous information not related to SA needs should be removed (while carefully ensuring that such information is not needed for broader SA needs); and (6) support for parallel processing, such as multimodal displays, should be provided in data-rich environments. SA-oriented design is applicable to a wide variety of system designs. It has been used successfully as a design philosophy for systems involving operations, medical systems, flexible manufacturing cells, and command and control for distributed teams (Endsley 2006; Endsley, Bolté & Jones 2003).

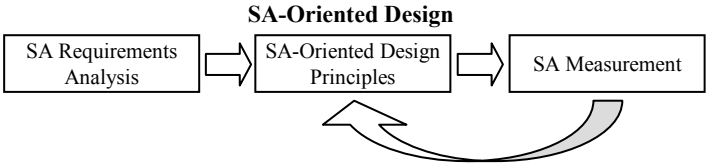


Figure 1.3: SA-oriented design process

1.5.3 RESEARCH PLAN

Considering design research and SA-oriented design methodologies, the research plan of this study consisted of the following steps:

Step 1: Select a topic: The choice of a research topic can arise from personal interest, from observation, or from the literatures describing previous theory and research in the area, from social concern or as the outcome of some currently popular issues. The topic of this research was chosen from the previous literature and research and also the author's observation and experience in the process industry.

Step 2: Review the literature: Irrespective of the reason for choosing a particular topic, a literature review of previous research in the topic area is an essential component of the research process. Existing literature was retrieved and critically reviewed.

Step 3: Finalize research problems: The results of the literature review helped to define the specific research questions for this research. The research questions were directly addressed in this research project.

Step 4: Determine SA requirements: To identify the aspects of a situation that are important for an operator's SA, GDTA methodology, which is a form of cognitive task analysis, was 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) (Jones et al. 2011). In this analysis, the major goals and sub-goals of a particular job were initially identified, after which important decisions that need to be made were determined. The SA requirements for making these decisions and achieving each sub-goal were then identified. GDTA is not task-based analysis because in many environments the goals, not the tasks, form the basis for decision-making (Endsley 2006).

Step 5: Develop a modelling method to represent operators' mental models: The abnormal situations were defined using risk indicators and were modelled using BNs. Bayesian networks are able to visually represent all the relationships between the objects in the situation with connecting arcs. It is easy to recognize the dependence and independence between various objects and situations. They can handle situations where the data set is incomplete since the model accounts for dependencies between all variables.

Step 6: Develop a situation assessment method: Situation awareness as a product of situation assessment process provides input to the decision-making procedure. Therefore, it is an important part of the DSS model. A situation assessment method was proposed that exploits the capabilities of fuzzy logic systems.

Step 7: Develop the situation awareness support system (SASS) model: A cognition-driven DSS called the SASS was developed that consisted of five major

components. It included a knowledge-base that contained abnormal situation models that were developed based on the proposed method in Step 5. It needs the related data of a situation (for example sensors) to be collected from the operation area, so the SASS includes a component to provide updated values of observable variables. Then it contains a situation assessment component based on the proposed method on Step 6 to dynamically show the risk level of situations of interests. If the risk level of a situation is not acceptable (that is 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 8: Design and implement the proposed SASS: The SASS prototype system is designed and implemented in this step according to the proposed model and SA-oriented design principles. This step includes the following sub-steps to create the prototype (Niu, Lu & Zhang 2009):

- Planning: Define the system to be developed. Set the scope and define high-level system requirements. Develop the project plan and establish milestones including tasks and resources, and identify critical success factors which requires end users and experts to work together to develop system requirements.
- Analysis: Design the technical architecture required to support the system models and algorithms that are developed in previous steps
- Design: Build a technical blueprint of how the system will function. Technical architecture defines the hardware and software equipment required

to run the system. The design phase uses models and graphical representation of designs including the GUI.

- Development: During this phase the design is developed into a functional system by developing the technical architecture, database and programs.
- Testing: This phase involves writing the test conditions, developing detailed steps the system must perform along with the expected results of each step. The system is tested to verify that it actually works and meets all of the requirements defined. End-user acceptance testing is performed to duplicate actual use. Testing should be done under conditions as close to operational as possible.
- Implementation: Implementation includes making the system operational, writing detailed user documentation, and providing training for the systems end users.
- Maintenance: Monitor system to ensure it continues to function. Establishes a help report to support system end users and provides an environment to support system changes and upgrades.

Step 9: Demonstrate the performance of the proposed SASS through case studies: The literature provides many examples of incidents and accidents that could have been avoided if operators had recognized the situation in time. Therefore, three investigated cases related to SA are chosen to demonstrate the performance of the SASS.

Step 10: 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. As BNs are utilized to develop the situation models, the sensitivity analysis can therefore be used for the partial evaluation of the SASS. In addition, a multi-perspective evaluation approach based on SA measures is proposed for full evaluation of the SASS.

1.6 THESIS STRUCTURE

This thesis contains nine chapters as shown in Figure 1.4. Chapter 1 presented the research background, challenges, objectives, contributions, methodology, and is presenting the thesis structure.

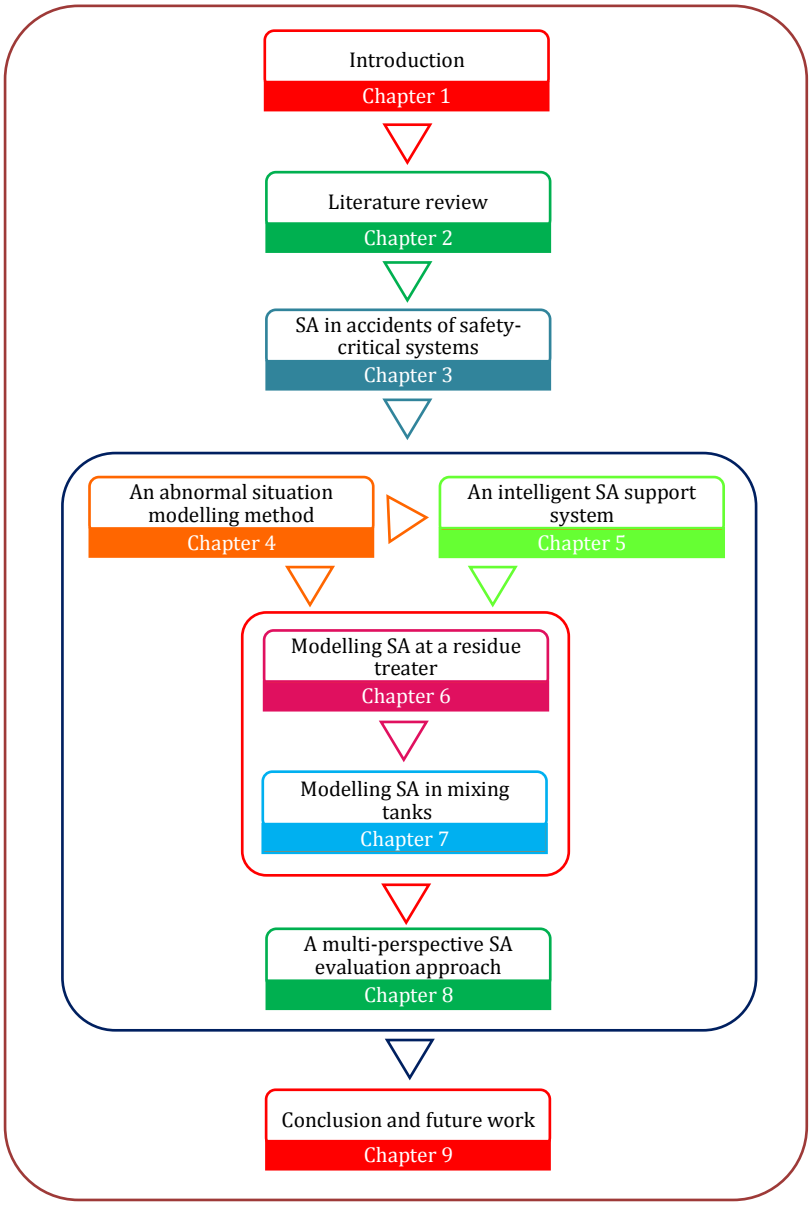


Figure 1.4: Thesis structure

Chapter 2 reviews the literature in regard with SA, situation assessment, SA measurements, BNs theory, and fuzzy systems. Chapter 3 analyses three major accidents in recent US history and highlights the role of SA in their occurrence. Chapter 4 introduces a

novel abnormal situation modelling method. Chapter 5 describes the SASS and its component in details. Chapters 6 and 7 present the performance of the proposed SASS in three safety-critical environments. Chapter 8 shows the multi-perspective evaluation approach for validating the SASS. Chapter 9 presents the conclusion and future research directions of this study.

1.7 PUBLICATIONS AND AWARDS OF THIS RESEARCH

Some chapters of the thesis are based on articles that were published in the peer-reviewed scientific literature during my Ph.D. education. In addition, the research study has gained several awards. The details are as follows:

PEER REVIEWED INTERNATIONAL JOURNAL PAPERS

(1) M. Naderpour, J. Lu, G. Zhang, "An Intelligent Situation Awareness Support System for Safety-Critical Environments", Decision Support Systems 59 (2014) 325-340 (ERA Tier A* Journal).

(2) M. Naderpour, J. Lu, G. Zhang, "The Explosion at Institute: Modeling and Analyzing the Situation Awareness Factor", Accident Analysis and Prevention 73 (2014) 209-224 (ERA Tier A* Journal).

(3) M. Naderpour, J. Lu, G. Zhang, "Modeling Abnormal Situations in Safety-Critical Systems to Support Operators' Situation Awareness", Reliability Engineering & System Safety 133 (2015) 33-47 (ERA Tier A Journal).

(4) M. Naderpour, J. Lu, G. Zhang, "A Situation Risk Awareness Approach for Process Systems Safety", Safety Science 64 (2014) 173-189 (ERA Tier A Journal).

(5) M. Naderpour, J. Lu, "A Situation Analysis Decision Support System Based on Dynamic Object Oriented Bayesian Networks", Journal of Software 9 (8) (2014) 2194-2199 (ERA Tier B Journal).

(6) M. Naderpour, J. Lu, G. Zhang, "A Multi-Perspective Approach for Evaluating a Situation Awareness Support System in a Safety-Critical Environment", Submitted to Applied Ergonomics, 2014 (ERA Tier A* Journal).

(7) M. Naderpour, S. Nazir, J. Lu, "The Role of Situation Awareness in Accidents of Large-scale Technological Systems", Submitted to Process Safety and Environmental Protection, 2014 (ERA Tier B Journal).

PEER REVIEWED INTERNATIONAL CONFERENCE PAPERS

(8) M. Naderpour, J. Lu, "A Hybrid Bayesian Network for Safety of Chemical Plants", the 17th Pacific Asia Conference on Information Systems (PACIS), 2013, Jeju Island, Korea (ERA Tier A Conference).

(9) M. Naderpour, J. Lu, G. Zhang, "A Fuzzy Dynamic Bayesian Network-Based Situation Assessment Approach", the 22nd IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), 2013, Hyderabad, India (ERA Tier A Conference).

(10) M. Naderpour, J. Lu, "A Fuzzy Dual Expert System for Managing Situation Awareness in a Safety Supervisory System", the 21st IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), 2012, Brisbane, Australia (ERA Tier A Conference).

(11) M. Naderpour, J. Lu, "Supporting Situation Awareness Using Neural Networks and Expert Systems", the 10th International FLINS Conference on Uncertainty Modeling in Knowledge Engineering and Decision Making, 2012, Istanbul-Turkey (ERA Tier B Conference).

(12) M. Naderpour, J. Lu, E. Kerre, "A Conceptual Model for Risk-based Situation Awareness", the 6th International Conference on Intelligent Systems and Knowledge Engineering (ISKE), 2011, Shanghai, China (ERA Tier B Conference).

(13) J. Lu, M. Naderpour, "Reducing Human Error in Abnormal Situations: A Situation Risk Awareness Approach", the 5th Early Recognition, Monitoring and Integrated Management of Emerging, New Technology related Risks Conference (iNTeg-Risk), 2013, Stuttgart, Germany.

BOOK CHAPTER

(14) M. Naderpour and J. Lu, 2013, "A Human Situation Awareness Support System to Avoid Technological Disasters", in B. Vitoriano, J. Montero & D. Ruan (eds),

Decision Aid Models for Disaster Management and Emergencies, vol. 7, Atlantis Press, pp. 307-325.

AWARDS

(15) Best Poster Award in the 6th International Conference on Intelligent Systems and Knowledge Engineering (ISKE), 2011, Shanghai, China.

(16) Higher Degree Research Student High Quality Publication Award, the Faculty of Engineering and Information Technology, the University of Technology Sydney, 2014, Sydney, Australia.

(17) UTS Finalist in Trailblazer Competition (competition of innovative ideas which have the potential to benefit the community), UniQuest, 2012, Sydney, Australia.

Chapter 2:

LITERATURE REVIEW

2.1 INTRODUCTION

To get a better understanding of this thesis, this chapter explains important background information regarding situation awareness (SA), Bayesian networks (BNs), and fuzzy systems. Sections 2.2 to 2.7 describe the theories of SA and related concepts, explain the importance of the concept with respect to human decision making and describe how to measure it. Section 2.8 gives an overview of BNs. Section 2.9 provides the preliminary concepts of fuzzy systems.

2.2 THEORY OF SITUATION AWARENESS

The concept of SA was identified by Oswald Boelke who realized the importance of gaining an awareness of the enemy before the enemy gained a similar awareness, and devised methods for accomplishing this (Stanton, Chambers & Piggott 2001). The primary research into SA came from the aviation industry, where the importance of SA in maintaining safe control of an aircraft is obvious. One review of over 200 aircraft accidents found that poor SA was the main causal factor (Endsley 1997). A review in other domains, such as the nuclear power industry, showed that this is not a problem limited to aviation, but one faced by many complex systems where combining and presenting the vast amounts

of data available from many technological systems in order to provide true SA, is a challenge whether it is for a pilot, a physician, a business manager, or an automobile driver (Endsley 2006). Studies of accidents throughout many industries have found that loss of, or poor operator's SA, was related to accidents classified as human error.

Situation awareness is knowing and understanding what is going on around you and predicting how things will change (Vincenzi, Mouloua & Hancock 2004). To date, several SA models, such as Bendy and Meister (1999), Smith and Hancock's (1995) and Endsley (1995) have been developed as a consequence of the difficulty of defining SA; however, Endsley's model has undoubtedly received the most attention. This section presents three main SA theoretical approaches including the activity approach, the ecological approach, and the information processing approach.

2.2.1 INTERACTIVE SUB–SYSTEMS

This approach is based on a functional model of orientation activity that comprises eight main function blocks. The approach does not specify processes that are traditional to cognitive psychology, such as perception, memory, thinking, and action execution. Instead it proposes that the extent to which processes are involved is dependent on the nature of the task and the goals of the individual (Bedny & Meister 1999). The model shows eight functional blocks connected through feed-forwards and feedback loops, as illustrated in Figure 2.1. Each function block has a specific task in the development of SA and structure of activity, and depends upon the nature of the dynamic situation. A summary of the role of each block is presented in Table 2.1.

As can be seen from Figure 2.1, new information arrives via the sensory-perceptual systems to function block 1 to be interpreted through the individuals conceptual model of the world (function block 8), their 'image' of the purpose of the task goals (function block 2) and their orientation about what type of activity is required (function block 5). This interpretation then informs the person's pure image of the task goals (function block 2). The individual determines which features of the world are pertinent in function block 3 on

the basis of the significance and motivation toward the task goals (function block 4) as well as their engagement with the world (function block 5). The extent to which they engage the task goals is determined in function block 2, which in turn is influenced by the criteria developed for evaluation (function block 6) and the current state of the world (function block 3). The outcome of this evaluation directs performance and the person's engagement with the work (function block 5) from which further criteria are developed (function block 6). Interaction with the world is stored as experience (function block 7) and informs the individuals stored representation of the world (function block 8). As the interactive model shows, information from the person's actions and their conceptual model (function blocks 5 and 8) feed forward into the new interpretation of information from the world (function block 1).

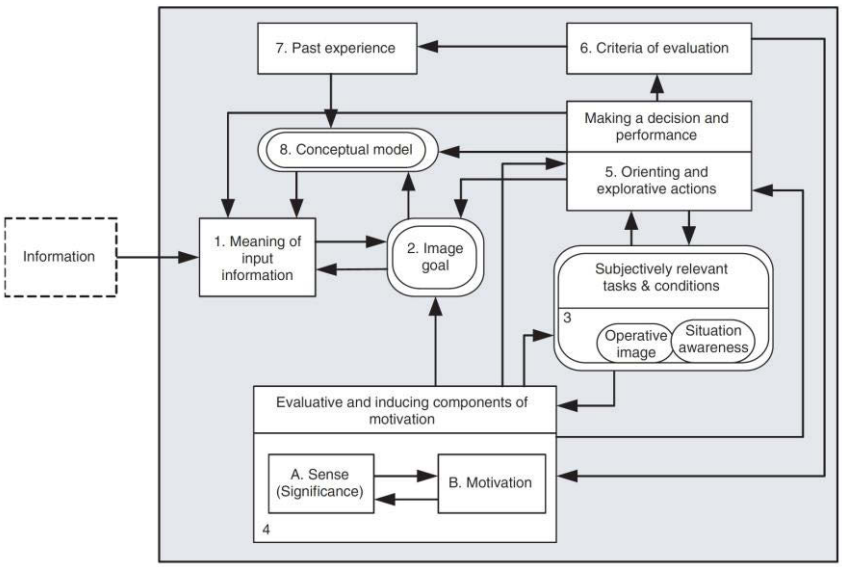


Figure 2.1: The interactive sub-systems approach to situation awareness

As a systems theory of activity, the model looks incomplete. Two glaring problems seem to be the lack of feed-forward from function block 2 (for example a direct link to function block 4) and no link to the world from function block 5. Despite this, the interacting sub-systems present an appealing description of human cognition (Stanton, Chambers & Piggott 2001).

Table 2.1: Summary of the role and inputs to function blocks

Block	Function	Input block	Summary of role
1	Meaning	0,2,5,7	Interpretation of information from world
2	Image	1,4,5,8	Conceptual 'image' of information–task–goal
3	Conditions	4,5	Dynamic reflection of situation and task
4	Evaluation	3,6	Comparing motivation and performance
5	Performance	3,4	Interacting with the world
6	Criteria	4,5	Determining relevant criteria for evaluation
7	Experience	6	Modify experience to interpret new information
8	Model	7	Modify world model to interpret new information

2.2.2 THE PERCEPTUAL CYCLE

Smith and Hancock's (1995) ecological approach takes a more holistic stance, viewing SA as a "generative process of knowledge creation and informed action taking". Their description is based upon Niesser's (1976) perceptual cycle model, which describes an individual's interaction with the world and the influential role of schemata in these interactions. According to the perceptual cycle model, one's interaction with the world (termed 'explorations') is directed by internally held schemata. The outcome of interaction modifies the original schemata, which in turn directs further exploration. This process of directed interaction and modification continues in an infinite cyclical nature.

Using this model, Smith and Hancock (1995) suggest that SA is neither resident in the world nor in the person, but resides through the interaction of the person with the world. They describe SA as: 'externally, directed consciousness' that is an 'invariant component in an adaptive cycle of knowledge, action and information'. They believe that the process of achieving and maintaining SA revolves around internally held mental models, which contain information regarding certain situations. These mental models facilitate the anticipation of situational events, directing an individual's attention to cues in the environment and directing their eventual course of action. An individual then conducts checks to confirm that the evolving situation conforms to their expectations. Any unexpected events serve to prompt further search and explanation, which in turn modifies the operator's existing model (Salmon et al. 2008). The perceptual cycle can be used to explain human information processing in control rooms. For example, assume that the

control room engineers have the correct knowledge of the system that they are controlling, therefore, their mental models enable them to anticipate events such as the morning and evening peaks in demand, search for confirmatory evidence, direct a course of action and continually check that the outcome is as expected. If they uncover some data they do not expect (such as a rise or fall in pressures not in line with those anticipated) they are required to source a wider knowledge of the world to consider possible explanations that direct future search activities. The completeness of the model is in the description of process (the cyclical nature of sampling the world) and product (the updating of the world model at any point in time) (Stanton, Chambers & Piggott 2001).

Adams et al. (1995) argue that process–product dichotomy of SA embraced in differing degrees by the theorists can be taken in context through consideration of a theory of human information processing. Process refers to the perceptual and cognitive activities involved in revising the state of SA whereas product refers to the state of SA with regard to available information and knowledge. An illustration of the perceptual cycle is shown in Figure 2.2.

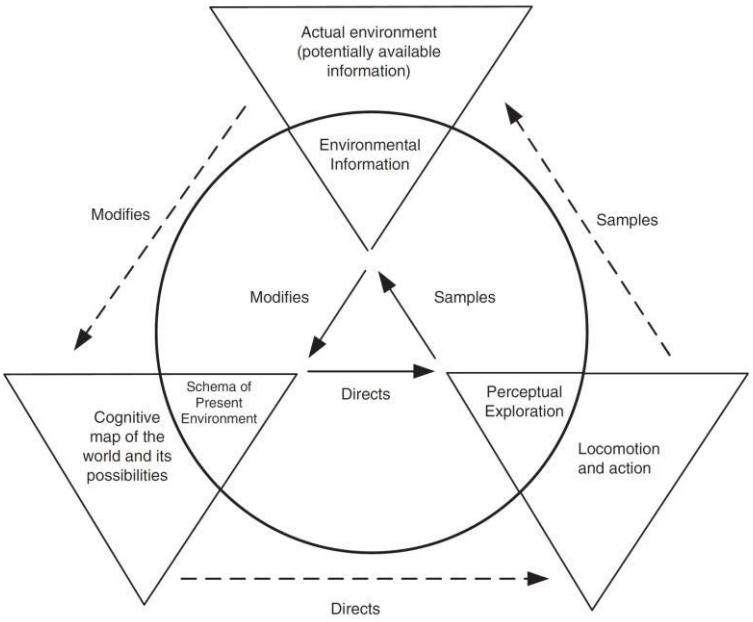


Figure 2.2: The perceptual cycle model of situation awareness

2.2.3 INFORMATION PROCESSING MODEL

Endsley (1995b) 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". This SA model follows an information processing chain from perception, through comprehension, to projection as shown in Figure 2.3. From the lowest to the highest, the levels of SA are as follows (Endsley 1995b; Sneddon, Mearns & Flin 2006; Stanton, Chambers & Piggott 2001):

- *Perception*: Perception involves the sensory detection of significant environmental cues. It means in order to achieve SA, the work environment should be continually monitored to encode sensory information and to detect changes in significant stimuli. Attentional processing is intrinsically linked to the theory of SA, but attention is bound by the limits of the working memory system. This means that workers are unable to pay close attention to every single detail of their environment. Consequently, attention is selective, and critical elements may be missed or ignored in the perception stage.
- *Comprehension*: Comprehension involves the combination, interpretation, storage, and retention of the incoming information to form a picture of the situation whereby the significance of objects/events is understood essentially as a derivation of meaning from the elements perceived. This is partly driven by mental models (representations of objects, people, and tasks) already stored in long-term memory. The degree of comprehension that is achieved will vary from person to person, and the level attained is an indication of the skill and expertise (richness and accessibility of mental models) held by the operator.

- *Projection*: The final level is projection, which occurs as a result of the combination of levels 1 and 2. This stage consists of extrapolating information forward in time to determine how it will affect future states of the operating environment. The higher levels of SA allow operators to function in a timely and effective manner, even with very complex and challenging tasks.

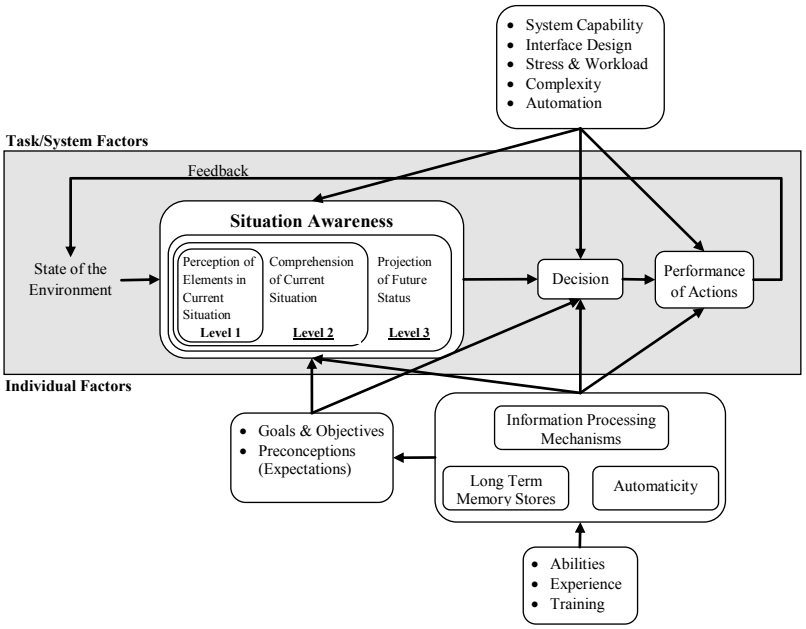


Figure 2.3: The information processing model of situation awareness

McGuinness and Foy (2000) extend Endsley's model by adding a fourth level, which is called Resolution. This level provides awareness of the best path to follow to achieve the desired outcome to the situation. They believe that for any successful fusion, it must be flexible and dynamic. It must also address the entire process; from data acquisition to awareness, prediction and the ability to request elaboration or additional data. Roy (2001) proposed a situation analysis process to provide and maintain a state of SA. Salerno et al. (2004) have proposed a framework for SA under the title of data fusion. The concept of situation management in dynamic systems proposed by Jakobson et al. (2007) includes not only the processes of perceiving and recognizing situations, but also the analysis of past situations and the prediction of future situations.

The concept that was established by Endsley, has been more or less accepted by the information fusion community. Moreover, this model has been used in various studies as a justification for structuring the computer-supported SA process (Kokar, Matheus & Baclawski 2009). Her model has been used in a variety of complex environments such as air traffic controllers, nuclear power plant operators, anesthesiologists, military commanders, electronic warfare tacticians, automobile drivers, power plant, and so on (Banbury & Tremblay 2004; Endsley 2006; Endsley & Connors 2008; Endsley & Garland 2000).

2.2.4 SUMMARY OF SA THEORIES

Apart from the three SA theories presented above, there are several other theories that try to underpin individual SA. In this research the information processing model developed by Endsley (1995b) is relied upon. Table 2.2 shows the summery of some theories (Salmon et al. 2008; Stanton, Chambers & Piggott 2001).

Table 2.2: Summary of situation awareness theories

Theory	Applications	Strengths	Weaknesses
Three Level Model (Endsley, 1995)	Military, Air Traffic Control, Aviation, Driving, Nuclear Power	1- Simple intuitive of SA 2- Division of SA into levels is neat and permits simplistic measurement using SAGAT 3- Holistic approach that considers factors such as system and interface design, workload and training	1- Fails to clear for dynamic nature of SA 2- SA process oriented definition is contradictory to the description of SA as a product comprising three levels 3- Based on ill defined and poorly understood psychological models
Perceptual Cycle Model (Smith & Hancock, 1995)	Air Traffic Control	1- Dynamic description of SA acquisition, maintenance and update of schema 2- Sound theoretical underpinning 3- Completeness of model is attractive i.e. it describes both the process of acquiring SA and the product of SA	1- Dose not translate easily to SA description and measurement 2- Limited applications 3- The actual correlation between SA and performance is complex and not yet fully understood
Theory of Activity (Bedny & Meister, 1999)	-	1- Models offer a more complete, dynamic description of SA than the three level model 2- Clear description of each functional blocks role in SA acquisition and maintenance is useful 3- Sound theoretical underpinning	1- Very limited application and model lacks supporting empirical evidence 2- Not measurement approach suggested 3- Individual approach that does not attempt to describe team SA
Sarter & Woods (1991)	Aviation	1- Focus on the temporal dimensions of SA 2- Emphasize the differences between SA, mental models and situation assessment	1- Very limited application and model lacks supporting empirical evidence
Adams, Tenney & Pew (1995)	Aviation	1- Describe how SA is dynamically acquired, maintained and updated 2- Use logically the model to explain anticipation	1- Measuring the construct in accordance with the perceptual cycle description is very difficult

2.3 SITUATION ASSESSMENT

Situation awareness is a state of knowledge that has to be distinguished from the processes underlying the achievement of SA, which should be more properly termed 'situation assessment' (Endsley 1995b). Situation assessment models describe basic principles and general features about how people process information or interact with the environment to attain their SA. In fact, awareness information for a situation is derived as a result of situation assessment. There is a rich literature on SA, ranging from SA system modelling to cognitive workload assessment and support. However, the majority of them to date have focused on the development of situation assessment models, rather than the implementation of SA systems. Since SA is a dynamic and collaborative process, assessing a situation requires data integration with the support of computer-based intelligent techniques. In addition, as 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. (2008) 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. In another study, a fuzzy least squares support vector machine technique for situation assessment using the integration of information obtained from related data sources was proposed. An artificially generated dataset to show the accuracy of the technique was utilized (Lu, Yang & Zhang 2008). A neural network-based situation assessment module was developed by Brannon et al. (2009) to provide a high level of SA for decision makers in force protection. 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 (Brannon et al. 2009).

Kim and Seong (2006a) 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. They extended their proposed approach by considering the interdependency of instrumentation and control systems and the operators in the NPP (Kim & Seong 2006b). Other than in NPPs, Bayesian theory has been widely considered in the situation assessment configuration of command and control domains. For instance, Chai and Wang (2011) developed a hierarchical BN-based situation assessment model that includes two layers: the top layer, which serves as a fusion centre, 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 Das et al. (2002) 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 (2012a) developed a dual expert system for situation assessment in a chemical plant and extended it to incorporate the ability of neural networks to project the state of the environment in the near future (Naderpour & Lu 2012b). However, because of the lack of appropriate data for abnormal situations, it could not be implemented in the real world.

2.4 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 system in different domains. Two SA support systems 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 behaviour (Van den Broek et al. 2011). In the second, a model-driven situation analysis decision support system was developed based on abstract state machine modelling and CoreASM tool support for the purpose of infrastructure protection and emergency response (Farahbod et al. 2011). In military services, there are several SA systems, such as systems developed by 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 modelling 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 by Baader et al. (2009) 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 by Brannon et al. (2009) 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 signalling. 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 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 (Kim & Hoffmann 2003).

Although the majority of SA systems modelling 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 (Niu et al. 2013). 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 (Qian et al. 2008) or the prediction of process variables (Juricek, Seborg & Larimore 2001) 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 (Klashner & Sabet 2007).

2.5 SITUATION AWARENESS IN COLLABORATIVE SYSTEMS

Today, in safety-critical systems the overall performance of systems depends on coordinated work among individuals that have responsibility for different subsets of goals, different access to data, and different situation perspectives. Therefore, there is a growing interest in understanding the cognitive and collaborative factors that enable such teams to work effectively (Roth, Multer & Raslear 2006). Thus, the concepts of team SA and shared SA are equally important in this regard. The degree to which every team member possesses SA on these elements for task performance is team SA (Kaber & Endsley 1998). Therefore, the success or failure of a team depends on the success or failure of each of its team members. In contrast, shared SA is defined as the degree to which team members possess the same SA on shared SA requirements (Endsley & Jones 2001). Shared SA allows team members to efficiently coordinate work by enabling them to understand what is going on

with the task, interpret what others are doing, and anticipate what will happen next. It enables team members to anticipate the information and support needs of other team members, resulting in reduced need for explicit communication and improved action coordination (Roth, Multer & Raslear 2006). However, Stanton et al. (2006) showed that because of complexity of current socio-technical systems and the increasing presence of teams, the concept of shared SA is not able to explain appropriately the interactions between agents (i.e. both human and non-human) in subsystems. Therefore, the concept of compatible SA has emerged. Rather than possess shared SA, the new Distributed SA (DSA) based on compatible SA suggests that team members possess unique, but compatible, portions of awareness. The distributive nature of process plants, the importance and necessity of coordination and communication among various team members, located at different locations, the co-existence of technical and non-technical personnel within different units/sections of the plant call for a greater appreciation of DSA. Generally, operators are expected to monitor recurrently the dynamics of the process and to make timely correct decisions based on their mutual comprehension deduced from the available information that is changing dynamically. Team members experience a situation in different ways, as defined by their own personal experience, goals, roles, tasks, training, skills and so on. So whilst some of the information required by two different team members may be 'shared' in the sense that they both need to attend to it as part of their job, their resultant understanding and use of it is different. Ultimately, the picture developed by each team member is unique to themselves. Compatible awareness is therefore the phenomenon that holds distributed systems together (Salmon, Stanton, Walker, Jenkins & Rafferty 2009). The first effort to use the DSA in improving safety in safety-critical environments has been conducted by Nazir et al. (2014). They explain how the ultimate consequences of abnormal situations depend on the shared understanding, compatibility, and effective communication among operators. They also highlight the importance of a shared mental model and joint cognition to facilitate communication and the subsequently necessary actions.

2.6 SITUATION AWARENESS REPRESENTATION

A methodology called Goal-Directed Task Analysis (GDTA) is used to determine the aspects of a situation that are important for a particular user's SA requirements. This methodology is a specific form of cognitive task analysis that focuses on identifying goals and critical information needs in a task context. The GDTA process forms an exemplary template for incorporating human cognition into an actionable model by describing in detail not only a user's information data needs (Level 1), but also how that information should be combined to form the comprehension (Level 2) and projection of future events (Level 3) that are critical to SA, thereby providing a critical link between the data input and the decisions to be made in a goal-directed environment (Jones et al. 2011). In this analysis, the major goals of a particular job class are identified, along with the major sub-goals necessary for meeting each goal. The major decisions that need to be made in association with each sub-goal are then identified. The SA requirements for making these decisions and carrying out each sub-goal is identified (Figure 2.4).

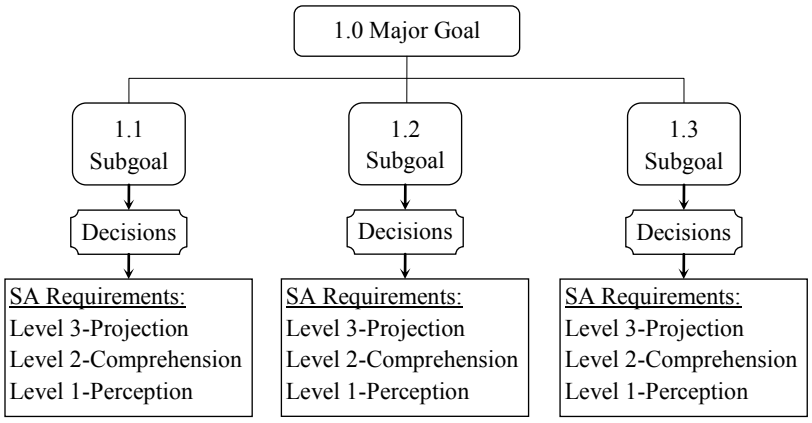


Figure 2.4: Goal-directed task analysis hierarchy

These requirements focus not only on what data the operator needs, but also on how that information is integrated, or combined, to address each decision. This type of analysis is based on goals or objectives, not tasks. This is because goals form the basis for decision-making in many complex environments. Conducting such an analysis is usually carried out

using a combination of cognitive engineering procedures such as expert elicitation, observation of operator performance and analysis of documentation (Endsley 2006).

2.7 SITUATION AWARENESS MEASUREMENT

Stanton et al. (2010) identified three approaches to describe the different contexts, in which the SA concept was developed and measured over the years. These approaches can be categorized as: (a) physiological, (b) engineering, and (c) ergonomics, and they were developed in parallel to social, technical, and socio-technical systems accordingly. In practice, different SA measurement techniques are rooted in these three approaches that correspond to researchers' different perceptions of SA: individual, technical, or systemic endeavour (Chatzimichailidou, Protopapas & Dokas 2015).

The first approach perceives SA as an individual psychological phenomenon. It has gained the interest of many researchers, such as Endsley, who consider SA as a cognitive in-the-head process, without taking into account that human reasoning is usually affected by outer stimuli, owing to their communication with their environment, whether it consists of human or nonhuman elements. The second approach, i.e. the engineering one, describes the "world view" of SA. In this approach, SA is considered to be affected mostly by information possession and flow, as well as by technical infrastructure, for example computers, displays, information systems. The way in which information is presented by artefacts influences SA by determining how much information can be acquired, how accurately it can be acquired, and to what degree it is compatible with SA needs. The third approach is based on the idea that SA is distributed and it emerges from the interactions between human and nonhuman system elements, because the system is viewed as a whole. All in all, the DSA aspect combines the view of SA in the mind and SA in the world (Salmon, Stanton, Walker & Jenkins 2009).

A recent review by Stanton (2005) has identified over thirty different SA measurement approaches. These can be categorized into the following types of SA measures: (1) freeze probe techniques, (2) real-time probe techniques, (3) self-rating techniques, (4) observer

rating techniques, (5) performance measures, (6) process indices, as well as into three categories, and shared SA: (1) team probe-recall techniques, (2) observer rating team SA, and (3) team task performance-based SA measurement techniques.

Endsley's research shows that the direct SA measurements, including subjective and objective measures, are the best way to evaluate a system design (Endsley, Bolté & Jones 2003); however, even the most successful measures are not able to assess operators' SA during real operations (Jones & Endsley 2004). This section reviews the common direct including subjective and objective measures of SA, and provides some information about indirect measures.

2.7.1 SUBJECTIVE MEASURES

In subjective measures, SA is assessed by either an expert observer or the operator during a specified period when they have to rate the quality of the operator's SA. The rating results can then be used to compare the quality of SA in various systems.

- Self-rating techniques assess their own degree of confidence in SA. In these techniques, participants use a rating scale of some sort to provide a subjective rating of their perceived SA. The techniques are quick, easy, low cost, and have a non-intrusive nature because they are administrated post-trial. However, there are several problems associated with post-trial data collection of SA because there is a correlation between SA and performance. In addition, there are some issues in regard to their sensitivity (Salmon, Stanton, Walker, Jenkins, Ladva, et al. 2009). The Situational Awareness Rating Technique (SART) based on Taylor's SA theory (1990), is a self-rating technique that, at the conclusion of an operation, is administered to participants who should subjectively rate their SA based on a 10-dimensional bipolar scale. The participants' ratings on each of the 10 items are combined to form a rating for each of the three major categories, including understanding, attention demand, and attention supply, as well as an overall rating. Although SART effectively provides information regarding participants' confidence in their SA, it can be influenced by performance outcome, because a person

who successfully performs the task may rate SA higher based on the positive outcome of an event, or by memory decay where it is taken at the end of the event. More importantly, people do not know what they do not know, and thus, may be poor at accurately assessing their own SA (Jones & Endsley 2004). Most SART applications have been reported in the domain of air traffic control (Endsley, Selcon, et al. 1998b; Jones & Endsley 2004; Pierce, Strybel & Vu 2008). Another self-rating approach is the Situation Awareness-Subjective Workload Dominance Technique (SA-SWORD), which requires operators to perform a comparative evaluation of systems based on a nine-point scale. Each level of the scale represents the person's belief in the amount of SA that is provided by each system. Further evaluation studies are needed to prove the effectiveness and accuracy of SA-SWORD (Endsley, Bolté & Jones 2003).

- Observer rating approaches include observing participants during task performance by subject matter experts (SMEs) who then rate the participants' SA. Typically, the SA ratings are provided based on pre-defined observable SA related behaviours that participants display during task performance. Observer rating techniques have some advantages. They can be used during real world activities and have no impact on the task being performed. However, they need more scientific reviews because their validity is between doubt and certainty (Salmon, Stanton, Walker, Jenkins, Ladva, et al. 2009). The Situation Awareness Behavioural Rating Scale (SABARS) is an observer rating approach that has been developed to assess infantry SA in field training exercises (Matthews et al. 2005). The Situational Awareness Rating Scale (SARS) represents another observer rating technique that consists of 31 behavioural elements in eight categories. Pilots use a six-point scale to complete the SARS measure for themselves and others in their units by providing a rating on each element (Waag & Houck 1994). The usefulness of SARS is very limited because it only considers a particular type of aircraft, flight skill and mission, and therefore, is not easy to use in other domains.

2.7.2 OBJECTIVE MEASURES

Objective measures attempt to evaluate SA by conducting a direct comparison between operators' SA and reality. This comparison is often concluded either offline or online/real time during a process of querying operators about some aspects of an environment and determining the accuracy of responses by comparing them with reality.

- Freeze probe techniques administer online SA queries during freezes in a simulation environment of tasks under analysis. The simulation is frozen and suspended at randomly selected times, user interfaces are then blanked, and the operator is asked to quickly answer questions about his or her current understanding of the situation. An overall SA score is calculated at the end of the trial by comparing the participant's responses with the real state of the system at the freeze time (Salmon, Stanton, Walker, Jenkins, Ladva, et al. 2009). Freeze probe techniques have no issues associated with collecting SA data post trial. However, they measure SA via information in working memory as operators do not have access to displays when answering the queries (Paige Bacon & Strybel 2013). Situation Awareness Global Assessment Technique (SAGAT) is the most popular freeze probe technique; it was developed to assess pilots' SA based on Endsley's three level model (Endsley & Garland 2000). It has been widely used in a variety of domains, such as air traffic control (Endsley 2000a), commercial and military aviation (Endsley, Farley, et al. 1998), nuclear power plant operations (Jenkins, Stanton & Walker 2012), and simulated air traffic management (Paige Bacon & Strybel 2013).
- Real-time probe techniques, unlike freeze probe techniques, involve the administration of SA related queries on-line with no-freeze of the task under analysis. The queries are developed by SMEs prior to the task or during task performance, and administered when the participant is performing the task. Response content and response time are used to conclude a measure of the participant's SA. Since no-freeze of the task is required in real-time probe techniques, therefore their level of intrusiveness is less than freeze probe approaches (Endsley, Bolté & Jones 2003). The Situation Present Assessment Method

(SPAM) is a real-time probe technique developed for SA assessment of air traffic controllers (Durso, Dattel & Banbury 2004). SPAM has been developed on the basis of this theory that operators who have good SA answer the probes more quickly because they know where to look to find a particular piece of information in the environment. To use SPAM, questions are concurrently asked of operators while they are performing activities and have an access to their displays in full view. Response time is considered as a measure of operators' SA.

2.7.3 INDIRECT MEASURES

Indirect measures try to infer how much SA a person has by measuring the cognitive processes involved in developing SA or by measuring performance issues related to the operator's interaction with the system. Process measures and behavioural and performance measures are sometimes used to infer SA in this manner (Endsley, Bolté & Jones 2003).

- Performance measures are utilized for measuring relevant aspects of participant performance during the task under analysis. Depending upon the task, certain aspects of performance are recorded in order to determine an indirect measure of SA (Salmon, Stanton, Walker, Jenkins, Ladva, et al. 2009). For example, when assessing driver SA, hazard detection, blocking car detection, and crash avoidance during a simulated driving task might be measured.
- Process indices involve recording the processes that participants use in order to develop SA during the task under analysis. Examples of SA-related process indices include the use of eye tracking devices to measure participant eye movements during task performance, the results of which can then be used to determine how the participant's attention was allocated during task performance, and concurrent verbal protocol analysis, which involves creating a written transcript of operator behaviour as they perform the task under analysis. The transcript is based upon the operator 'thinking aloud' as he conducts the task under analysis. Verbal protocol analysis is used as a means of gaining an insight

into the cognitive aspects of complex behaviours and is often used to indicate operator SA during task performance (Salmon, Stanton, Walker, Jenkins, Ladva, et al. 2009).

2.8 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.

2.8.1 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 (Hu et al. 2013). 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 (Hu et al. 2013). In this study, 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 (Khakzad, Khan & Amyotte 2012):

$$P(X) = \prod_{i=1}^{n} P(X_i|Pa(X_i)) \tag{2.1}$$

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 $P\big(X_i\big|Pa(X_i)\big) = P(X_i)$ 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:

$$P(X|E) = \frac{P(X,E)}{P(E)} = \frac{P(X,E)}{\sum_x P(X,E)} \tag{2.2}$$

This equation will be used for probability prediction or probability updating in a given network. In predictive analysis, the conditional probabilities of the form $P(situation|object)$ 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.

2.8.2 Dynamic Bayesian Networks

A DBN model can be obtained from a static BN by introducing relevant temporal dependencies among variables to describe the behaviour 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 (Murphy 2002). 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

$$P(X_t|X_{t-1}) = \prod_{i=1}^{n} P\left(X_t^i|Pa(X_t^i)\right) \tag{2.3}$$

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 $P\left(X_t^i|Pa(X_t^i)\right)$ 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 (Murphy 2002):

$$P(X_{1:T}) = \prod_{t=1}^{T}\prod_{i=1}^{n} P\left(X_t^i | Pa\left(X_t^i\right)\right) \tag{2.4}$$

2.8.3 Object Oriented Bayesian Networks

Modelling systems containing an important number of variables with BNs generally lead to complex models. To avoid this, Object Oriented BNs (OOBNs) have been defined that comprise both instance nodes and usual nodes (Bangso & Wuillemin 2000). An instance node is a sub-network, representing another BN. Using OOBNs, a large complex BN can be constructed as a hierarchy of sub-networks with desired levels of abstraction. This representation method allows the decentralization and structure of the knowledge within BNs of reduced size. Therefore, model construction is facilitated and communication between the model's sub-networks is performed more effectively (Khakzad, Khan & Amyotte 2013).

An OOBN class is a BN fragment containing output, input, and protected (or encapsulated) nodes. The input and output variables form the interface of the class. The interface encapsulates the internal variables of the class, d-separating them from the rest of the network. All communication with other instances is formulated in terms of probability statements over the instance's interface. Further, the tedious task of repeating identical structured fragments and probability tables is alleviated. Instance nodes are connected to other nodes through interface nodes, including input and output nodes. Input nodes accept the same probability values as their immediate parents. Thus, no input node can have more than one parent. In contrast, output nodes are ordinary nodes, conveying their probability values to other input nodes or affecting the probabilities of other usual nodes. Therefore, each output node can have more than one child. Figure 2.5 illustrates how a BN can be developed using a hierarchy of smaller and simpler BNs (Khakzad, Khan & Amyotte 2013).

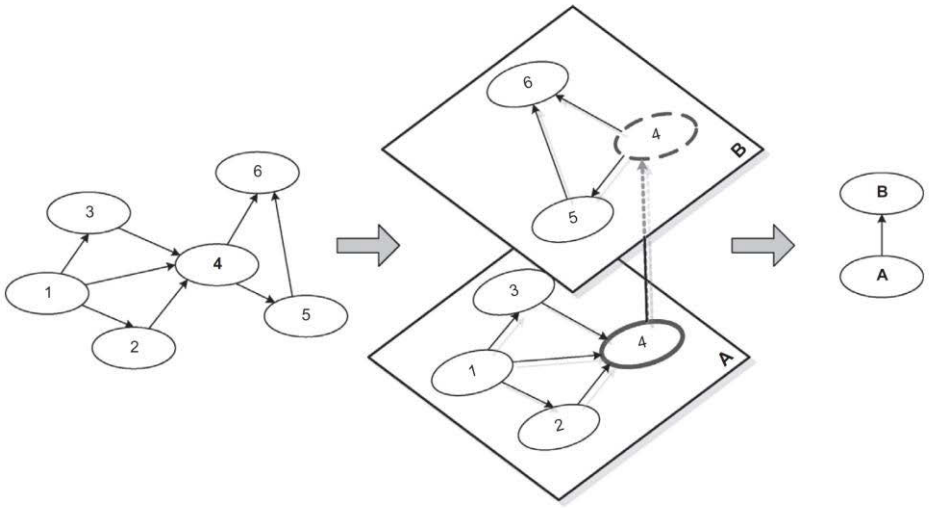


Figure 2.5: Modularize BN into sub-networks using OOBN

Therefore, a class is a BN fragment containing three sets of nodes (Naderpour & Lu 2014):

- *O* is a set of output nodes. Output nodes can be referenced outside the class, hence they can be parents of nodes outside instances of the class;
- *I* is a set of input nodes. Input nodes represent nodes that are actually not in the class; they act as place-holders for parents of nodes inside instances of the class. Input nodes cannot have parents within the class;
- *P* is a set of protected nodes, i.e. nodes that can only have parents and children inside the class itself.

A class encapsulates nodes and restricts the visibility of its nodes to the interior; in order to use a class it must be instantiated. When an instantiation of a class is created, it can be linked to the rest of the network by a reference link. In this study, the class definition is used to develop similar situations.

2.8.4 INFERENCE IN BAYESIAN NETWORKS

As explained, belief updating or probabilistic inference is the basic task for any BN including the computation of the posterior probability distribution for a set of query nodes,

given values for some evidence nodes. Inference in BNs is very flexible, as evidence can be entered about any node while beliefs in any other nodes are updated. There are several major classes of inference algorithms including exact and approximate algorithms that have been developed over the past 20 years.

As a matter of fact, different algorithms are suited to different network structures and performance requirements. Networks that are simple chains merely require repeated application of Bayes' theorem. Inference in simple tree structures can be done using local computations and message passing between nodes. When pairs of nodes in the BN are connected by multiple paths the inference algorithms become more complex. For some networks, exact inference becomes computationally infeasible, in which case approximate inference algorithms must be used. In general, both exact and approximate inference are NP-hard problem (Korb & Nicholson 2003).

Apart from belief updating, given a Bayesian over variables X, which induces a probability distribution P, one can pose a number of fundamental queries with respect to the distribution P:

- Most Probable Explanation (MPE): The most likely instantiation of network variables X, given some evidence e:

$$MPE(e) = \text{argmax}_x P(X, e) \quad (2.5)$$

- Maximum a Posteriori Hypothesis (MAP): The most likely instantiation of some network variables M, given some evidence e:

$$MAP(e, M) = \text{argmax}_m P(m, e) \quad (2.6)$$

These problems are also difficult and are known to be NP-complete, and NPPP-complete, respectively. The exact approaches include structure-based algorithms, inference with local parametric structure, solving MAP and MPE by search, compiling BNs, inference by reduction to logicc (Darwiche 2008). Some approximation algorithms can also be used, such as clustering, unrolled junction tree, and the forward-backward algorithm.

- **INFERENCE BY TREE CLUSTERING**

Tree clustering is an algorithm for exact inference, which is also known as the junction tree algorithm. The idea is to organize the given set of factors into a tree structure, using a junction tree for the given BN. Figure 2.6 depicts a BN, a corresponding junction tree, and assignment of the factors to the junction tree clusters.

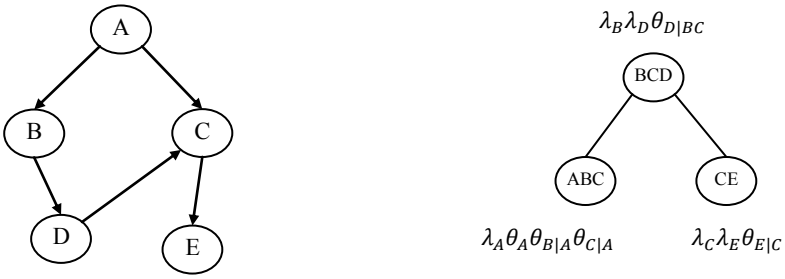


Figure 2.6: A Bayesian network and corresponding junction tree

The junction tree algorithm provides a methodical and efficient method of clustering, versions of which are implemented in the main BN software packages. The junction tree clustering algorithm is as follows (Korb & Nicholson 2003):

Step 1. Moralize: Connect all parents and remove arrows; this produces a so-called moral graph.

Step 2. Triangulate: Add arcs so that every cycle of length > 3 has a chord (i.e., so there is a sub-cycle composed of exactly three of its nodes); this produces a triangulated graph.

Step 3. Create new structure: Identify maximal cliques in the triangulated graph to become new compound nodes, then connect to form the so-called junction tree.

Step 4. Create separators: Each arc on the junction tree has an attached separator, which consists of the intersection of adjacent nodes.

Step 5. Compute new parameters: Each node and separator in the junction tree has an associated table over the configurations of its constituent variables. These are all a table of 'ones' to start with:

For each node X in the original network,

a. Choose one node Y in the junction tree that contains X and all of X's parents,

b. Multiply $P(X|Parents(X))$ on Y's table.

Step 6. Belief updating: Evidence is added and propagated using a message passing algorithm.

2.9 FUZZY SETS AND SYSTEMS

Fuzzy logic is a concept to deal with uncertainty, vagueness, or imprecise problems that uses membership functions with values between 0 and 1. Fuzzy set theory, which is based on fuzzy logic, was first proposed by Zadeh in 1965. In fuzzy set theory unlike conventional set theory based on Boolean logic, a particular object or variable 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) (Zadeh 1965).

2.9.1 FUZZY SETS AND NUMBERS

Definition 1 (Fuzzy set): A 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. $A: X \rightarrow [0,1]$ (Zadeh 1965).

Definition 2 (Support of a fuzzy set): The support of a fuzzy set A in the universe of discourse X is a set that contains all the elements of X that have nonzero membership values in A, that is,

$$supp(A) = \{ x \in X | \mu_A(x) > 0 \} \quad (2.7)$$

where $supp(A)$denotes the support of fuzzy set A.

Definition 3 (α-cut): 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 set A_α defined by (Shapiro 2009):

$$A_\alpha = \{ x \in X | \mu_A(x) \geq \alpha \} \quad (2.8)$$

Figure 2.7 shows an example of an α-cut in which the domain under consideration is limited to a set of elements with a degree of membership of at least alpha. The support of

fuzzy set A is all x such that $\mu_A(x) > 0$, and its α-cut is from X_{left}^{α} to X_{right}^{α}. Values outside the interval are considered as insignificant values that should be excluded from consideration i.e. this is cut out.

Definition 4 (Fuzzy number): A fuzzy set A in $\mathbb{R}$ satisfies the following conditions (Dubois & Prade 1978):

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

Figure 2.7 represents the general characteristic of a fuzzy number A where $\mu_A(x)$ denotes the membership function of x in the fuzzy set. This shape of fuzzy number is referred to as a "triangular" fuzzy number, and is denoted by the triple (a_1, a_2, a_3).

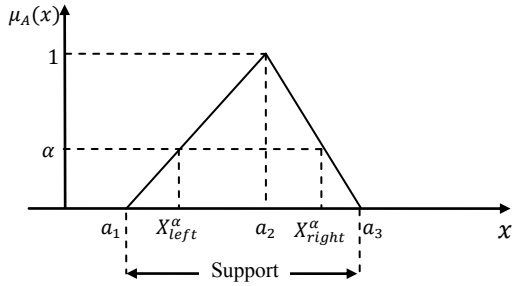


Figure 2.7: A fuzzy number

Definition 5 (Fuzzy random variable): Let $(\Omega, \mathcal{F}, \mathrm{P})$ be a probability space, $\mathrm{F}(\mathbb{R})$ the set of fuzzy numbers in $\mathbb{R}$ with compact supports and W is a mapping $\Omega \to \mathrm{F}(\mathbb{R})$. Then W is a fuzzy random variable if and only if given $\omega \in \Omega$, $\mathrm{W}_\alpha(\omega)$ is a random interval for any $\alpha \in [0,1]$ where $\mathrm{W}_\alpha(\omega)$ is a α-level set of the fuzzy set $\mathrm{W}(\omega)$ (Kwakernaak 1978).

Note: A subset of Euclidean space $\mathbb{R}^n$ is called compact if it is closed and bounded. For example, in $\mathbb{R}$, the closed unit interval $[0,1]$ is compact.

Definition 6 (Fuzzy state): Let the crisp state set $\mathcal{P}$ consist of the states $\mathrm{p}_1, \mathrm{p}_2, \ldots, \mathrm{p}_n$. Then, each fuzzy state can be written as a vector $\mathrm{q} = [\mathrm{q}_1, \mathrm{q}_2, \ldots, \mathrm{q}_n]$, where $\mathrm{q}_i \in [0,1]$. This way, each fuzzy state can be considered as a possibility distribution or alternatively as a fuzzy set $\mathrm{q} \in \mathcal{F}(\mathcal{P})$, ($\mathcal{F}(\mathcal{P})$ the set of all fuzzy subsets defined for $\mathcal{P}$) determining the degree q_i by

which the system participates in each crisp state p_i, provided it is in the current fuzzy state q (Schmidt & Boutalis 2012).

Definition 7 (Linguistic variable): Linguistic variable is a variable whose values are words or sentences in a natural or artificial language (Zadeh 1975). Linguistic variable is characterized by (*X*, *T*, *U*, *M*) where:

- *X* is the name of the linguistic variable (Weather temperature)
- *T* is the set of linguistic values that X can take (*T* = {Cold, Pleasant, Hot})
- *U* is the actual physical domain in which the linguistic variable *X* takes its quantitative (crisp) values (*U* = [−20, 40] °C).
- *M* is a semantic rule that relates each linguistic value in *T* with a fuzzy set in *U*; (*M* relates 'Cold', 'Pleasant', and 'Hot' with the membership functions shown in Figure 2.8).

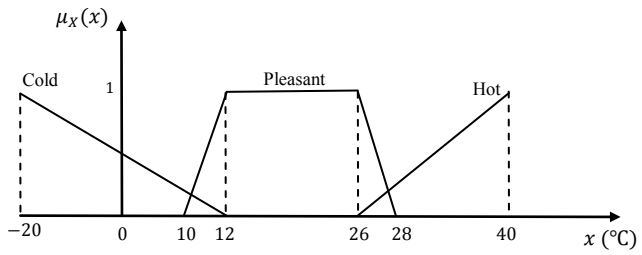


Figure 2.8: **Membership function of weather temperature**

Let *x*, *y* be linguistic variables in the physical domains *U*, *V*, and *A*, *B* be fuzzy sets in *U*, *V*:

- Connective 'And' *x* is *A* and *y* is *B* use fuzzy intersection:
  - $A \cap B \in U * V: \mu_{A \cap B}(x, y) = t[\mu_A(x), \mu_B(y)]$
  - $t: [0,1] * [0,1] \rightarrow [0,1]$ is any *t*-conorm that for $x, y, z \in [0,1]$ satisfies the following four axioms (Wang 1999):
    - $t(x, y) = t(y, x)$ (commutativity),
    - $t(x, t(y, z)) = t(t(x, y), z)$ (associativity),
    - $t(x, y) \leq t(x, z)$ whenever $y \leq z$ (monotonicity),

- $t(x, 1) = x$ (boundary condition).

- Connective 'Or' x is A or y is B use fuzzy union:
  - $A \cup B \in U * V: \mu_{A \cup B}(x, y) = s[\mu_A(x), \mu_B(y)]$
  - $s: [0,1] * [0,1] \rightarrow [0,1]$ is any s-norm that for $x, y, z \in [0,1]$ satisfies the following four axioms (Wang 1999):
    - $s(1,1) = 1,\ s(0, x) = s(x, 0)$ (boundary condition),
    - $s(x, y) = s(y, x)$ (commutative),
    - If $x \leq x'$ and $y \leq y'$ then $s(x, y) \leq s(x', y')$ (nondecreasing),
    - $s(s(x, y), z) = s(x, s(y, z))$ (associative).
- Connective 'Not' x is not A use fuzzy complements

2.9.2 FUZZY LOGIC SYSTEMS

A fuzzy logic system (FLS) as shown in Figure 2.9 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 (Markowski et al. 2011).

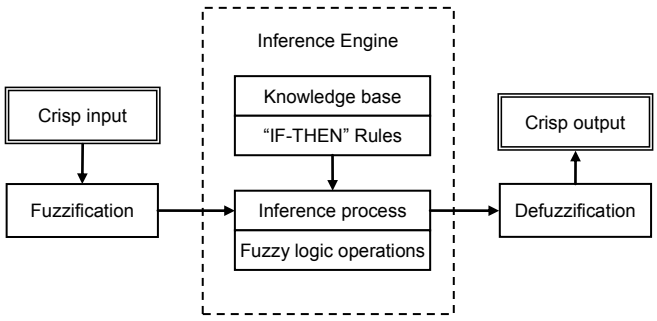


Figure 2.9: A fuzzy logic system

There are several inference methods, however, Mamdani (1977) and Takagi and Sugeno (1985) methods are most commonly used in industrial and fuzzy software tools.

The characteristic of Mamdani's model also known as the Max-Min fuzzy rule based inference are presented in Table 2.3.

Table 2.3: Characteristics of the Mamdani model

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	$min(\mu_A(x), \mu_B(x))$
Aggregation	MAX	$max(min(\mu_A(x), \mu_B(x)))$
Defuzzification	CENTROID	$COA = Z^* = \frac{\int z\, \mu_C(z)\, dz}{\int \mu_C(z)\, dz}$

$\mu_C(x)$ = 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).

In summary, Figure 2.10 shows a Mamdani fuzzy inference system with two rules. It fuzzifies the two inputs by finding the intersection of the crisp input value with the input membership function. It uses the minimum operator to compute the fuzzy AND for combining the two fuzzified inputs to obtain a rule strength. It clips the output membership function at the rule strength. Finally, it uses the maximum operator to compute the fuzzy OR for combining the outputs of the two rules.

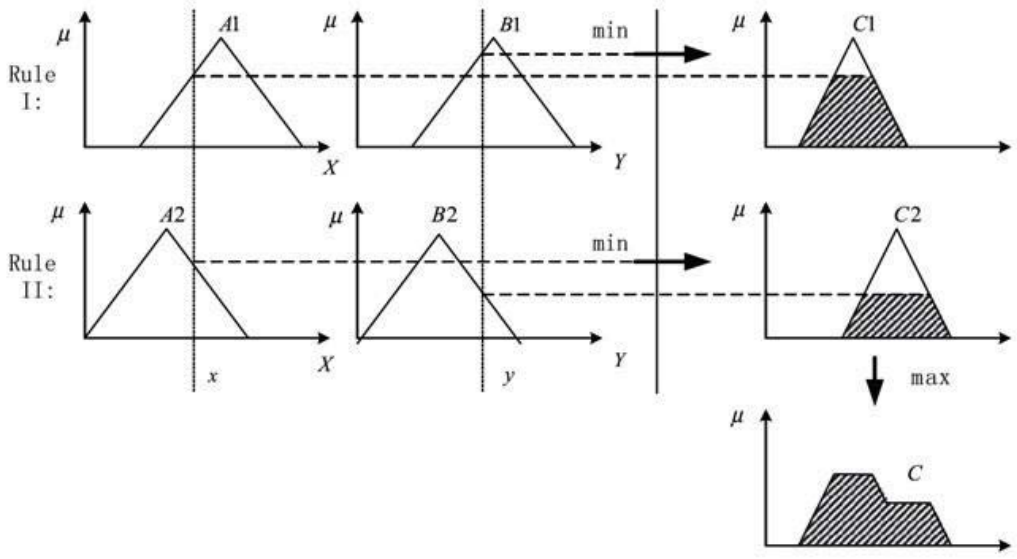


Figure 2.10: Mamdani fuzzy inference system for two inputs and single output

The Sugeno fuzzy inference method is quite similar to the Mamdani's, however the difference is that the output consequence is not computed by clipping an output membership function at the rule strength. In fact, in the Sugeno's model there is no output membership function at all. Instead the output is a crisp number computed by multiplying each input by a constant and then adding up the results.

2.10 SUMMARY

This chapter reviews the background and related literature of this research. First, the SA theories including interactive sub-systems, the perceptual cycle, and the information processing model, and related concepts are described. It is worth noting that the information processing model of Endsley (1995b) is relied on throughout this research as a justification for structuring the computer-supported SA support system. Second, the chapter presents the theory of Bayesian networks, and the preliminary introduction of fuzzy systems to provide a strong foundation for the subsequent analysis, methods, and systems presented in later chapters.

Chapter 3:

SITUATION AWARENESS IN ACCIDENTS OF SAFETY–CRITICAL SYSTEMS

3.1 INTRODUCTION

In the early morning hours of 3 December 1984, more than 40 metric tons of methyl isocyanate (MIC) gas leaked into the air from a pesticide plant located in the region of Bhopal, central India causing one of the worst industrial disasters in history. Several hundred thousand people in towns nearby were exposed to the chemicals, and approximately 3,800 were killed immediately, at least 600,000 were injured, and at least 6,000 have died since (Broughton 2005). Three decades after the disaster, still high levels of contamination of toxic organic chemicals are found in the soil and water samples.

The investigation of the disaster showed that on account of a series of mechanical and human errors in the production plant, water entered a tank containing a large amount of MIC, reacted exothermically and increased the temperature and pressure inside the tank, resulting in the release of MIC into the atmosphere. Although multiple factors including poor maintenance, the failure of safety systems, and the missing substandard operating procedure have been identified as the underlying causes of the accident, the accident was

officially blamed on human error as workers did not close the critical isolation valve before pipes were flushed with water and did not shut down the flare (Shrivastava 1992).

The tragic event at Bhopal provides an extreme example of accidents in large-scale technological systems that have been attributed to human error. There are also several other accidents that show the difficulties of operators in working with complex systems or facing data overload. In fact, the majority of these accidents are caused by a combination of many factors which can be found in the lack of human factor considerations, particularly SA which is the most important factor for decision–making (Endsley 1995b; Kaber & Endsley 1998; Niu, Lu & Zhang 2009; Niu et al. 2013). Situation awareness describes how operators in dynamic complex systems develop and maintain a sufficient awareness of 'what is going on' in order to perform tasks successfully. Therefore, SA 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 time stress, and negative consequences associated with poor performance are anticipated (Naderpour, Lu & Zhang 2014b). The analysis of offshore drilling accidents has revealed that more than 40% of such accidents are related to SA, and that the majority of those SA errors (67%) occurred at the perceptual level, 20% concerned comprehension, and 13% arose during projection (Sneddon, Mearns & Flin 2013). Nazir et al. (2012) highlight the importance and significance of SA for Field Operators and Control-Room Operators in the process sector and identify the major factors that influence their SA.

Today in many large-scale technological systems, the automated systems and their over-deployment have changed the nature of operators work. In the past, the systems were analogue and a casual visit to the plant site was sufficient to monitor the progress and production of plants (Nazir et al. 2014). This approach is no longer feasible and operators must stay alert to monitor, assess, and understand the incoming information from various sources and act/react accordingly. The decisions made by operators define the outcomes of possible abnormal situations, near misses, or even accidents. A recent report shows that the

loss of abnormal situations cost 20 billion USD for US process plants every year. Among the attributes triggering these abnormal situations the contribution of human errors has been found to be 50% (Walker et al. 2011).

This chapter highlights the role of the SA factor in three catastrophic accidents in recent US history, and presents certain requirements for developing operator support systems.

3.2 THE ROLE OF SITUATION AWARENESS IN PROCESS ACCIDENTS

Loss of SA, poor SA and lack of SA as identified causal factors are now popular terms in accident investigation reports among several domains including aviation, nuclear industry, power plants, military, and process industry (Salmon & Stanton 2013). Although SA itself is not the only cause of accidents, it plays an important role in operators' decision making in time- and safety-critical situations.

3.2.1 THE EXPLOSION AT INSTITUTE, WEST VIRGINIA

On 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 fire fighters 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 (CSB 2011). Figure 3.1 shows the facility damage and aerial view of reported damaged properties. This case will be investigated further as a case study in Chapter 6.

- **PROCESS DESCRIPTION**

Methyl isocyanate (MIC) is one of the key chemicals used to make methomyl. 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. 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. Distillation separates the solvents in solvent recovery flashers and recycles the solvents to the start of the process. The unvaporized solvents and impurities, including up to 22% methomyl, accumulate in the bottom of the flasher. The residue treater dilutes the incoming flasher bottoms to decompose the methomyl in the flasher bottoms stream to below 0.5% by weight (CSB 2011).

Figure 3.1: Methomyl facility damage and aerial view of reported damaged properties

- **ACCIDENT ANALYSIS**

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 of deviation from the written start-up procedures and included the bypassing of critical safety devices intended to prevent such a condition occurring. In addition, CSB indicates that inadequate Distributed Control System[1] (DCS) checkout and a poor Human-System Interface (HSI) prevented the operators from achieving correct operating conditions and adequate SA. New display screens designed to mimic the process flow incorporated automated icons for critical equipment to show operating status and other parameters, included a mouse user interface, and featured improved HSI. The new control system significantly changed the interactions between the board operators and the DCS interface. It contained features intended to minimize human error such as graphical display screens that simulated process flow and icons to display process variables. However, the increased complexities of the new operating system challenged operators as they had to familiarize themselves with the system and units of measurement for process variables that differed from those in the previous system (Naderpour, Lu & Zhang 2014a).

Human interactions with computers are cognitive. New visual displays and modified command entry methods, such as changing from a keyboard to a mouse, can influence the usability of the HSI and impair human performance (Kaber & Endsley 2004). In this case, it has been expected that the automation of tasks in the control room would help to decrease operators' mental workload, enhance SA, and improve the whole system performance. However, the reality showed that human factor approaches in the modernization of analogue instrumentation and control system of the plant have not been considered sufficiently and appropriately. Further investigation has revealed that the detailed process equipment displays in the DCS were difficult to navigate and routine activities like starting a reaction or troubleshooting alarms would require operators to move between multiple screens to complete a task, which degraded operator awareness and response times. In this case, information was correctly perceived, but its significance or meaning was not

[1] DCS is a dedicated system used to control manufacturing processes; it is connected to sensors and actuators, and uses set point controls to control process variables

comprehended. This error corresponds to level 2 SA errors that might have occurred due to lack of a good mental model, most frequently associated with an automated system. It is also worth noting that the wrong mental model or the mental model of a similar system, i.e. the methomyl unit, might be used to interpret information, leading to an incorrect diagnosis or understanding of the situation. In addition, over-reliance on defaults in the mental models might be another problem. These defaults could be thought of as general expectations about how parts of the system function that might be used in the absence of real time data. In addition, perhaps several pieces of information were not properly integrated because of working memory limitations or other unknown cognitive lapses.

Apart from individual SA errors, another important contributing factor can be related to inadequate SA among night shift and day shift operators. Night shift outside and board operators did not inform the day shift crew that they had started filling the residue treater with flasher bottoms, and the methomyl unit day shift operator neglected to inform the incoming night shift operator that the lab results from the scheduled flasher bottoms sample identified excessively high methomyl concentration. This can be attributed to loss of Distributed SA (DSA) as the lack of communication among the agents, which are different teams in this case, resulted/enabled the accident.

3.2.2 THE EXPLOSION AT BELLWOOD, ILLINOIS

On 14 June 2006, the ignition of a vapour cloud generated by mixing and heating a flammable liquid in an open top tank located in a chemical plant in Bellwood, Illinois, a suburb of Chicago, killed one contractor and injured two employees, and caused a significant business interruption. The accident occurred when an operator was mixing and heating a flammable mixture of heptane and mineral spirits in a 2,200-gallon tank equipped with steam coils. The finished product, "Super Clean and Tilt", is a proprietary mixture which is applied to cured concrete surfaces to prevent bonding with wet concrete (CSB 2007). This case will be investigated further as a case study in Chapter 7.

Figure 3.2: Chemical mixing area damage

- **PROCESS DESCRIPTION**

The process for making Super Clean and Tilt required several hours of mixing and heating. To begin heating, the operator manually opened the steam valves to the tank heating coils and adjusted the temperature controller to maintain the temperature at 73°C. When the batch process was completed, the operator closed the steam valves and allowed the mixture to cool. The mixing tank was not equipped with a temperature display or high temperature alarm, and there was no backup shutoff device. The procedure for this mixture required the operator to verify the temperature by climbing the stairs to the upper level to measure it using a hand-held infrared thermometer, monitor the situation and conducts appropriate actions when necessary (CSB 2007).

On the day of the accident, when the operator was adding an ingredient to the batch, he observed a "dense fog" accumulating on the floor below the tank. He immediately notified a senior operator who helped him shut down the operation. They both exited the building and advised workers in adjoining areas to leave. As the vapour cloud spread throughout the mixing area and surrounding workspaces, other employees exited the building. Within about 10 minutes after the operator first observed the vapour cloud, most employees who were working in the area had evacuated before the cloud ignited. The pressure created by the ignition blew the doors open to an adjacent area, killing a contracted delivery driver

and injuring two employees. The Bellwood Fire Department battled a fire confined to a bagged resin storage area for about three and one-half hours. The fire and pressure from the initial ignition produced moderate damage to the structure and interrupted operations for one month.

- **ACCIDENT ANALYSIS**

The most important contributing factor to the accident was associated with the physical environment, i.e. the temperature controller malfunctioned, that allowed the steam valve to remain open and heat the mixture to its boiling point. In addition, at the basic level, important information i.e. the inside of the tank temperature was not available to the operator, due to a failure of the system design. Furthermore, the system lack of a high temperature alarm, made it difficult for the operator to perceive important information therefore contributed to the operator's reduced SA, resulting in the overflow of vapour from the tank. As the operator was responsible to verify the temperature during the production cycle, another hypothesis is that the information was available via infrared thermometer, but for various reasons, was not observed by the operator. This is due to several factors, including simple omission, attentional narrowing and external distractions that prevent the individuals from attending to important information. High task-load, even momentary, is another factor that prevents important information from being attended to. It is also probable that the operator attended to the temperature, but misperceived due to the influence of prior expectations, i.e. seeing what was expected rather that what was there. Finally, it is possible that the operator initially perceived information then forgot about it due to high workload. In summary, this accident accounts for level 1 SA error, failure to correctly perceive the situation.

3.2.3 THE EXPLOSION AT ONTARIO, CALIFORNIA

On 19 August 2004, an explosion inside an air pollution control device and medical products sterilization chamber at an Ethylene Oxide (EO) sterilization facility in Ontario, California, injured four workers and severely damaged the facility (Figure 3.3).

Neighbouring businesses were evacuated for several hours and operations at the facility were disrupted for nine months (CSB 2006).

Figure 3.3: Ethylene oxide sterilization facility damage

- **PROCESS DESCRIPTION**

Ethylene Oxide possesses an exposure hazard in addition to its high flammability. It kills microbes by disrupting life-sustaining molecules. Cycle variables include EO concentration, duration of exposure, temperature, humidity, vacuum applied during sterilization, and gas washing and aeration required to remove residual EO. Pre-conditioning is the first stage of the medical product sterilization process. It lasts from 6 to 24 hours and involves subjecting products to high levels of humidity, and temperatures between 27 and 49°C. Operators use forklifts to move products to the sterilization chambers. The sterilization process begins by placing pallets of products inside a large stainless steel chamber, applying a vacuum, and injecting pure EO to achieve a sterilizing concentration of approximately 400,000 ppm. At the end of this phase, the chamber gas mixture is evacuated to the acid scrubber that removes EO. Despite efforts to remove all of the EO from sterilized products, potentially toxic levels of EO remain in the chamber after gas washing. To purge this remaining EO, operators open the sterilizer door to approximately six inches, which automatically opens a ventilation duct located in the rear of the chamber. Operators leave the door in this position for several minutes to ventilate the chamber so that employees can safely enter to remove sterilized products. Air exhausted

through the back-vent flows to the oxidizer, which removes the remaining EO from the airstream. After ventilating the chamber, operators completely open the sterilizer door and use forklifts to move products to the aeration rooms. Circulating air in the aeration rooms, also vented to the oxidizer, removes any remaining residual EO (CSB 2006).

The sterilization cycle is monitored and controlled from a computerized process control system located at the west end of the facility. The system automatically controls levels of humidity, temperature, pressure, EO and dwell time. Facility management staff program cycle parameters and event sequencing into the system during the cycle design phase, based on specifications to achieve FDA[1]-mandated sterilization parameters. The system then controls the sequencing of that cycle from start to finish. Taking actions to manually intervene (advance or interrupt) a cycle sequence may present a considerable safety hazard because there is no monitoring or detection equipment to warn employees that an explosive concentration remains in the chamber (Nazir, Kluge & Manca 2014). If an unrecoverable problem occurs during the sterilization cycle, operators can immediately abort the cycle by activating a button located on the control room console. This initiates a pump that removes the high concentration gas from the sterilization chamber, followed by a sequence of gas washes that removes the remaining EO (CSB 2006).

- **ACCIDENT TIMELINE**

On the day of the accident, at approximately 1:30, the control system alerted operators of an EO injection failure during a cycle in Chamber 7. The operator immediately ran several routine system checks in the control room to determine that the alert was accurate, but was unable to identify any problems. The supervisor then decided to abort the cycle. In accordance with company protocol, they used the cycle abort button on the control room console. Upon completion of the abort cycle, operators removed the chamber contents to an aeration room, and the chamber was left open awaiting maintenance personnel. The maintenance supervisor arrived at the plant at approximately 7:30 and immediately assigned

[1] Food and Drug Administration

two technicians to work on the gas injection problem. He allowed maintenance personnel to enter a password to override computer safeguards, resulting in premature opening of the sterilizer door. Soon after that, the lower explosion limit alarm in the chamber was triggered, indicating the release of EO. The ignition of EO-air mixture took place before the oxidizer could be shut down (CSB 2006).

- **ACCIDENT ANALYSIS**

A deeper look into the events reveals that the operators had difficulties in understanding the behaviour and limitations of the automated system, which thus induced incorrect assumptions and led to wrong actions. The automation failure combined with operators' incorrect SA resulted in the accident. A further drawback of improperly designed automated systems is the progressive reduction of process understanding by the operators as they spend more time in passive vigilance instead of taking active decisions/actions. Consequently, they are unable to perform correctly when the system calls for unconventional and even manual actions under abnormal situations (Nazir, Kluge & Manca 2014). As a matter of fact, this particular accident resulted because of the loss of SA levels 2 and 3 of the operators. They were unable to identify the source of the problem and were not aware of the possible consequences of their decisions. In some cases, individuals may be fully aware of what is going on, but be unable to correctly project what that means for the future. This could be due to a poor mental model or due to over-projecting current trends. Generally, mental projection is a very demanding task at which people are poor. The CSB report also explicitly suggests that the training methods were inadequately designed and the job-specific maintenance-training was completely missed.

3.3 PROMOTING OPERATORS' SITUATION AWARENESS

Promoting SA is now an important design objective for safety-critical systems which employ digital instrumentation, control systems and computer-based HSIs. In their operations, operators need a greater level of support to control and maintain the facilities in safe condition due to an increasing amount of information that is passed to them through

automated systems. In fact, operators have to face both data overload and the challenge of working with a complex system. They are drilled with long lists of procedures and checklists designed to cope with some of these difficulties, but from time to time they are apt to fail. Operators generally have no difficulty in performing their tasks physically, and no difficulty in knowing what is the correct thing to do, but they are stressed by the task of understanding what is going on in the situations, particularly when they are confronted with abnormal situations (Burkolter & Kluge 2012; Naderpour, Lu & Kerre 2011).

Traditionally, there are two approaches to prevent human error during operation of safety-critical systems that are aimed at the provision of better training programs for operators, and the improvement of operator support systems (Lee & Seong 2014). However, it has been shown that in abnormal time pressure situations, ordinary training does not improve the quality of decision making (Zakay & Wooler 1984), therefore the role of cognitive support systems to assist operators in such situations is highlighted.

Usually, large-scale technological systems contain multilevel control loops and interconnections, which need to be monitored and supervised for normal operations. Once the system becomes unstable, the conditions are referred to as an abnormal situation, which can lead to near misses and possible accidents with both economic and human loss. In the last two decades, the technological systems have experienced a significant increase in multidimensional automation that has significantly increased the complexity and sensitivity of the role of operators and their teams. However, the operators lack of ability to intervene or tackle abnormal situations as they are usually designed for routine operating conditions (Nazir, Kluge & Manca 2014). Therefore, any attempt to develop operator support systems should consider both normal and abnormal situations.

Generally, operators perform two types of tasks to carry out their roles and responsibilities: Primary tasks and Secondary tasks. As illustrated in Figure 3.4, primary tasks consist of several cognitive tasks including monitoring and detection, situation assessment, response planning, and response implementation (O'Hara & Persensky 2011). Any

breakdown in generic primary tasks can lead to a human error. Therefore, a balanced automated system that avoids an excessive workload for the operators and keeps them in the loop of decision-making, taking action, and updating the related information would benefit the process industry. The activities involved in extracting information from the environment are referred to monitoring and detection. In current systems, this task is highly supported through various heterogeneous sensors and appropriate signal-processing methods that are used to extract as much information as possible about the dynamic environment. Good monitoring results in operators' perception or SA level 1.

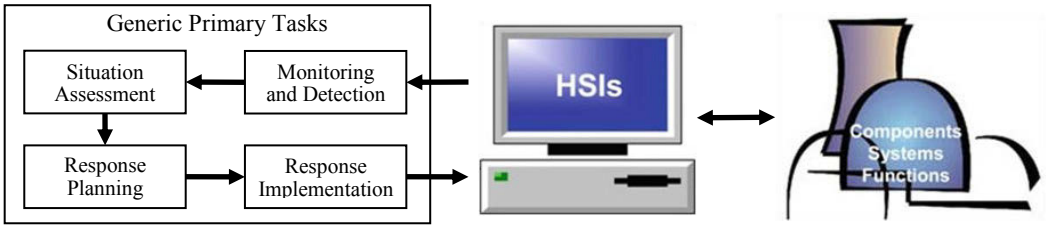


Figure 3.4: General primary tasks

Situation assessment is the evaluation of current conditions to determine that they are acceptable or to determine the underlying causes of abnormalities. Situation assessment which underlies the achievement of SA is therefore critical to taking proper human action. Thus, the HSI besides providing alarms and displays that are used to obtain information to support situation assessment must provide additional support for assessing the situation. This development corresponds to SA levels 2 and 3 that support operators to infer real situations and to project their status in the near future.

Response planning refers to deciding upon a course of action to address the current situation. In general, response planning involves operators using their situation model to identify goal states and the transformations required to achieve them.

Response implementation is performing the actions specified by response planning. These actions include selecting a control, providing control input, and monitoring the system and process response (O'Hara & Persensky 2011).

Apart from primary tasks, operators perform other kinds of tasks that are referred to as secondary tasks or "interface management tasks" such as navigating, configuring and arranging that assist operators to perform the primary tasks successfully. Secondary tasks create workload and may take much attention away from the primary task performance and generate a "keyhole effect" (Seong 2009) thus affecting operators' SA, which makes the operator out-of-the-loop. Thus, secondary tasks should be carefully addressed in design reviews as well.

In actual plant operation, individual operators typically do not perform these tasks alone; tasks are accomplished by the coordinated activity of multi-person teams. Therefore, the design of technology needs to consider not only individual performance but also team performance.

3.4 SUMMARY

Many attempts were made over the past 20 years to reduce human error in safety-critical systems such as process plants. The main conclusion is that few errors represent random events; instead, most human errors can be explained by human cognitive mechanisms. Among cognitive mechanisms, operators' SA is the most important pre-requisite for decision–making, especially in time-, safety-critical abnormal situations. Today, in control rooms, operators are supposed to manage large amounts of data, and deal with process details, control systems, set points and the delicate balance between safety and production. During the failure of automated systems and under abnormal situations, the urgency and sensitivity of decisions increase manifold. Effective solutions need to go beyond the delivery of more data and advanced technology for the operator. Establishing effective operations practices that enable high individual and distributed SA are important to effectively preventing and responding to abnormal situations and improving process safety performance. Therefore, the goals and activities of interactive systems should be well designed to support operators' SA and also should be optimized for abnormal situations.

This chapter reviews the role of SA in three accidents in the process sector and analysed the SA related errors. It also highlights the urgent need to discover cognitive support systems to manage abnormal situations in order to lower operator workload and stress and consequently human errors. In addition, as different bits of information are distributed among several operators/supervisors, artefacts, and technological tools, the implication of team SA, shared SA, or distributed SA are also highlighted.

Chapter 4:

AN ABNORMAL SITUATION MODELLING METHOD

4.1 INTRODUCTION

In abnormal situations, a well-trained operator should comprehend a malfunction in real time by analyzing alarms, assessing values, and recognizing unusual trends indicated by multiple instruments. In such a situation, many alarms from different systems are frequently triggered at the same time, making it difficult for the operator to make a decision within a very short time frame. If several abnormal situations occur at once, decisions have to be made in even less time. Operators are usually unable to judge which situation should be given priority when confronted with complex abnormal situations such as these (Hsieh et al. 2012; Jou et al. 2011). To return operational units to normal conditions, operators must respond quickly and make rapid decisions, but under these circumstances, the mental workload of operators rises sharply, and a mental workload that is too high may increase the rate of error.

When an abnormal situation occurs in a safety-critical system, operators firstly recognize it by an alarm, and secondly, need to perform a situation assessment which means that they try to understand what is happening in the plant. 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 & Seong 2006a).

In the context of automation systems, an operator's mental model will be greatly influenced by the system design being employed especially now since they are physically removed from the process. The visible aspects of the system, the actions that seem approachable and prior experience of the operator together form the mental model of how the process works. The degree to which the operator's mental model accurately reflects how the process truly does work has a significant effect on the operator's ability to use the automation system (Pridmore 2007).

This chapter provides the concept of mental models in Section 4.2, presents a new abnormal situation definition based on risk in Section 4.3, and develops an abnormal situation modelling (ASM) method in Section 4.4 based on this assumption that the operator's mental model can be modelled using BNs as a representation of static cause–effect relationships between objects in the situation. Section 4.5 reviews the sensitivity analysis for evaluating situation models.

4.2 Situation Awareness and Mental Models

Mental models refer to mechanisms whereby humans are able to generate descriptions of system purpose and explanations of system functioning (Endsley 2000b). Mental models embody stored long-term knowledge about the systems that can be called upon interaction with the relevant system when needed. These internally developed models aid in efficiently directing limited attention. They provide a way to integrate information without overloading working memory. The use of mental models in achieving SA is believed to be dependent on the individual's ability to pattern match critical cues in the environment with elements in their mental model, and being able to incorporate the use of these models into SA can provide the operator with quick retrieval of actions from memory (Pridmore 2007).

The concept of mental models has a very long tradition in applied cognition. It has often been used in studies trying to model, amongst others, human control of various processes. Rouse and Morris (1986) define mental models as "mechanisms whereby humans are able to generate descriptions of system purpose and form, explanations of system functioning and observed system states, and predictions of future states". They believe that mental models are multi-purpose mental devices. The three basic functions: (1) Description of system and form (2) Explanation of system functioning and observed system states and (3) Predictions of future system state, are all compatible with the three-level SA model. However, they believe that mental models are not a state but are sets of processes. Endsley's representations provide a context for some form of judgment and contribute to SA in the form of references to prior experience. Her approach presents mental models as default information that helps to form higher levels of SA even when needed data is missing or incomplete. Features in the environment are mapped to mental models in the operator's mind, and the models facilitate the development of SA. Mental models (formed by training and experience) are used to facilitate the achievement of SA by directing attention to critical elements in the environment (level 1), integrating the elements to aid understanding of their meaning (level 2) and generating possible future states and events (level 3) (Salmon et al. 2008).

As shown in Figure 4.1, a situation model can be developed not only by observing the world, but also is influenced by underlying mental models that the operator has. These mental models can help to determine what information is attended to, how that information is interpreted and integrated, and what projections are made about what will happen to the system in the near future. In this sense, the situation model is the current instantiation of the mental model which is more general in nature (Endsley 2000b). Therefore, it can be concluded that the situation model provides a useful window on the broader mental model. For example, an engineer may perceive several dynamics in the flow lines (considered to be important elements per the mental model) recognized as hydrate

forming conditions based on critical cues (perception). By pattern-matching to prototypes in memory, these separate pieces of information may be classified as a particular recognized hydrate formation (comprehension). According to an internally held mental model, the engineer is able to generate probable scenarios for this type of condition (projection). Based on this high-level SA, the engineer is then able to select suitable actions that will prevent their formation.

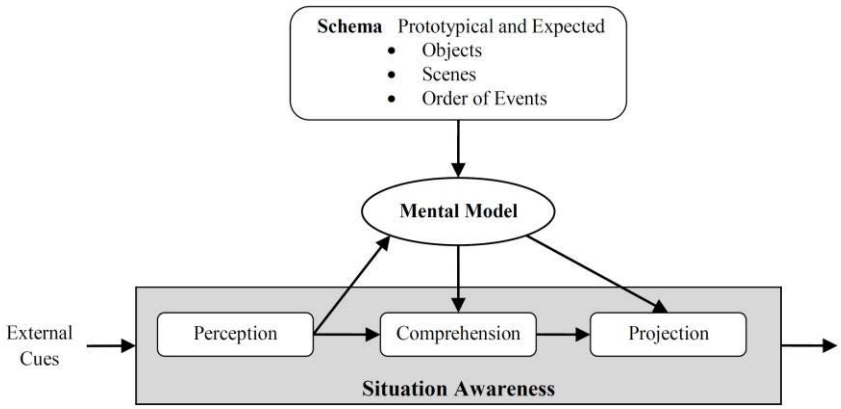


Figure 4.1: Relationship between situation awareness and mental models

4.3 ABNORMAL SITUATION DEFINITION

A situation is defined as a set of circumstance in which a number of objects may have relationships with one another and the environment. Any variety of relations – physical, organizational, informational, and perceptual – can be considered as being appropriate to the given information system's mission. Figure 4.2 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 (Kokar, Matheus & Baclawski 2009).

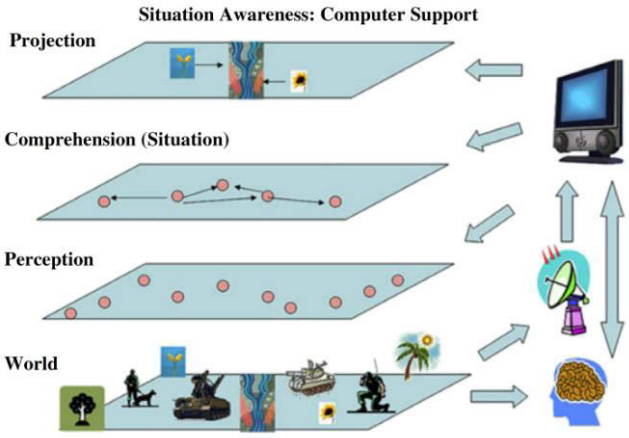


Figure 4.2: Situation and situation awareness

Based on above description, a hazardous situation is defined as a possible circumstance immediately before harm is produced by a hazard. Therefore, an abnormal situation is defined as a hazardous situation if its risk is not acceptable. The hazardous situations are categorized in two groups based on contributing objects:

- Independent situations: A hazardous situation is an independent situation if only its objects and their interactions create a hazardous condition;
- Dependent situations: A hazardous situation is a dependent situation if its objects and their interactions with other situations create a hazardous condition.

4.4 ABNORMAL SITUATION MODELLING

Mental models are a type of tacit knowledge which can be elicited from people's minds using cognitive mapping methods. This research applies BNs for this purpose and presents the ASM method as illustrated in Figure 4.3, which contains several steps that are explained as follows:

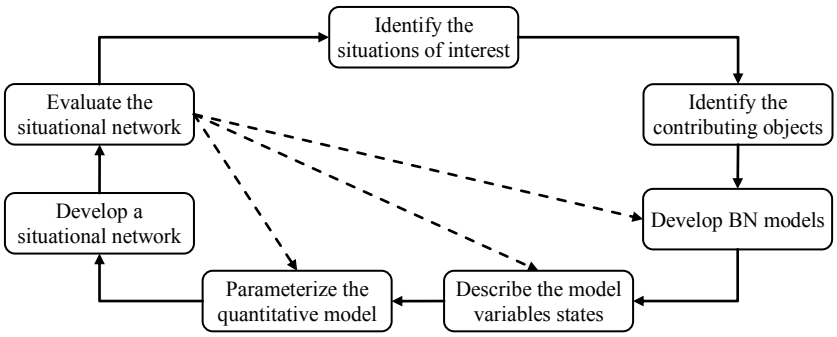


Figure 4.3: A cycle to describe the ASM method

Step 1: Identify the situations of interest: To find 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. The identified situations should have clear operational meaning to the modeller, the domain experts and the users. Where possible, this process should be undertaken in a participatory environment to ensure that the breadth of issues and potential inputs to the models are identified.

Step 2: Identify the contributing objects: The contributing objects (both physical and conceptual) can be obtained through several methods. In many areas, hazardous situations are obtained through the design and implementation phases, and various models are developed to identify their contributing objects. For example, HAZOP is one of the most powerful methods available and has been well

described in the literature, and fault tree, event tree, and bow-tie can be adopted as knowledge acquisition techniques which can provide proper materials to determine the contributing objects (Naderpour & Lu 2012a).

Step 3: Develop BN models: 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 between the root nodes and the pivot node define the relationships between the objects. The leaf nodes may be safety barriers that are physical objects in the environment that will connect to one another if there is a relationship between their performances. In addition, one of the leaf nodes may be a consequence node that has some states, and shows the possible accidents in this situation. If the situation is inferred by one or more observable variables, the focal object is connected to the observable variables. Figure 4.4 shows the situation *A* where the node *A* is focal and other nodes are related to it. There may be several situations that 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. Their existence in the next time-point has to be verified again.

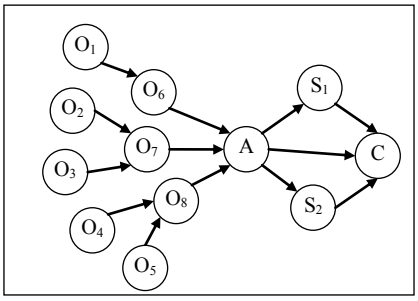


Figure 4.4: **A static situation model**

Step 4: Describe the states of model variables: 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 node, which delegates the situation, 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. Indeed, such an occurrence may lead to a wide range of consequences, some of which will probably be undesirable events. 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 set or a fuzzy set. As the concept of fuzzy set theory can provide a smoother structured means, the states of observable variables are determined using a fuzzy partitioning method and fuzzy states definition that be elaborated in the next chapter.

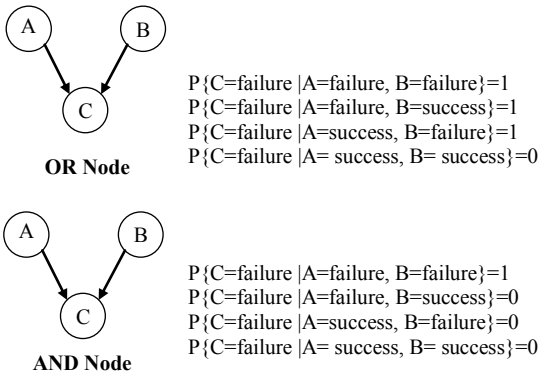


Figure 4.5: **The OR and AND gates in BN representation**

Step 5: Parameterize the quantitative model: 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 focal nodes are set based on the "OR gate" or "AND gate" definition, as described in (Bobbio et al.

2001) and represented in Figure 4.5. The CPTs of observable variables are determined by domain experts. The elicitation process is carried out with the recursive technique (e.g. Delphi method) to guarantee the convergence of the results. The final results are commented on and adjusted again during further interviews (Li et al. 2012). The CPTs of consequence nodes are determined by 0 and 1 values corresponding to appropriate states.

Step 6: Develop a situational network: Several situations can exist in parallel, or the existence of one situation can exclude the existence of another situation. Figure 4.6 shows an example network of situations. As can be seen, the situations A and B can be inferred directly from objects O_1, O_2 and O_3 while the existence of situations C and D are dependent on the existence of lower level situations. The temporal dependencies are illustrated by dashed lines. The complete modelling of the dependencies results in a network of situations. As a result of this modelling, 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.

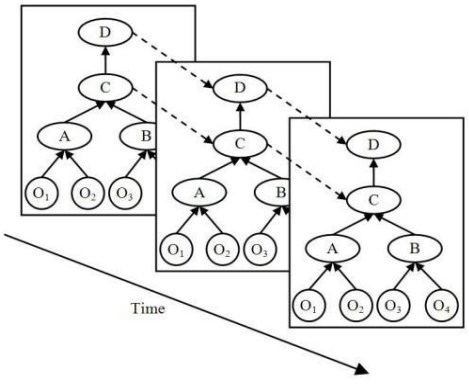


Figure 4.6: A dynamic situational network

Step 7: Evaluate the situational network: Evaluation of the situational network requires the assessment of model behaviour to ensure that the model demonstrates acceptable behaviour. The evaluation can be undertaken at several levels. The first level is to ensure that key objects and their relationships have been represented in the network, and the second level should review the determined states to ensure that they have been defined unambiguously. The third level considers evaluating the model performance by conducting some validation methods as well as by testing how the model behaves when analyzing well-known scenarios.

There are three evaluation methods to validate the performance of a BN: sensitivity analysis, data-based evaluation and non-quantitative evaluation of model outputs using experts. The next section presents the sensitivity analysis in detail.

4.5 SITUATION MODELS EVALUATION

In the event that large data sets are not available, and the probabilities must be elicited from domain experts, the sensitivity analysis technique is often used to investigate the effect of probability parameter changes on the performance of BNs. This analysis investigates the influence of variation in the model inputs on outcomes, where inputs can be real inputs (i.e. values of observable nodes) or the parameters (i.e. values of conditional probabilities). The output of sensitivity analysis requires evaluation by experts (Pollino et al. 2007).

Sensitivity to findings based on the 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:

$$H(X) = -\sum_{x \in X} P(x)\ log\ P(x) \quad (4.1)$$

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

$$I(X,Y) = H(X) - H(X|Y) \quad (4.2)$$

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 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 & 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):

$$f(x) = \frac{\alpha x + \beta}{\gamma x + \delta} \quad (4.3)$$

where $\alpha, \beta, \gamma, \delta \in \mathbb{R}$ and they are constants built from parameters which 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):

$$f'(x) = \frac{\alpha\delta - \beta\gamma}{(\gamma x + \delta)^2} \quad (4.4)$$

In some cases, finding parameter changes that satisfy constraints on probabilistic queries are required. The most common types of query constraints, given some value k are:

$$P(y|e) \geq k \quad (4.5)$$

$$P(y|e) \leq k \quad (4.6)$$

$$P(y|e) - P(z|e) \geq k \quad (4.7)$$

$$\frac{P(y|e)}{P(z|e)} \geq k \quad (4.8)$$

where evidence e is an instantiation of variables E, and events y and z are values of the variables Y and Z respectively. For example, if event y is more likely than event z given evidence e, then it can be specified the constraint $P(y|e) - P(z|e) \geq 0$. Also it is possible to make event y at least twice as likely as event z, given evidence e by specifying the constraint $P(y|e)/P(z|e) \geq 2$. For a binary variable X with two values x and $\bar{x}$, there are two parameters $\theta_{x|u}$ and $\theta_{\bar{x}|u}$ for every parent instantiation u. Consider $\tau_{x|u}$ as a meta-parameter and assigne $\theta_{x|u} = \tau_{x|u}$, therefore the goal is to determine the amount of change that must be applied to $\tau_{x|u}$ which would load to complementary changes in $\theta_{x|u}$ and $\theta_{\bar{x}|u}$ that can enforce the query constraint. To satisfy Inequalities 4.5 to 4.8, $\tau_{x|u}$ should be respectively changed by $\Delta\tau_{x|u}$ such that:

$$p(y,e) - k.p(e) \geq \Delta\tau_{x|u}(\pi_{x|u}^{y,e} + k.\pi_{x|u}^{e}) \quad (4.9)$$

$$p(y,e) - k.p(e) \leq \Delta\tau_{x|u}(-\pi_{x|u}^{y,e} + k.\pi_{x|u}^{e}) \quad (4.10)$$

$$p(y,e) - p(z,e) - k.p(e) \geq \Delta\tau_{x|u}(-\pi_{x|u}^{y,e} + \pi_{x|u}^{z,e} + k.\pi_{x|u}^{e}) \quad (4.11)$$

$$p(y,e) - k.p(z,e) \geq \Delta\tau_{x|u}(-\pi_{x|u}^{y,e} + k.\pi_{x|u}^{z,e}) \quad (4.12)$$

where $p(e)$ and $p(y,e)$ are the current probabilities of e and (y,e) and the constants $\pi_{x|u}^{e}$ is defined as follows (Chan 2005):

$$\pi_{x|u}^{e} = \frac{\partial P(e)}{\partial \tau_{x|u}} = \frac{P(e,x,u)}{\theta_{x|u}} - \frac{P(e,\bar{x},u)}{\theta_{\bar{x}|u}} \quad (4.13)$$

and $\pi_{x|u}^{y,e}$, as well as $\pi_{x|u}^{z,e}$ when applicable, are crucial to the procedure of finding the necessary change in $\tau_{x|u}$ to enforce the query constraint (Chan 2005). The solutions of $\Delta\tau_{x|u}$ in Inequalities 10 to 14 are always in one of the following forms:

- $\Delta\tau_{x|u} \leq \delta$, for some computed $\delta < 0$, in which case the new value of $\tau_{x|u}$ must be in the interval $[0, p + \delta]$ where p is the current value of $\tau_{x|u}$.
- $\Delta\tau_{x|u} \geq \delta$, for some computed $\delta < 0$, in which case the new value of $\tau_{x|u}$ must be in the interval $[p + \delta, 1]$ where p is the current value of $\tau_{x|u}$.

Therefore, δ is the minimum amount of change in $\tau_{x|u}$ that can enforce the query constraint. The proof of above results can be found in (Chan 2005) as well as extended binary variable X to a multi-valued variable.

4.6 SUMMARY

The lack of an accurate mental model can cause the operator a lack of understanding, in turn making the automation system harder to use (Pridmore 2007). This increases the cognitive effort required to accomplish a task or to project future events. With experience, an operator might be able to overcome the effects of the automation system with a poorly designed mental model. Designing based on a mental model concept could be helpful in that it offers a method for directing attention to important aspects of the situation and promoting understanding of the relationships within the process.

This chapter introduces an abnormal situation modelling (ASM) method that tries to represent operators' mental models in regard to abnormal situations. The ASM method models the operators' mental model using BNs to represent these cause–effect relationships between objects in a situation. It also describes how the states and CPTs of objects in the models should be determined, and how they should be connected to each other to create the situational networks. As the situations of interest can be inferred by some observable variable distributed in the environment, the ASM method explains how the situations can be connected to observable variables.

The ASM method is reasonable as it provides a basis for modelling the situations that might be inclusive, it enables the understanding of situations by providing the contributing objects, and it provides the projection of future situations or events. It also has a limitation as in the developing of situation models, some data are collected from experts; therefore some uncertainty associated with the probability distributions is unavoidable.

Chapter 5:

AN INTELLIGENT SITUATION AWARENESS SUPPORT SYSTEM

5.1 INTRODUCTION

Maintaining a complex and dynamic system in safe conditions, 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. The key focus must be on keeping the human operator aware of the situation, showing the risk level of hazardous situations and providing the base to reduce risks until they reach a level that is ALARP. Previous researches in the field of system safety have only considered developing scenarios for specific undesirable events from an engineering perspective, whereas in today's safety-critical systems, operators face several hazardous situations from different sub-systems which dynamically threaten the system, and they have to comprehend both the current state and the near future state to make correct decisions. A human-centric system is therefore needed to support operators in understanding and assessing the current state of an abnormal situation and to assist them to take appropriate actions. This chapter presents the SA requirements for such system and develops the situation awareness support system (SASS).

5.2 THE GOAL OF SASS

The ALARP principle, which is now widely applied in safety decision-making, requires that those responsible for safety in the workplace- and, indeed, public safety-should reduce risks to levels that are "As Low As Reasonably Practicable". As such, the principle involves effective recognition of the fact that, while in most circumstances risk can be reduced, beyond some point further risk-reduction is increasingly costly to implement. In the UK, the ALARP principle is specified as a regulatory requirement by the Health and Safety at Work Act 1974 (HSWA) following recommendations set out in the Robens Report on Safety and Health at Work in 1972. In fact the HSWA refers to the principle as 'So Far As Is Reasonably Practicable' (SFAIRP), but in practice this is treated as being synonymous with ALARP, as is the term 'As Low As Reasonably Achievable' (ALARA) which is used in some other contexts, particularly in the USA (Jones-Lee & Aven 2011).

Conceptually the ALARP approach can be illustrated as in Figure 5.1. This shows an upper limit of risk that can be tolerated in any circumstances and a lower limit below which risk is of no practical interest. Indicative numbers for risks are shown only for illustration and the precise values are not central to the discussion herein but can be found in relevant country-specific documentation. The ALARP approach requires that risks between these two limits must be reduced to a level "as low as reasonably practicable". In relevant regulations it is usually required that a detailed justification be given for what is considered by the applicant to satisfy this "criterion" (Melchers 2001).

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) (Melchers 2001). Therefore, the main goal of the system is to eliminate the risk or reduce it to an acceptable level. The main goal is supported by two sub-goals: risk determination and risk reduction.

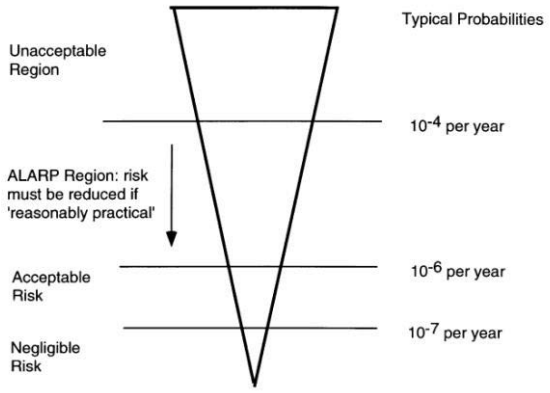


Figure 5.1: **Levels of risk and ALARP based on UK experience**

5.3 THE REQUIREMENTS OF SASS

The SASS requirements are determined by GDTA. 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 as shown in Table 5.1.

Table 5.1: **Safety goals**, **decisions and SA requirement**.

Goal: **Eliminate or reduce the risks to a level that is as low as reasonably practicable**
Sub-goal 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*
Sub-goal 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 abnormal situation*
• *L3: Projecting the new probability of the abnormal situation*
• *L3: New level of risk*

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

5.4 THE FRAMEWORK OF SASS

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 SCADA[1] monitoring system, and how the risk of situations can be reduced to an acceptable level. The system's proposed framework is shown in Figure 5.2. 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.

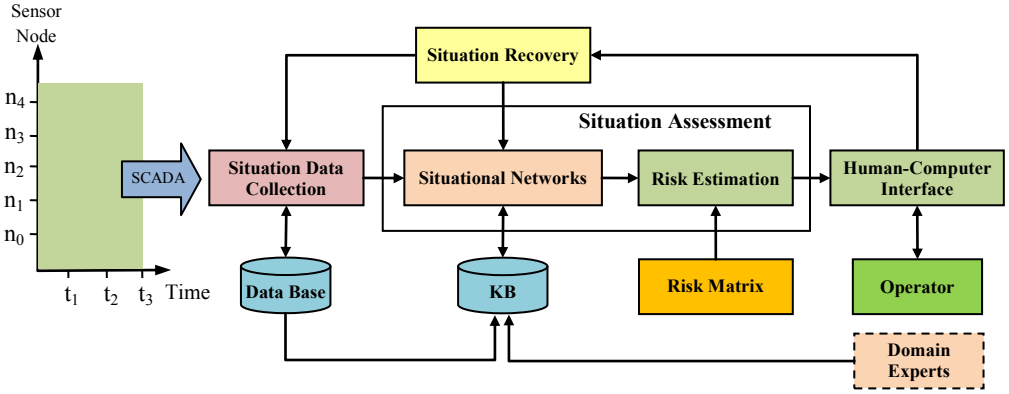


Figure 5.2: The framework of the situation awareness support system

5.4.1 THE KNOWLEDGE-BASE

The knowledge-base contains the situation models of the intended safety-critical environment developed according to the ASM method presented in Chapter 4. As explained, analysis of written materials, observation of operator performance, expert elicitation and formal questionnaires would help with knowledge-base design and establishment. The knowledge-base is verified in a participatory environment to ensure that the breadth of issues is identified. A complete determination and modelling of situations of interest covers the SA requirements which are necessary for Decision 1-1 in Table 5.1.

[1] Supervisory Control and Data Acquisition

5.4.2 THE SITUATION DATA COLLECTION COMPONENT

The situation data collection component provides the current state of the observable variables, which is 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 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 labelled 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 5.3 shows a fuzzy partition, but non-symmetric fuzzy sets or sets with a different shape can be used.

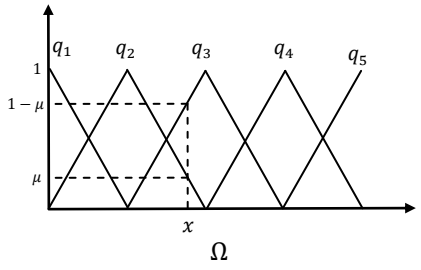


Figure 5.3: A fuzzy partition

If x is a value of a variable X occurring on a domain partitioned as in Figure 5.3, 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 1 (Fuzzy partition): A fuzzy partition on the universe Ω is a set of fuzzy sets $\{q_1, q_2, \dots, q_m\}$ such that:

$$\forall x \in \Omega, \ \sum_{i=1}^{m} \mu_{q_i}(x) = 1 \quad (5.1)$$

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

Definition 2 (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:

$$q_i = \{\mu_{q_i}(x) | x \in \Omega\} \quad (5.2)$$

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 $i = 1, \dots, n$ 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 $(j = 1, \dots, m)$ as hypotheses that X_i is in fuzzy state q_j . The results of membership functions $\mu_{q_j}(x)$ $j = 1, \dots, m$ form the soft evidence vector:

$$e = \{\mu_{q_1}(x), \mu_{q_2}(x), \dots, \mu_{q_m}(x)\} \quad (5.3)$$

The $\mu_{q_j}(x)$ is considered to be approximately equivalent to the condition probability $P(q_j|X_i = x)$ (Chai & Wang 2011).

Table 5.2 gives an example showing the temperature limits for a chemical plant involving two reactors and two distillation columns, including the limits for the six-sigma quality, high alarm and automatic shut-down (Naderpour & Lu 2012a).

Table 5.2: Temperature limits of a chemical plant

Unit	Operating value	Six-sigma quality	High alarm	Automatic shutdown
Reactor 1	160	165	170	180
Reactor 2	166	170	175	185
Distillation 1	186	190	195	200
Distillation 2	200	205	210	220

Note: Temperatures are in °C

The temperature continuous variable of Reactor 1 in terms of operation can be partitioned by fuzzy mapping into the fuzzy states including Low, Normal and High, and the membership function is defined as follows, as well as being shown in Figure 5.4:

$$\mu_{T(L)}(x) = \begin{cases} 1 & 0 \le x \le t_1 \\ (t_2 - x)/(t_2 - t_1) & t_1 < x \le t_2 \\ 0 & x > t_2 \end{cases} \quad (5.4)$$

$$\mu_{T(N)}(x) = \begin{cases} 0 & 0 \le x < t_1 \\ (x - t_1)/(t_2 - t_1) & t_1 \le x < t_2 \\ (t_3 - x)/(t_3 - t_2) & t_2 \le x < t_3 \\ 0 & x \ge t_3 \end{cases} \quad (5.5)$$

$$\mu_{T(H)}(x) = \begin{cases} 0 & 0 \le x < t_2 \\ (x - t_2)/(t_3 - t_2) & t_2 \le x < t_3 \\ 1 & x \ge t_3 \end{cases} \quad (5.6)$$

where t_1=155°C, t_2=160°C and t_3=165°C, and $\mu_{T(L)}(x)$, $\mu_{T(N)}(x)$ and $\mu_{T(H)}(x)$ denote the membership function of fuzzy states Low, Normal and High respectively. At time *T*, the temperature inside the Reactor 1 is reported 164°C therefore the soft evidence vector will be: e={Low=0 , Normal=0.2 , High=0.8}.

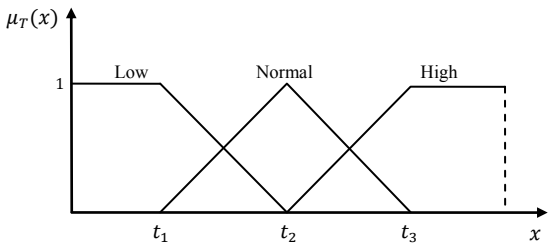


Figure 5.4: The membership function of Reactor 1 temperature

5.4.3 THE SITUATION ASSESSMENT COMPONENT

Mathematically, a situation at time *t* can be modelled using a subset $\tilde{\sigma}$ of the configuration space as a statement, which is either hazardous or safe:

$$S_t = \begin{cases} Hazardous & if\ R(S_t) > Risk\ Criteria \\ Safe & if\ R(S_t) \leq Risk\ Criteria \end{cases} \quad (5.7)$$

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

$$R(S_t) = P(S_t) * S(S_t) \quad (5.8)$$

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

$$P(S_t) \coloneqq P(S_t | o_1, o_2, \dots, o_m)\ with\ o_1, o_2, \dots, o_m \in \tilde{\sigma} \quad (5.9)$$

and $S(S_t)$ is the severity of the situation. As a result of this modelling, 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.

Usually, well trained operators are able to form rules for every situation to assess their risks, 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 vapour 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 vapour is increasing, the occurrence of an explosion is possible'. In this sense, it is assumed that the operator's mental model can be tailored using the rules for the hazardous situations of the 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 analyse situations behaviour based on operators' thinking, the situation assessment component needs to generate an assessment level of risk for every situation over time. The results of this assessment are necessary for the subsequent component, 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 process including the following steps is utilized:

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

5.4.3.1 THE SITUATION PROBABILITY ESTIMATION

The DBN-based situational networks provide the prior and posterior probabilities (Decision 1-2 in Table 5.1). The quantitative analysis can be achieved by two methods: the forward method (or probability prediction) and the backward method (or probability diagnosis). Both probability prediction and probability diagnosis are used for this analysis. In predictive analysis, conditional probabilities of the form $P(S_t|V_t^s)$ are calculated, indicating the occurrence probability of situation S_t at time t, given current value of observable variable V_t^s. In diagnostic analysis, conditional probabilities of the form $P(O_i^s|S_t)$ are evaluated, showing the occurrence probability of a particular object O_i^s given the occurrence of situation S_t. It can also be conducted to find the most probable explanation (MPE) of the states of the objects leading to abnormal situations or specific consequences.

5.4.3.2 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 (Hessami 2010).

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 (Hessami 2010).

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 5.3 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 5.1).

Table 5.3: 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-1million	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

5.4.3.3 THE SITUATION RISK ESTIMATION

To estimate the risk level of a situation, a fuzzy logic system (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 can be defined using failure mode and effect analysis (FMEA) tool. However, in this study the membership functions as shown in Figure 5.5 are defined as a combination of trapezoidal and triangular numbers to simplify the operation and increase the sensitivity in a number of bounds (Pedrycz 1994). The α level cuts "1" and "0" are used to describe the fuzzy sets for each variable as explained in Table 5.5. To achieve this, 25 rules in terms of linguistic variables elicited from operators and shown in Table 5.4, are developed. For example, IF $P(S_t)$ is Even AND $S(S_t)$ is Major THEN $R(S_t)$ is Not acceptable. To generate the output, Mamdani's fuzzy inference method is used to implicate each single rule and aggregate the outcome from all rules into a single output fuzzy set (Mamdani 1977). 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 5.1).

Table 5.4: Operator's rules for assessing situations

Probability	**Severity**				
	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

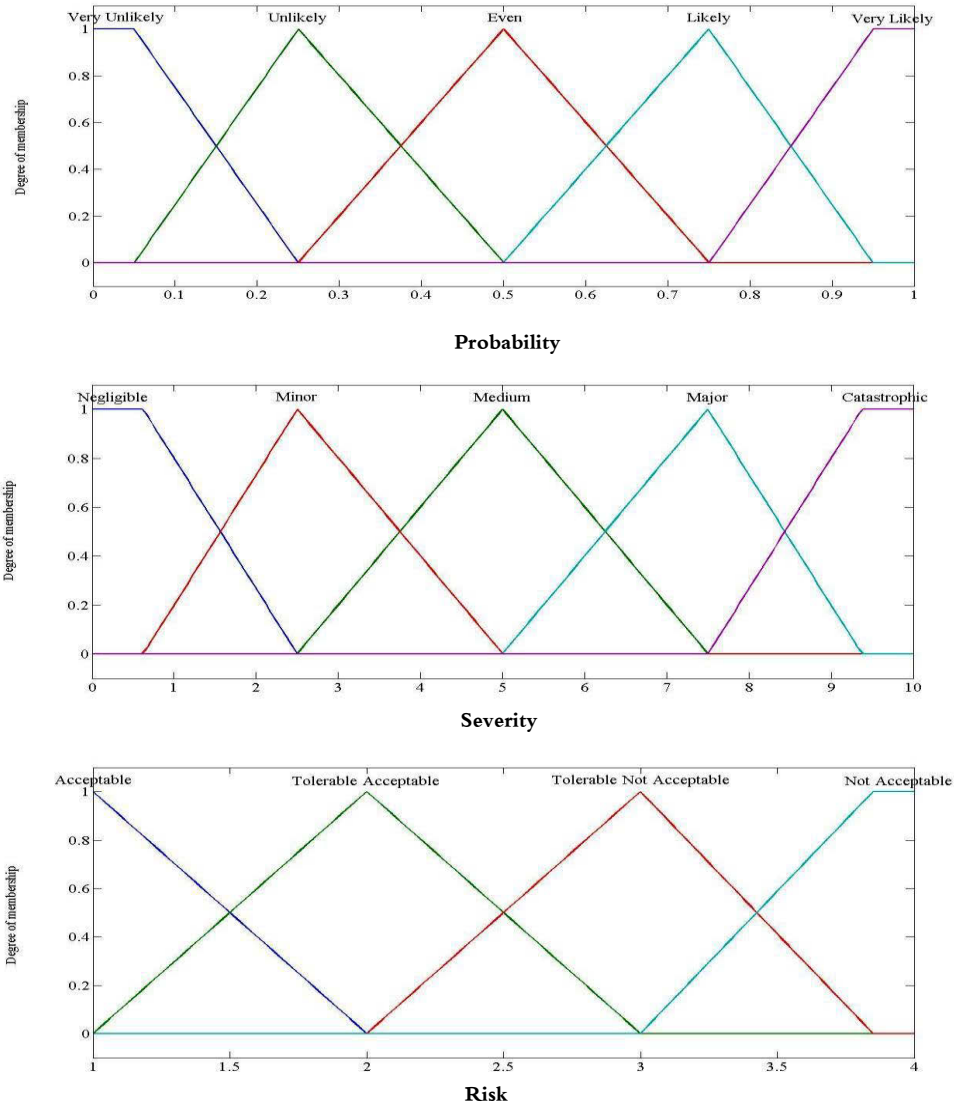


Figure 5.5: Membership functions of probability, severity, and risk

Table 5.5: Fuzzification of input and output variables

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

5.4.4 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 situational network does not provide the risk reduction measures; it provides the most probable explanation for the given abnormal situation that can be used for making appropriate maintenance decisions, and 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 5.1). 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 5.1). The aim is to eliminate or reduce the risk level of situations to an acceptable level.

5.4.5 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 Modelling, Inference, and Learning Engine), which is a library of C++ classes for implementing BNs in intelligent systems (Laboratory 1998). 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 (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.

5.5 Comparison with other Studies and Limitations

To date, several BN-based situation assessment methods have been proposed in the literature. This section compares the SASS with another study conducted by Kim and Seong (2006a). The differences between the two researches 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 this study is clearly defined, and a situation modelling 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 modelled 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 thesis, 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 this research, 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 (its risk level is unacceptable), and to help operators to understand the hierarchy of investigations (a situation with a higher risk has priority over other situations to be investigated).
- The authors provide no evaluation method for the KS method. This study 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 a multi-perspective evaluation approach based on SA measures is developed in Chapter 8 for the full evaluation of the SASS.

The proposed SASS is anticipated to provide adequate 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 behaviour 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 (Kim & Seong 2006a). 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.

5.6 SUMMARY

During abnormal situations, many alarms from different systems are usually triggered at the same time, making it difficult for the operator to make a decision within a very short period of time. Operators are frequently unable to judge which situation should be given priority in a short timeframe, when confronted with complex abnormal situations. Under these circumstances, the mental workload of operators rises sharply and too high mental workload possibly increases their error rate (Hsieh et al. 2012; Jou et al. 2011). Therefore, a system is needed to support operators' SA in understanding and assessing the situation and to assist them to take appropriate actions.

This chapter defines the goal of the support system based on ALARP, and presents a set of requirements based on GDTA methodology for the development of the SASS to help operators in abnormal situations. The proposed ASM method explained in Chapter 4 has been used to develop a comprehensive knowledge-base of the system. A situation assessment method that uses a fuzzy logic system to resemble operators thinking in assessing situations, is developed. A situation recovery component and a human-computer interface are designed to complete the SASS creation. The SASS reasoning is carried out using the Bayesian theorem that facilitates the inclusion and updating of prior background knowledge when new information is available from the SCADA monitoring system. A comparison with another study and the limitation of the system are ultimately reviewed.

Chapter 6:

MODELLING SITUATION AWARENESS AT A RESIDUE TREATER UNIT

6.1 INTRODUCTION

As described in Chapter 3, the explosion at the methomyl production facility in Institute, West Virginia killed two employees and injured eight people. The intense fire burned for more than four hours, forced many residents to shelter-in-place for over three hours, and closed the nearby highway because of smoke disruption to traffic. The CSB investigation team determined that the runaway chemical reaction and loss of containment of the flammable and toxic chemicals was the result 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 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).

This chapter demonstrates the performance of the SASS at the residue treater unit. Two kinds of operations for the residue treater can be considered: Start-up and Routine. As

described in Chapter 3, the accident happened during the unit start-up after extended outage. Therefore, firstly start-up operation is considered and real data collected from the unit are used in the SASS. Then, the performance of the SASS is investigated through an unreal scenario during routine operation.

6.2 PLANT DESCRIPTION

Methomyl is classified as a carbamate insecticide and is a white crystalline solid with a slight sulfurous odor that is usually produced from methyl isocyanate (MIC). MIC can cause a highly exothermic reaction if mixed with water, therefore it needs to be stored in stainless steel or glass containers at temperatures below 40°C. The production process of methomyl as illustrated in Figure 6.1 starts with the production of methylthioacetaldoxime (MSAO) by reacting chloroacetaldoxime with sodium methyl mercaptide. The MSAO then reacts with MIC to produce methomyl.

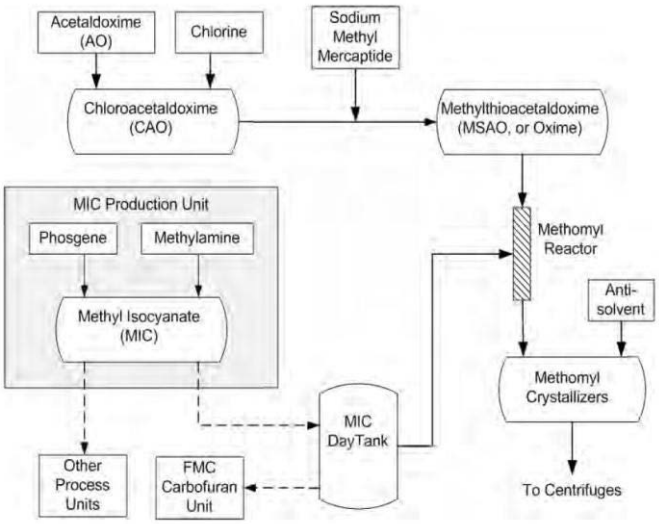


Figure 6.1: Methomyl synthesis process flow

The crystallizers remove excess MIC from the methomyl-solvent solution by adding an anti-solvent that causes the methomyl becomes crystallized. Lastly, a centrifuge separates the crystallized methomyl from the solvents. The methomyl cake is dried, packaged and

moved to the warehouse. The liquid residue in the centrifuge contains very small quantities of methomyl and other impurities (CSB 2011).

As can be seen from Figure 6.2, the solvent recovery flasher separates the solvents and recycles them to the beginning of the process. The accumulated liquid in the bottom of the flasher, which is called "flasher bottoms", includes unvaporized solvents and impurities containing up to 22% methomyl. The flasher bottoms are used as fuel in the facility steam boilers after the methomyl concentration has been reduced to less than 0.5% by weight. This rate is essential for environmental and processing considerations (CSB 2011).

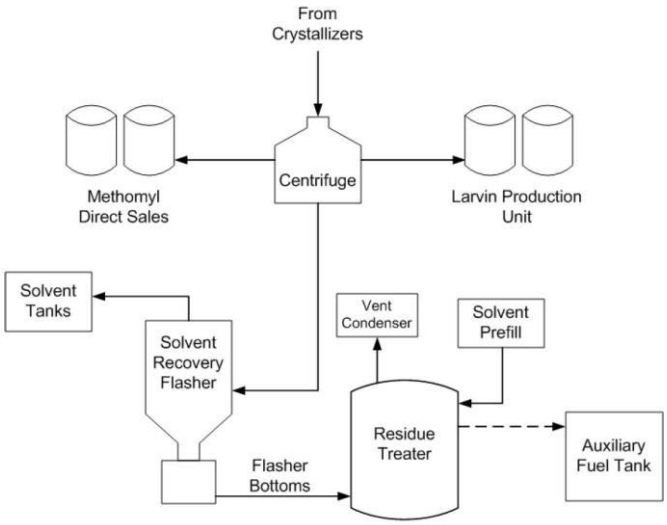


Figure 6.2: Methomyl centrifuge and solvent recovery process flow

The incoming flasher bottoms are diluted in a 4500-gallon pressure vessel (50 psig is the maximum allowable operating pressure) called the residue treater, as shown in Figure 6.3. The concentration of methomyl in the flasher bottom stream will be below 0.5% by weight if the residue treater is operated at a high enough temperature, and with sufficient residence time, to decompose the content. An auxiliary fuel tank is used to store the solvent and residual waste material and to transfer them to the facility steam boiler where they will be used as fuel. Toxic and flammable vapours are removed from vapour generated in the methomyl decomposition reaction when it exits through the vent condenser to the process vent system (CSB 2011).

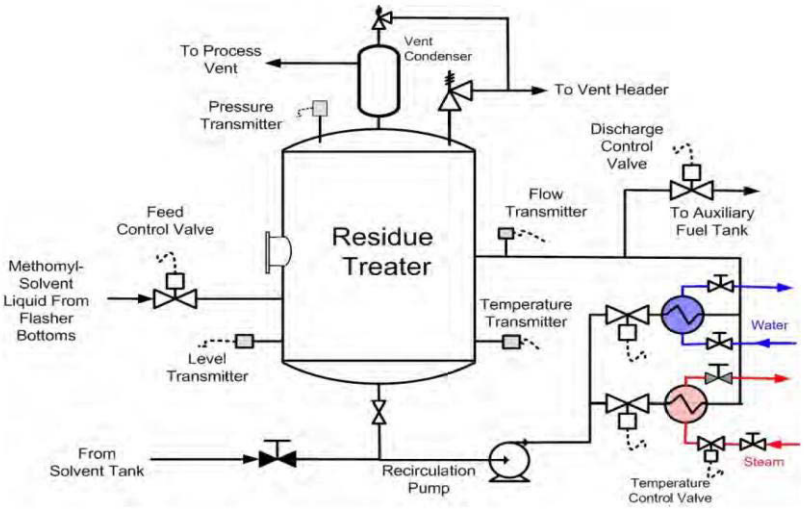


Figure 6.3: Residue treater piping system layout

6.3 OBSERVABLE VARIABLES

There are several transmitters in the environment that provide the online condition for the residue treater. Discrete states of the observable variables are determined in terms of operation and safety set-points as follows:

- Liquid level: A level transmitter provides the residue treater liquid level (L). The routine operation is not started at a level lower than 30%, and the maximum permissible level of liquid is 50%. The value range of the liquid level variable is divided into three fuzzy states: Low, Normal and High. The membership function of L is illustrated in Figure 6.4 and determined as follows:

$$\mu_{L(LO)}(x) = \begin{cases} 1 & x \leq 25 \\ (30 - x)/5 & 25 < x \leq 30 \end{cases} \quad (6.1)$$

$$\mu_{L(N)}(x) = \begin{cases} (x - 25)/5 & 25 \leq x < 30 \\ (35 - x)/5 & 30 \leq x < 35 \end{cases} \quad (6.2)$$

$$\mu_{L(H)}(x) = \begin{cases} (x - 30)/5 & 30 \leq x < 35 \\ 1 & x \geq 35 \end{cases} \quad (6.3)$$

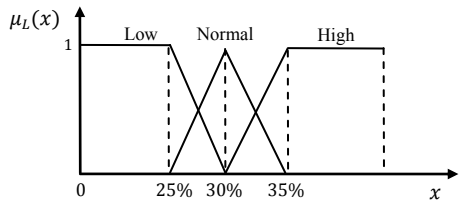


Figure 6.4: **Membership function of liquid level**

- Recirculation flow: During the operation, a pump provides a steady state of recirculation, and a flow transmitter measures the flow of liquid through the recirculation pipeline. The measurement is converted to electrical signals and sent to the DCS by the flow transmitter. This allows operators to visualize the amount of liquid being transferred through the cooling cycle. The value range of the recirculation flow (F) is divided into three fuzzy states, Very Low, Low, and Normal, as shown in Figure 6.5, and the membership function of F is determined as follows:

$$\mu_{F(VL)}(x) = \begin{cases} 1 & x \leq 10 \\ (20 - x)/10 & 10 < x \leq 20 \end{cases} \quad (6.4)$$

$$\mu_{F(L)}(x) = \begin{cases} (x - 10)/10 & 10 \leq x < 20 \\ 1 & 20 \leq x < 40 \\ (60 - x)/20 & 40 \leq x < 60 \end{cases} \quad (6.5)$$

$$\mu_{F(N)}(x) = \begin{cases} (x - 40)/20 & 40 \leq x < 60 \\ 1 & x \geq 60 \end{cases} \quad (6.6)$$

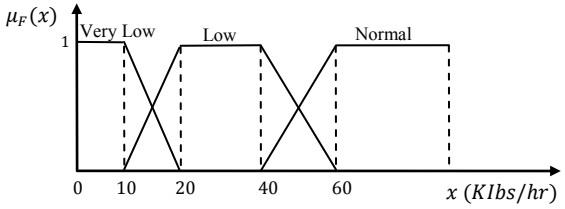


Figure 6.5: **Membership function of recirculation flow**

- Temperature: The content of the residue treater should be maintained around 135°C to decompose the incoming methomyl quickly and prevent the accumulation of methomyl at an unsafe concentration inside the residue treater. A

temperature transmitter provides the residue treater temperature (T). The temperature value range is divided into three fuzzy states, Low, Normal, and High, as shown in Figure 6.6, and the membership function of T is determined as follows:

$$\mu_{T(L)}(x) = \begin{cases} 1 & x \leq 130 \\ (135 - x)/5 & 130 < x \leq 135 \end{cases} \quad (6.7)$$

$$\mu_{T(N)}(x) = \begin{cases} (x - 130)/5 & 130 < x \leq 135 \\ (140 - x)/5 & 135 < x \leq 140 \end{cases} \quad (6.8)$$

$$\mu_{T(H)}(x) = \begin{cases} (x - 135)/5 & 135 \leq x < 140 \\ 1 & x \geq 140 \end{cases} \quad (6.9)$$

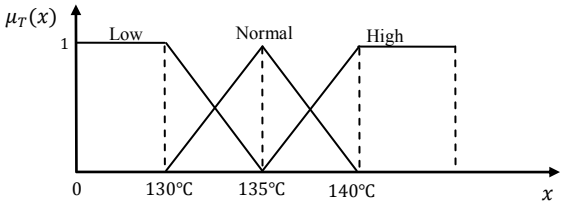


Figure 6.6: Membership function of temperature

- Pressure: The maximum allowable operating pressure of the residue treater is 50 psig, but it is normally operated at 20 psig. A pressure transmitter provides the residue treater pressure (P). 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 6.7:

$$\mu_{P(N)}(x) = \begin{cases} 1 & x \leq 20 \\ (25 - x)/5 & 20 < x \leq 25 \end{cases} \quad (6.10)$$

$$\mu_{P(H)}(x) = \begin{cases} (x - 20)/5 & 20 \leq x < 25 \\ (30 - x)/5 & 25 \leq x \leq 30 \end{cases} \quad (6.11)$$

$$\mu_{P(VH)}(x) = \begin{cases} (x - 25)/5 & 25 \leq x < 30 \\ 1 & x \geq 30 \end{cases} \quad (6.12)$$

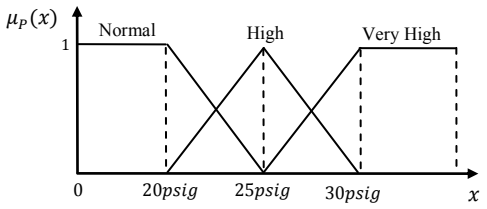


Figure 6.7: Membership function of pressure

6.4 START–UP OPERATION

During start-up, the residue treater is manually pre-filled with solvent to a minimum level of 30%. This means that the operation will not start at a lower level. The solvent is heated by steam that flows through the heater. When the liquid temperature has increased to set-point limit, the steam flow valve is closed, recirculation flow is redirected from the heater to the cooler, and routine operation is started.

6.4.1 EVENTS TIMELINE

At approximately 23:33 on 28 August 2008, the runaway chemical reaction caused a violent explosion at the methomyl manufacturing facility. 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. 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%, 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% (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 6.8). At 22:21, the level was 51% 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 vapour. 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 epicentre 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).

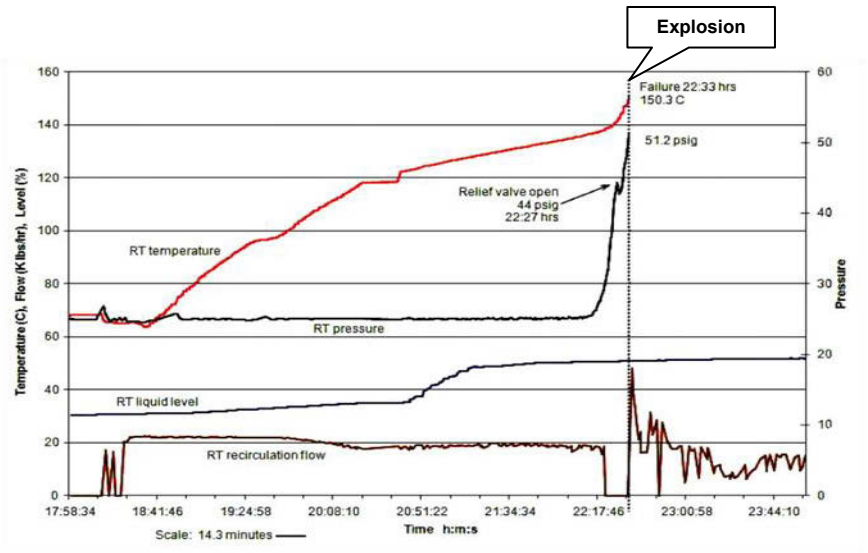


Figure 6.8: Residue treater process variables before the explosion

6.4.2 Abnormal Situations

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)

The first three situations, SVC, SAL, SAR, are independent situations and are modelled based on their objects. The four other situations, SHP, SAT, SHC and SRR are dependent situations

In the following sections, the situations are modelled based on the proposed ASM 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 coloured blue, other objects are shown in yellow and observable variables are coloured green. It is worth noting that the states of observable variables were determined in Section 6.3.

(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, vapour generated in the methomyl decomposition reaction exits through the vent condenser to the process vent system where toxic and flammable vapour 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 6.1, Figure 6.9, and Table 6.2, respectively.

Table 6.1: Situation of vent condenser failure 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

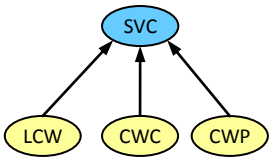


Figure 6.9: Situation of vent condenser failure model

Table 6.2: 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

(2) SITUATION OF ABNORMAL LIQUID LEVEL (SAL)

The start-up 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% and to start the pump and achieve steady state recirculation. This is essential for safe, controlled methomyl decomposition, and starting routine operation, 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 6.3, Figure 6.10, and Table 6.4, respectively. The level transmitter provides the residue treater liquid level, so SAL can be inferred by this variable.

Table 6.3: Situation of abnormal liquid level 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

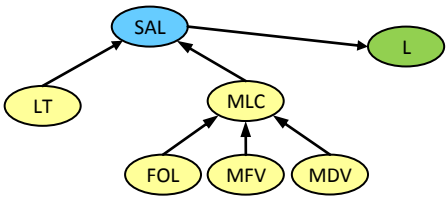


Figure 6.10: Situation of abnormal liquid level model

Table 6.4: 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

(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 start-up, 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 SAR are presented in Table 6.5, Figure 6.11, and Table 6.6, respectively. The situation can be inferred by recirculation flow.

Table 6.5: Situation of abnormal recirculation 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

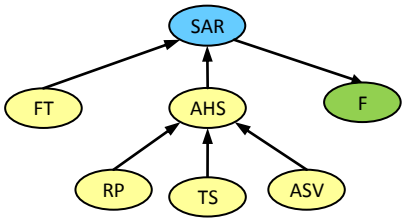


Figure 6.11: Situation of abnormal recirculation model

Table 6.6: 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) SITUATION OF HIGH PRESSURE (SHP)

The residue treater includes an automatic pressure control to ensure that process is normally operated at 20 psig. 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 6.7, Figure 6.12, and Table 6.8 respectively. The situation is connected to node *P* because it can be inferred from the pressure variable.

Table 6.7: Situation of high pressure 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	Independent situation
Inadequate ventilation	IV	OR gate

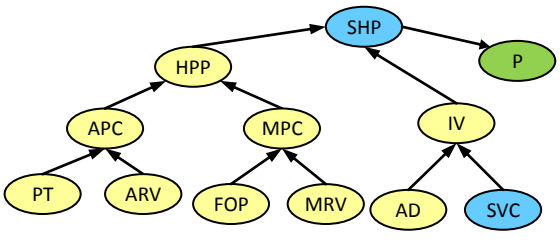


Figure 6.12: Situation of high pressure model

Table 6.8: 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

(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 start-up, 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 6.9, Figure 6.13, and Table 6.10, respectively. The temperature transmitter that provides the residue treater temperature, is used for inferring SAT.

Table 6.9: Situation of abnormal temperature objects and symbols.

Objects	Symbol	Failure Probability
Temperature transmitter	TT	6.84E-06
Situation of abnormal recirculation	SAR	Independent situation
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

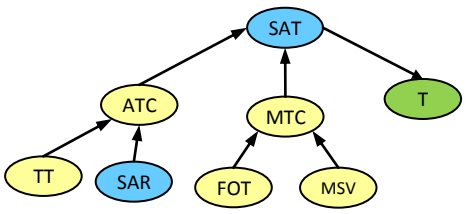


Figure 6.13: Situation of abnormal temperature model

Table 6.10: 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

(6) SITUATION OF HIGH CONCENTRATION OF METHOMYL (SHC)

The methomyl safely decomposes inside the residue treater to a concentration of less than 0.5% 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%, the concentration of methomyl will increase when the flasher bottoms are introduced into the residue treater. The objects, model, and CPT of SHC are presented in Table 6.11, Figure 6.14, and Table .12, respectively.

Table 6.11: Situation of high concentration of methomyl objects and symbols

Objects	Symbol	Failure Probability
Situation of abnormal liquid level	SAL	Independent situation
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	Independent situation
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

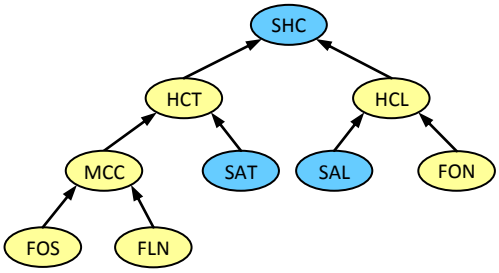


Figure 6.14: Situation of high concentration of methomyl model

Table 6.12: 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

(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 6.13, Figure 6.15, and Table 6.14, respectively.

Table 6.13: Situation of runaway reaction objects and symbols

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

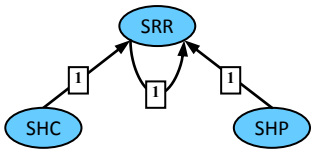


Figure 6.15: Situation of runaway reaction model

Table 6.14: 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

6.4.3 SITUATIONAL NETWORK DEVELOPMENT

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 6.15. The probability of the existence of spark is also estimated in this table.

Table 6.15: **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 Chapter 5 and presented in Table 6.16.

Table 6.16: **The states of 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 vapour 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.

The table contains the degree of loss corresponding to every state, which is evaluated by the expert. 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 6.17. A situational network for the residue treater is developed and illustrated in Figure 6.16.

Table 6.17: **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

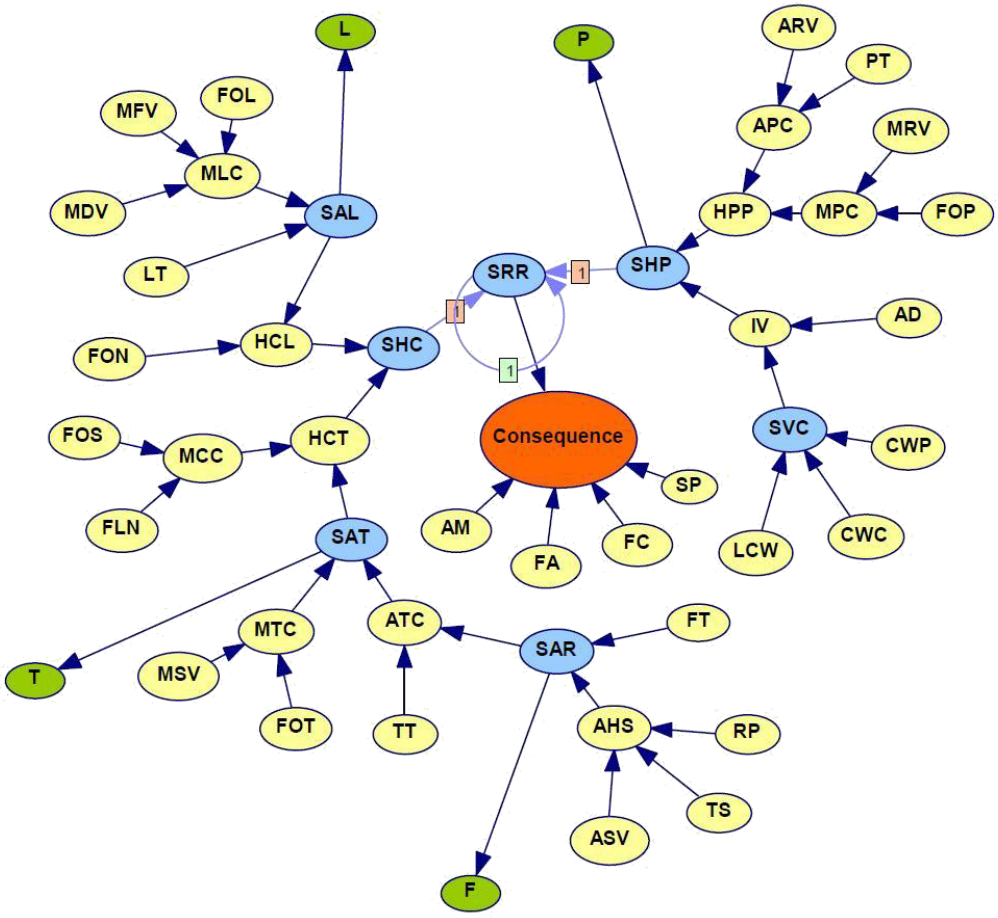


Figure 6.16: **The start–up operation situational network**

6.4.4 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 (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 analysed 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:

$$f(t) = P(SRR = \ Hazardous \mid SHP = Hazardous, T = High) = \frac{\alpha t+\beta}{\gamma t+\delta} \qquad (6.13)$$

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:

$$f(t) = \frac{6.31t+0.0001}{6.09t+1} \qquad (6.14)$$

The graph of the sensitivity function $f(t)$ for all possible values of t, values between zero and one, is plotted in Figure 6.17. 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.

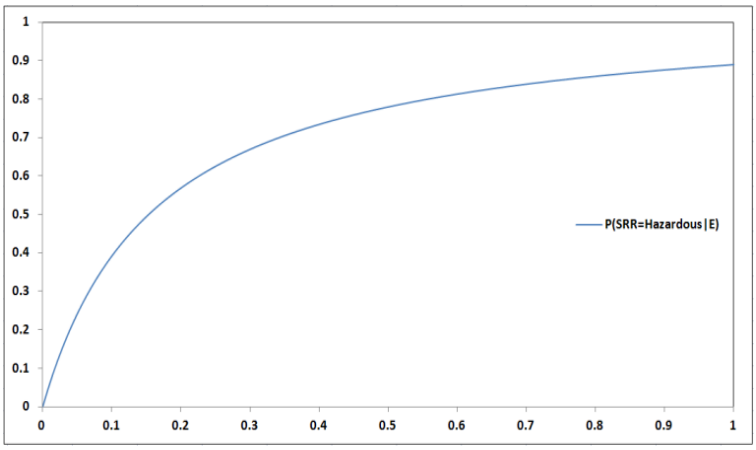


Figure 6.17: The graph of the sensitivity function $f(t)$ = P(SRR= Hazardous | E).

6.4.5 THE SASS PERFORMANCE

On the night of the accident, the critical start-up 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%, significantly below the critical required solvent level (30%), 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, from 21:30 to 22:30 on 28 August. The trend of observable variables for the period of study is illustrated in Figure 6.18. At 21:30, the residue treater liquid level was approximately 50%, 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% 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.

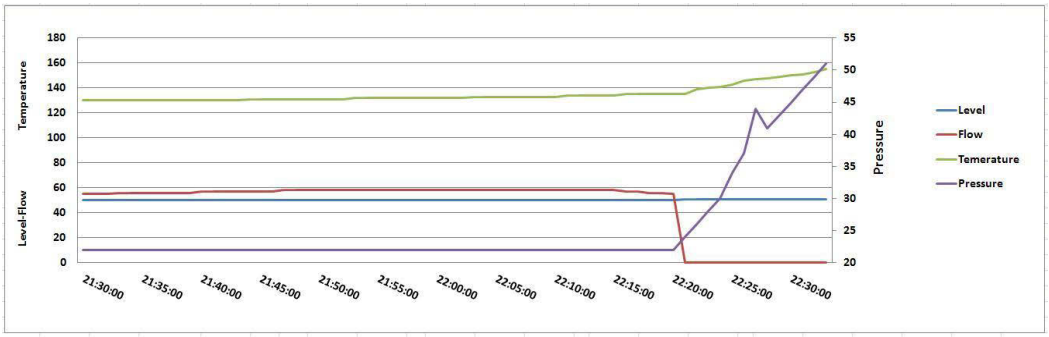


Figure 6.18: The trend of observable variables.

The data collection component provides the fuzzy partitioning values of observable variables based on the proposed membership functions and assigned them 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 6.19. 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%), 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.

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 system 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.

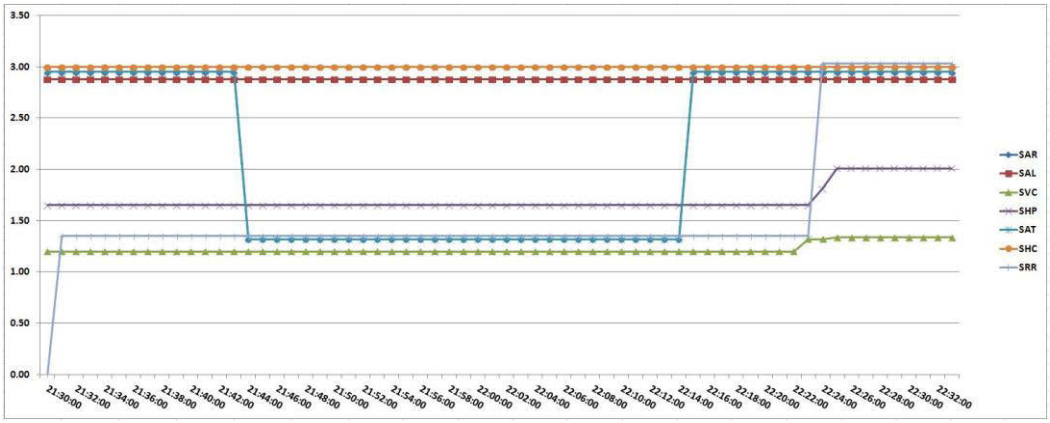


Figure 6.19: **Projection of situation risk levels**.

6.5 Routine Operation

To prepare for a routine operation, the vessel is filled with solvent and heated. Dissolved methomyl and other waste chemicals are fed into the preheated residue treater, which is partially filled with solvent. A normal recirculation loop flow is ensured to mix the concentrated methomyl feed with preheated solvent in the residue treater. The methomyl safely decomposes inside the residue treater to a concentration of less than 0.5% by weight.

6.5.1 Abnormal Situations

Several possible abnormal situations for routine operation are determined as follows:

- Situation of vent condenser failure (SVC)
- Situation of high liquid level (SHL)
- Situation of abnormal recirculation (SAR)
- Situation of high pressure (SHP)
- Situation of high temperature (SHT)

- Situation of high concentration of methomyl (SHC)
- Situation of runaway reaction (SRR)

As can be seen, there are some common situations between Start-up and Routine operations, i.e. SVC, SHP, and SAR. The following sections outline the new situations, which are modelled based on the proposed ASM method. The CPTs of focal objects that delegate the situations are presented, and the CPTs of other objects are omitted. The first three situations, i.e. SVC, SHL, SAR, are independent situations and are modelled based on their objects. The four other situations, i.e. SHP, SHT, SHC and SRR are dependent situations and are modelled based on their objects and the independent situations.

(1) SITUATION OF HIGH LIQUID LEVEL (SHL)

Operation at a liquid level higher than 50% of vessel capacity is dangerous. Therefore, the residue treater has an automatic level control system and a manual level controller to maintain the liquid level at less than 50%. The objects, model, and CPT of SHL are presented in Table 6.18, Figure 6.20, and Table 6.19, respectively. This situation can be inferred by the liquid level variable.

Table 6.18: Situation of high liquid level objects and symbols

Objects	Symbol	Failure Probability
Level transmitter	LT	1.40E-04
Automatic feed valve	AFV	2.02E-05
Automatic feed control	AFC	OR gate
Automatic discharge valve	ADV	2.75E-05
Automatic discharge control	ADC	OR gate
Automatic level control	ALC	OR gate
Failure of operator in operating manual valves	FOL	2.70E-01
Manual feed valve	MFV	1.40E-01
Manual discharge valve	MDV	1.40E-01
Manual level control	MLC	OR gate

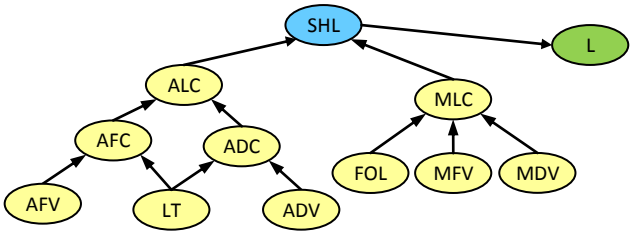


Figure 6.20: Situation of high liquid level

Table 6.19: CPT of P(SHL| ALC, MLC)

Variables	**States and probabilities**			
ALC	Failure		Success	
MLC	Failure	Success	Failure	Success
Hazardous	1	0	0	0
Safe	0	1	1	1

(2) SITUATION OF HIGH TEMPERATURE (SHT)

During routine operation, water flows to remove excess heat generated by the exothermic decomposition of the methomyl inside the vessel. The exothermic heat of decomposition is controlled by vaporization and condensing of the solvent in the vent cooler, supplemented as needed by the recirculation loop cooler. The objects, model, and CPT of SHT are presented in Table 6.20, Figure 6.21, and Table 6.21, respectively. SHT is also inferred from temperature variable.

Table 6.20: Situation of high temperature objects and symbols

Objects	**Symbol**	**Failure Probability**
Temperature transmitter	TT	6.84E-06
Situation of abnormal recirculation	SAR	Independent situation
Automatic temperature control	ATC	OR gate
Failure of operator to notice temperature change	FOT	1.00E-01
Manual water valve	MWV	1.39E-06
Manual temperature control	MTC	OR gate

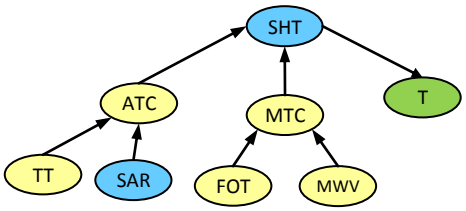


Figure 6.21: Situation of high

Table 6.21: CPT of P(SHT | ATC, MTC)

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

(3) SITUATION OF HIGH CONCENTRATION OF METHOMYL

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, the temperature that ensures that the incoming methomyl quickly decomposes to avoid accumulation to an unsafe concentration inside the residue treater. If the tank is allowed to cool below 130 °C for any reason, it must be sampled before being heated again. It is assumed that operators will sample the residue treater liquid and that appropriate testing will be conducted be the laboratory. The objects, model, and CPT of SHC are presented in Table 6.22, Figure 6.22, and Table 6.23, respectively.

Table 6.22: Situation of high concentration of methomyl objects and symbols

Objects	**Symbol**	**Description**
Situation of high liquid level	SHL	Independent situation
Situation of high temperature	SHT	Dependent situation

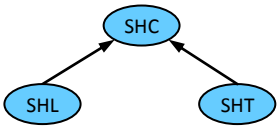


Figure 6.22: Situation of high

Table 6.23: CPT of P(SHC| SHL, SHT)

Variables	**States and probabilities**			
SHL	Hazardous		Safe	
SHT	Hazardous	Safe	Hazardous	Safe
Hazardous	1	1	1	0
Safe	0	0	0	1

(4) SITUATION OF RUNAWAY REACTION

The runaway reaction results if methomyl is allowed to accumulate in the residue treater and a high pressure situation exists in the environment, the relief system is not working properly, which leads to a runaway reaction. The objects, model, and CPT of SRR are presented in Table 6.24, Figure 6.23, and Table 6.25 respectively.

Table 6.24: Situation of runaway reaction objects and symbols

Objects	**Symbol**	**Description**
Situation of high pressure	SHP	Dependent situation
Situation of high concentration of methomyl	SHC	Dependent situation

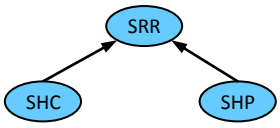


Figure 6.23: Situation of runaway reaction model

Table 6.25: CPT of P(SRR | SHC, SHP)

Variables	**States and probabilities**			
SHC	Hazardous		Safe	
SHP	Hazardous	Safe	Hazardous	Safe
Hazardous	1	0	0	0
Safe	0	1	1	1

6.5.2 Situational Network Development

It is assumed that the safety systems are the same as previously explained in Section 6.4.3 and the states of consequence node are as explained in Table 6.16. A situational network for the routine operation is developed and illustrated in Figure 6.24. As there is no situation to be inferred during the timeframe, the situational network does not consist of a temporal arc.

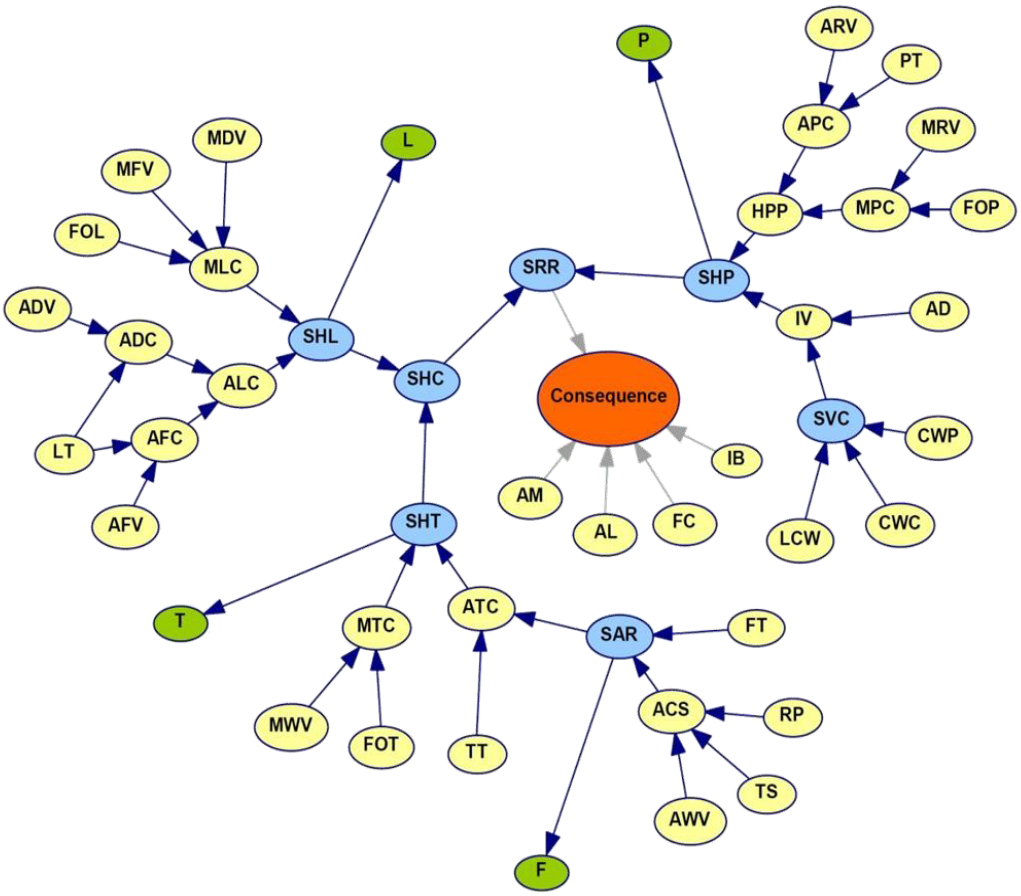


Figure 6.24: The routine operation situational network

6.5.3 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 as shown in Table 6.26. This is what the experts have 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 (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 SHL followed by observable variable L. Alternatively, when P=High and L=High are entered into the network, some of remaining variables become more influential. These observations agreed with the experts understanding of the situational network.

Sensitivity to parameters was analysed in the CTPs of observable variables which were determined by the experts. A model deficiency was the posterior probability P(SAR=Hazardous| F=Low)=0.4333. The experts believed that the probability should be no less than 0.65 given this evidence. Therefore, some of the network parameters were changed to satisfy this query constraint. The use of SamIam software (UCLA 2004) for any solution for every network parameter returned seven suggestions of single parameter changes. Four of the parameter changes were ruled out as they were changing the failure probabilities of basic objects. The only sensible parameter change was to decrease P(F=Low| SAR=Safe) from 0.1 to <=0.01374.

Table 6.26: **Sensitivity to findings analysis performed on SRR**.

	No Evidence	P=High	P=High, L=High
P(SRR=Hazardous)	0.00210	0.42300	0.91900
Entropy of SRR	0.02152	0.9828	0.4060
Node	Mutual Information	Mutual Information	Mutual Information
SHP	0.01702	0.06805	0.40595
P	0.01684	---	----
IV	0.01093	0.06642	0.38678
SVC	0.01093	0.06572	0.38510
CWC	0.00702	0.00837	0.00135
HPP	0.00539	0.05643	0.30601
MPC	0.00298	0.04205	0.21444
APC	0.00241	0.03675	0.18410
MLC	0.00233	0.79470	0.00000
SHC	0.00233	0.79596	0.00000
SHL	0.00233	0.79595	0.00000
CWP	0.00214	0.00119	0.02937
FOP	0.00136	0.00344	0.04824
L	0.00121	0.48338	-----
ARV	0.00110	0.00310	0.04167
FOL	0.00066	0.29350	0.00000
MRV	0.00051	0.00085	0.01506
PT	0.00036	0.00063	0.01090
MDV	0.00027	0.12885	0.00000
MFV	0.00027	0.12885	0.00000
LCW	0.00011	0.00005	0.38510
ALC	0.00000	0.00015	0.00000
AFC	0.00000	0.00013	0.00000
AFV	0.00000	0.00002	0.00000
ADC	0.00000	0.00013	0.00000
ADV	0.00000	0.00002	0.00000
LT	0.00000	0.00011	0.00000
SHT	0.00000	0.00000	0.00000
MTC	0.00000	0.00000	0.00000
F	0.00000	0.00000	0.00000
T	0.00000	0.00000	0.00000
FC	0.00000	0.00000	0.00000
FA	0.00000	0.00000	0.00000
IB	0.00000	0.00000	0.00000
AM	0.00000	0.00000	0.00000
AD	0.00000	0.00000	0.00002
FOT	0.00000	0.00000	0.00000
MWV	0.00000	0.00000	0.00000
ATC	0.00000	0.00000	0.00000
TT	0.00000	0.00000	0.00000
SAR	0.00000	0.00000	0.00000
ACS	0.00000	0.00000	0.00000
AWV	0.00000	0.00000	0.00000
TS	0.00000	0.00000	0.00000
RP	0.00000	0.00000	0.00000
FT	0.00000	0.00000	0.00000

6.5.4 THE SASS PERFORMANCE

To prepare for a routine operation, the vessel was filled with solvent and heated. Methomyl was added into the residue treater, and a normal recirculation loop flow was ensured to mix the concentrated methomyl feed with preheated solvent in the residue treater. At approximately 12 pm, the board operator manually opened the residue treater feed control valve and began feeding flasher bottoms into the vessel. At normal flow rate, it would take approximately 30 minutes to fill the residue treater to 50%, the normal operating level. The outside operator started the recirculation pump at 12:30 pm, as directed by the board operator. The residue treater liquid level was approximately 50% and the temperature ranged between 130 and 135 °C. The pressure remained constant at 22 psig. The trends of observable variables are illustrated in Figure 6.25. At 12:41 pm, the temperature began to rise steadily about 1 degree per minute. At 12:49 pm, the level was 51% when the recirculation flow suddenly dropped to zero. In less than 3 minutes, the temperature was at 147 °C, the highest safe operating limit.

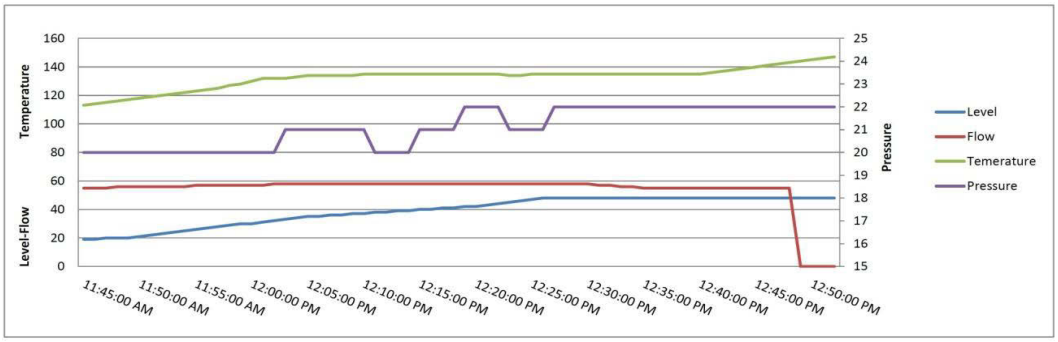


Figure 6.25: The trend of observable variables

By assigning fuzzy partitioning values of observable variables after starting the routine operation, i.e. after 12:00 pm, to the situational network, the posterior probabilities of the situations are calculated, as shown in Figures 6.26 and 6.27. As can be seen, there is a sharp increase in the probabilities of SHL at 12:24 pm, SVC and SAR at 12:44 pm, SHC at 12:40 pm and SHT at 12:43 pm. The posterior probabilities are unable to support the operators' understanding of the current state of the situation. The operators must still rely on their

knowledge and mental models to comprehend what is going on; therefore, the use of risk indicators and situational models are used to support their comprehension and projection. The risk level of situations is calculated and summarized in Figures 6.28 and 6.29. As can be seen, the estimated risk level of SAR increases at 12:45 pm from 1.32 (acceptable) to 2.95 (tolerable not acceptable) which means this hazardous situation is abnormal at present and needs to be recovered. The risk level of other independent situations, i.e. SHL and SVC, remains acceptable; however, there is a rise in their posterior probabilities. The risk level of SHP is steady and acceptable as expected, i.e. the pressure inside the vessel is almost normal. The risk level of SHT and SHC increases from acceptable at 12:45 pm, i.e. 1.32 and 1.65, respectively, to tolerable not acceptable, i.e. 2.95 and 3, respectively. Likewise, although there is an increase in the risk level of SRR, it remains acceptable during the study period, which means that this hazardous situation does not threaten the system.

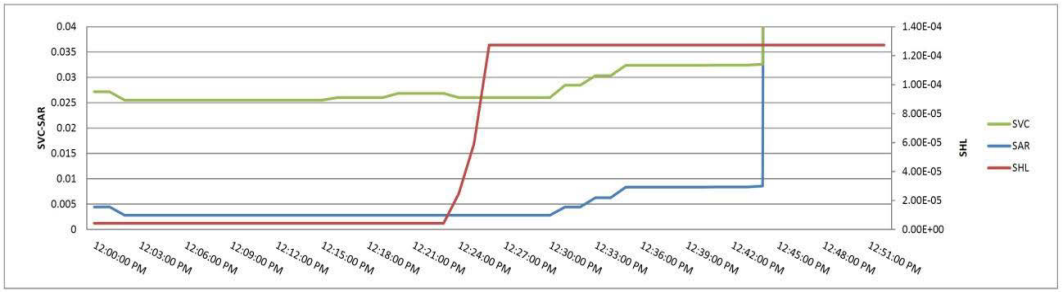


Figure 6.26: Posterior probability of independent situations

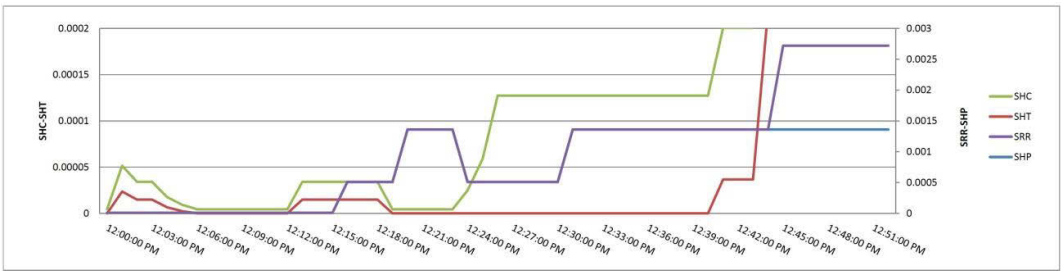


Figure 6.27: Posterior probability of dependent situations

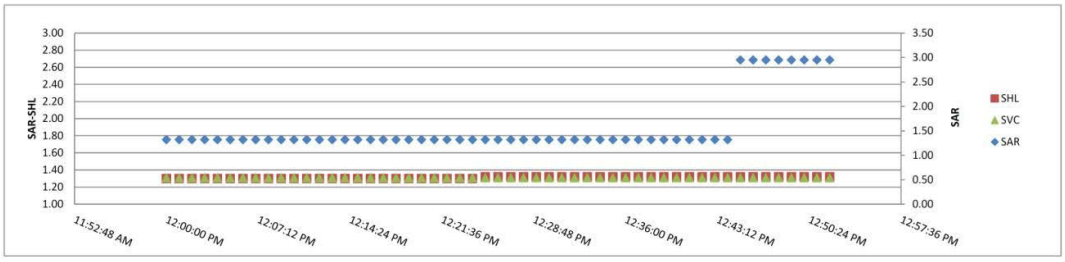


Figure 6.28: Risk level of independent situations

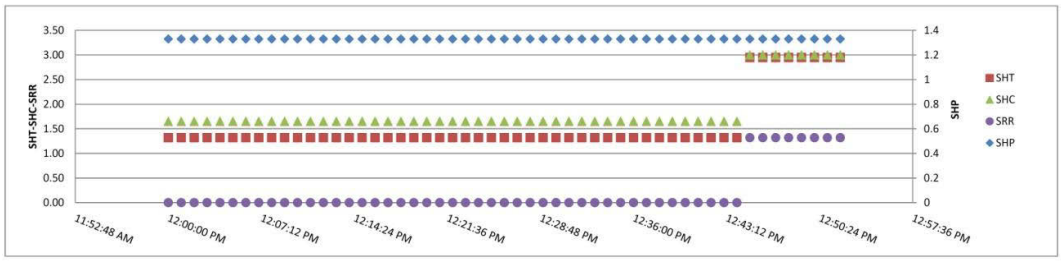


Figure 6.29: Risk level of dependent situations

At 12:45 pm when the risk level of SAR rises, the situational network shows that the most probable explanation is the failure of the recirculation pump (RP). The board operator immediately contacts the outside operator and directs him to check the recirculation pump. The outside operator's inspection at 12:47 pm determines the valid performance of the RP. With new evidence (success of the RP), the board operator realized that the failure of the temperature sensor (TS) in the recirculation is the most likely factor. Considering the result of the situation assessment, maintenance decisions are made to recover the situation. The trend of observable variables after abnormal situation recovery is illustrated in Figure 6.30.

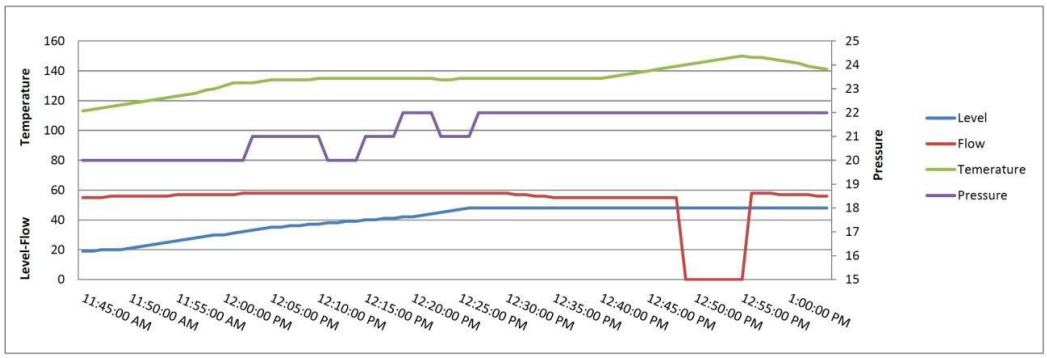


Figure 6.30: The trend of observable variables after abnormal situation recovery.

The system helps the operator to prevent accidents in abnormal situations, but it also presents the factors that contribute to the creation of an accident, or a specific consequence. For instance, if at 12:52 pm a fire with low death and moderate property damage (C4) 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.

6.6 SUMMARY

This chapter has shown the performance of the SASS in supporting the control room operator' SA in the residue treater unit. As reviewed, the accident happened when a new mimic screen installed at the unit. Mimic screen is a simplified graphical representation of a process that uses icons to display piping and equipment with color-coded operating status, instrumentation with output values and set-point data, and other key equipment and information to maintain SA and to control the process. However, in the presence of several precursors, the DCS could not support SA. The explosion occurred during start-up operation, so real data taken from the CBS report has been used to verify the SASS performance. After that, the routine operation has been considered through an unreal scenario.

As has been shown, the SASS provides a useful graphical system that meets the requirements of a practical SA system. The BN-based mental models provide the base for knowledge-base preparation, and 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.

Chapter 7:

MODELLING SITUATION AWARENESS IN MIXING TANKS

7.1 INTRODUCTION

Following on from the previous chapter, this chapter also aims to demonstrate and test the performance of the SASS in different chemical plants. Two kind of mixing tanks are used: a tank equipped with steam coils at a chemical plant (CSB 2007), and an ink vehicle insulated mix tank at a paint manufacturing company (CSB 2008). The presented case studies can add a sense of urgency or reality to the proposed system, and shows how the system works. In addition, they provide a real application of the proposed system and help to validate its performance.

The first case, as reviewed in Chapter 3, relates to the open top tank located in a chemical mixing area in which the ignition of a vapour cloud generated by mixing and heating a flammable liquid killed one contractor and injured two employees, and caused a significant business interruption. The accident occurred when an operator was mixing and heating a flammable mixture of heptane and mineral spirits in a tank equipped with steam coils.

The second case relates to a paint manufacturing plant in which, following an incident, the explosion and subsequent fire destroyed the facility, heavily damaged dozens of nearby homes and businesses, and shattered windows as far away as two miles. At least 10 residents required hospital treatment for cuts and bruises. Twenty-four homes and six businesses were damaged beyond repair. Dozens of boats at a nearby marina were heavily damaged by blast overpressure and debris strikes. The explosion was fuelled by vapour released from a 2000-gallon tank of highly flammable liquid.

7.2 A TANK EQUIPPED WITH STEAM COILS

The tank in this case is equipped with steam coils (Figure 7.1) 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 (Figure 7.2) has local and area heating, and exhaust ventilation systems that are assumed to have sufficient capacity to collect a huge volume of vapour. The sprinkler system and fire alarm system have been designed to reduce damage if a fire occurs or vapour accumulates. An operator checks the temperature using an infrared thermometer, monitors the environment and conducts appropriate actions when necessary.

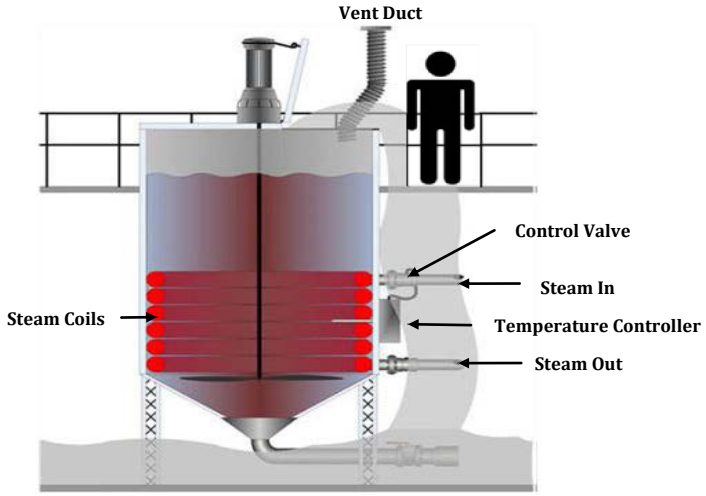


Figure 7.1: The tank equipped with steam coils

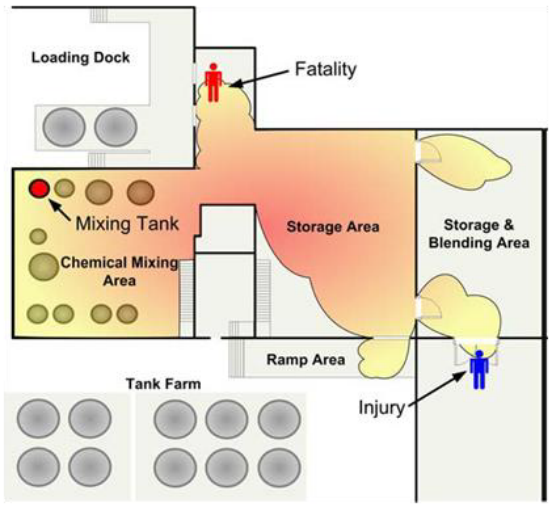


Figure 7.2: The open-top tank environment

7.2.1 OBSERVABLE VARIABLES

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 7.3 and determined as follows:

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

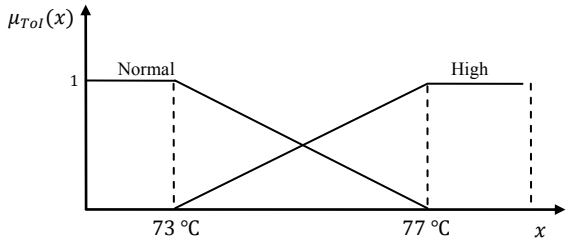
$$\mu_{ToI(N)}(x) = \begin{cases} 1 & x \leq 73 \\ (77 - x)/4 & 73 < x \leq 77 \end{cases} \quad (7.1)$$

$$\mu_{ToI(H)}(x) = \begin{cases} (x - 73)/4 & 73 \leq x < 77 \\ 1 & x \geq 77 \end{cases} \quad (7.2)$$

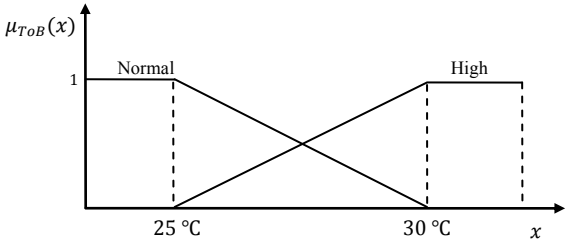
- Temperature of the production building (ToB): {Normal, High}

$$\mu_{ToB(N)}(x) = \begin{cases} 1 & x \leq 25 \\ (40 - x)/5 & 25 < x \leq 30 \end{cases} \quad (7.3)$$

$$\mu_{ToB(H)}(x) = \begin{cases} (x - 35)/5 & 25 \leq x < 30 \\ 1 & x \geq 30 \end{cases} \quad (7.4)$$



(a)



(b)

Figure 7.3: The membership functions of observable variables

7.2.2 ABNORMAL SITUATIONS

There are three possible abnormal situations in the environment:

- Situation of accumulated vapour in the production building (SAV)
- Situation of high temperature inside the tank (SHT)
- Situation of inadequate building ventilation (SIV)

The first situation is not directly inferable from the objects, i.e. it is a dependent situation, and has to be defined by the dependencies on independent situations. The second and third situations can be inferred from their contributor objects and observable variables. Table 7.1 shows a number of physical and conceptual objects that contribute to these situations. The failure probabilities are determined based on data recorded by OREDA (2002).

Table 7.1: The open-top tank situations

Situation/Object	Symbol	Failure Probability
SAV		
High temperature inside the tank	SHT	Independent situation
Inadequate building ventilation	SIV	Independent situation
Ignition Barrier	I	0.1000
Alarm System	A	0.0013, 0.2250
Sprinkler System	P	0.04000
Consequences	C	NA
SHT		
Operator	O	0.0200
Infrared Thermometer	T	0.0468
Sensor	S	0.0400
Pneumatic Unit	PU	0.2015
Temperature Measurement System	TMS	OR gate
Manual Steam Valve	MSV	0.0243
Automatic Steam Valve	ASV	0.0276
Temperature Control System	TCS	OR gate
Manual Temperature Control	MTC	OR gate
Automatic Temperature Control	ATC	OR gate
SIV		
Belt	B	0.0500
Fan	F	0.0100
Duct Plugging	D	0.0010

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

The situation models are summarized in Figure 7.4. The figure shows three situations of interest in which the dependent situation is coloured red, the independent situations are coloured blue, and objects are shown in yellow. The CPTs of SAV, SIV and SHT are shown in Tables 7.2-7.4, and other CPTs are omitted.

Table 7.2: CPT of P(SAV| SAV, SHT, SIV)

SAV	SHT	SIV	SAV=Hazardous	SAV=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 7.3: CPT of P(SHT | MTC, ATC)

MTC	ATC	SHT=Hazardous	SHT=Safe
Failure	Failure	1	0
Failure	Success	0	1
Success	Failure	0	1
Success	Success	0	1

Table 7.4: CPT of P(SIV | D, F, B)

D	F	B	SIV=Hazardous	SIV=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

7.2.3 SITUATIONAL NETWORK DEVELOPMENT

Figure 7.4 shows the developed situational network. The temporal arc points to the SAV 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 vapour accumulates when the high temperature persists for a few minutes inside the tank and the ventilation system is unable to disperse it. The prior probability of the higher level situation, i.e. SAV, is set to 1 for safe state and 0 for hazardous state, and it is assumed that the environment is initially safe. The states of consequence node is determined as shown in Table 7.5. It is worth noting that, for situations SHT and SIV, the accumulated vapour can be considered as their consequence in which the degree of loss is about $1E+06.

Table 7.5: The consequences of SAV

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
Vapour 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

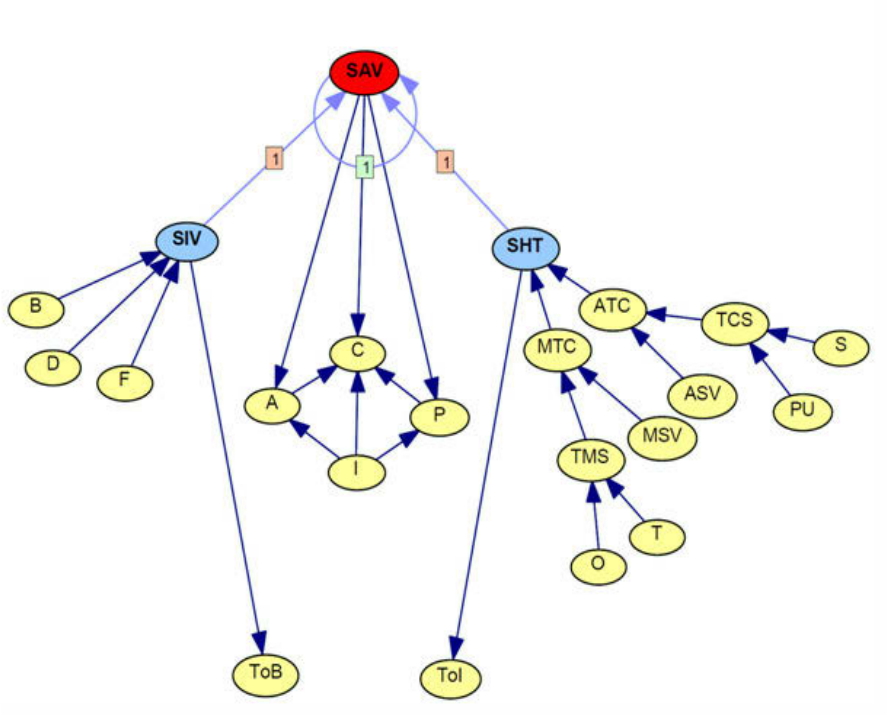


Figure 7.4: The open-top tank situational network

7.2.4 SITUATIONAL NETWORK EVALUATION

To evaluate the situational network, the sensitivity analysis is conducted according to the following three axioms (Jones et al. 2010):

- 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.
- 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.
- 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).

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 SHT from 0.02 to 0.08. Likewise, at time *t*, when the failure probability of the "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 SHT is increased to 1 from 0.08. The evidence increases the failure probability 0.1 for SAV 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 SIV because of OR gate definition, and failure probability of 0.9 from 0.1 for SAV at time *t*+1.

7.2.5 THE SASS PERFORMANCE

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 7.5 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.

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 SAV is 0.05 and the probabilities of the consequence states are calculated as shown in Table 7.5. As can be seen, the safe state is the most probable consequence of SAV. The total loss of SAV, i.e. its severity, can be calculated by multiplication of the probabilities and loss of consequences, which is about $2.56E+04. Therefore, the estimated risk level is 1.3, which means that the current risk level of SAV is acceptable.

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 7.6. As can be seen, the SHT situation is hazardous from minutes 16 to 31 and situation SIV becomes hazardous from minutes 24 to

28, as is expected as a result of the observable variables. In parallel, the risk level of SHT is 2.95, i.e. TNA from minutes 16 to 31, and the risk level of SIV is TNA during minutes 24 to 28, as shown in Figure 7.6. It is assumed that the local and area ventilation systems have the ability to evacuate the vapour, thus the risk level of SAV 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.

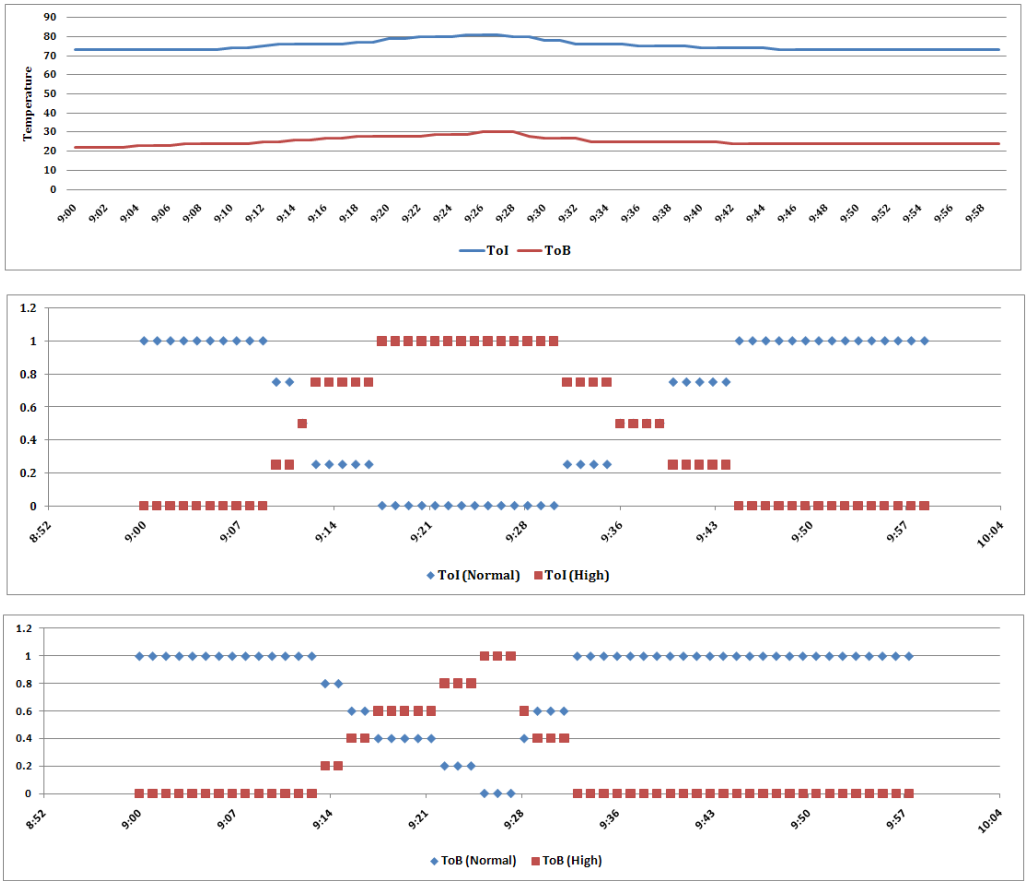


Figure 7.5: The observable variables and their fuzzy partitioning values

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 SHT 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 vapour, and failure of the ignition barrier caused the fire.

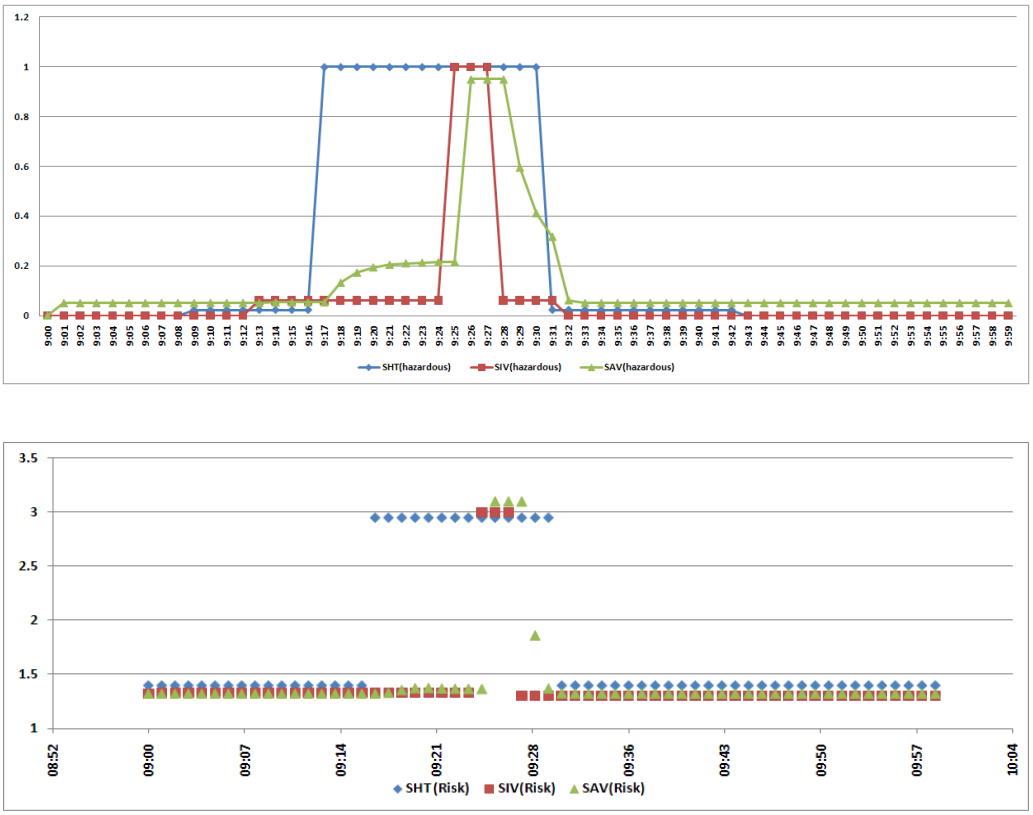


Figure 7.6: The posterior probabilities and risk levels of situations.

7.3 AN INK VEHICLE MIX TANK

The environment includes an ink vehicle mix tank, approximately 3000 gallons in capacity, 10 feet tall and eight feet in diameter with a top-mounted mixer and a 12-inch diameter access hatch that does not prevent air or vapour from passing through the opening. The tank is equipped with a steam heating jacket connected to the steam boiler. An operator controls the temperature of the mixture by opening and closing a turn ball valve on the steam pipe connected to the tank jacket. The operator accesses the tank top, weight and temperature display consoles, mixer control switches, and steam valves from a steel-grated mezzanine deck on the north side of the tank. The operator opens the slide valve on the dust collector suction line during the addition of dusty materials to the mix tank and closes it afterward. There are also eight 500 gallon steel totes in the area for the storage of solvents (Figure 7.7).

The building heating and ventilation system consists of a number of steam-coil fan units mounted near the ceiling, a fresh air distribution system and production area exhaust fans to remove flammable vapour from around the unsealed ink and paint mixers. It is assumed that the ventilation system has sufficient capacity to collect a huge volume of vapour. There are also safety systems which include a sprinkler system, an ignition barrier and an alarm system. A foam fire suppression sprinkler system is installed in the production area. In the event of a fire, fusible plugs on the ½-inch orifice standard sprinkler heads will melt to activate the sprinkler head. Water flow in the fire suppression system will trigger the fire alarm box, which will send a signal to the fire department.

7.3.1 OBSERVABLE VARIABLES

The monitoring system provides update information about these observable variables to the evidence preparation component, and they are stored in a database and fuzzily prepared as inference evidence for use in the situation assessment component. The process for mixing 2000-gallons of ink in a tank involves heating for several hours, with the temperature controller being adjusted to maintain the temperature at 32°C (90°F).

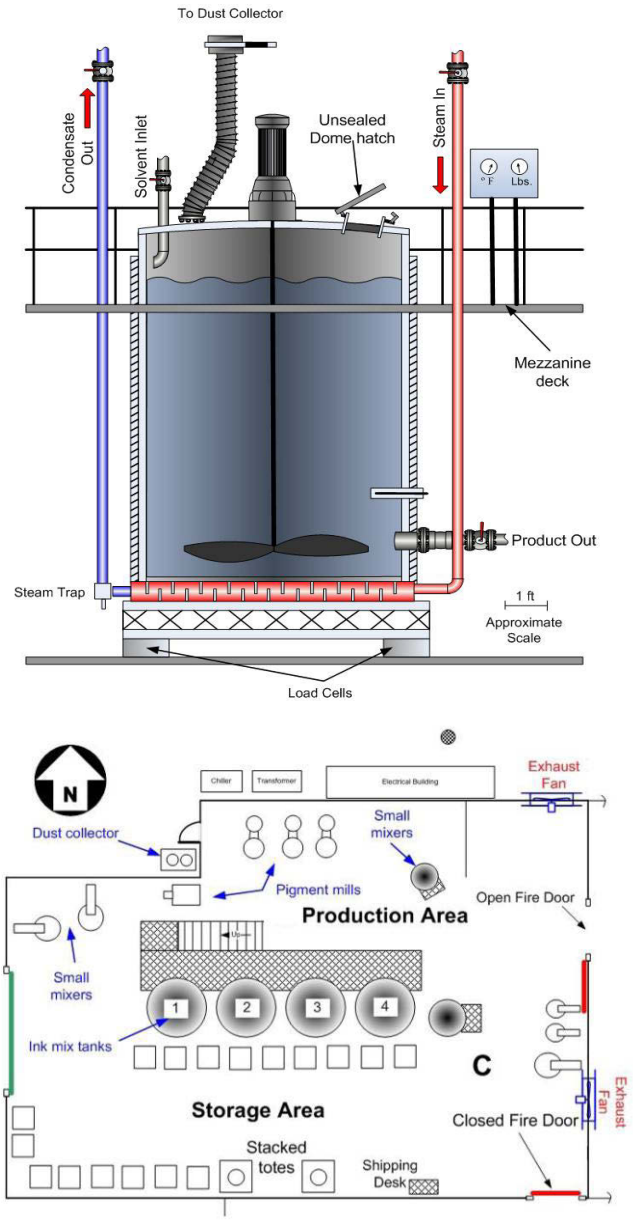


Figure 7.7: The ink vehicle mix tank environment

The temperature of the production unit in normal operation is about 25°C and the normal interval of the outside temperature is (0,40). The value ranges of the temperature variables are divided into fuzzy states as follows and their membership functions are illustrated in Figure 7.8:

- The temperature of the inside of the tank (ToI): {Normal, High}

$$\mu_{ToI(N)}(x) = \begin{cases} 1 & x \leq 32 \\ (47 - x)/15 & 32 < x \leq 47 \end{cases} \quad (7.5)$$

$$\mu_{ToI(H)}(x) = \begin{cases} (x - 32)/15 & 32 \leq x < 47 \\ 1 & x \geq 47 \end{cases} \quad (7.6)$$

- The temperature of the production unit (ToP): {Normal, High}

$$\mu_{ToP(N)}(x) = \begin{cases} 1 & x \leq 25 \\ (30 - x)/5 & 25 < x \leq 30 \end{cases} \quad (7.7)$$

$$\mu_{ToP(H)}(x) = \begin{cases} (x - 25)/5 & 25 \leq x < 30 \\ 1 & x \geq 30 \end{cases} \quad (7.8)$$

- The temperature of the outside environment (ToE): {Low, Normal, High}

$$\mu_{ToE(L)}(x) = \begin{cases} 1 & x \leq 0 \\ (10 - x)/10 & 0 < x \leq 10 \end{cases} \quad (7.9)$$

$$\mu_{ToE(N)}(x) = \begin{cases} x/10 & 0 \leq x < 10 \\ 1 & 10 \leq x < 30 \\ (40 - x)/10 & 30 \leq x < 40 \end{cases} \quad (7.10)$$

$$\mu_{ToE(H)}(x) = \begin{cases} (x - 30)/10 & 30 \leq x < 40 \\ 1 & x \geq 40 \end{cases} \quad (7.11)$$

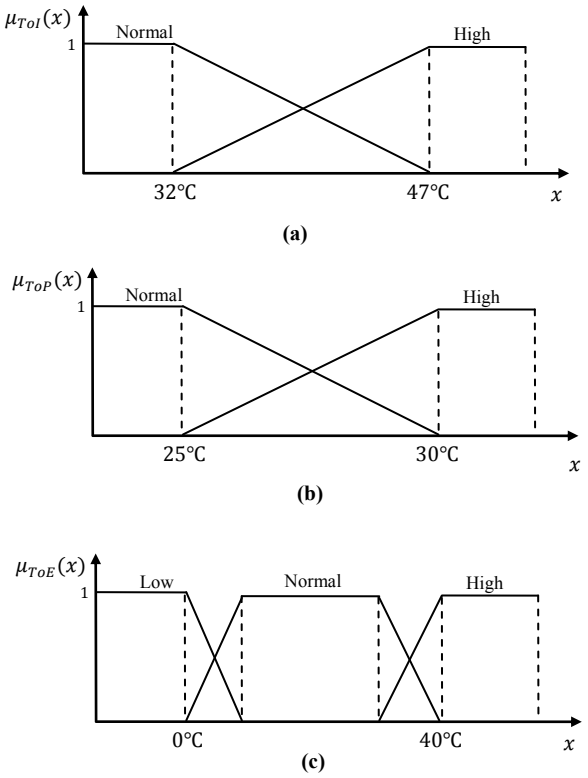


Figure 7.8: The membership functions of the observable variables

7.3.2 ABNORMAL SITUATIONS

There are several possible hazardous situations in the environment which threaten the system. To simplify the demonstration, one tank is chosen. As the investigation report shows, the important hazardous situations are as follow:

- Situation of accumulated vapour in the production area (SAV)
- Situation of high temperature inside the tank (SHT)
- Situation of building ventilation system malfunction (SBV)
- Situation of large spill from storage system (SLS)

The SAV is dependant and has to be defined by dependencies on independent situations. First, the independent situations (i.e. SHT, SBV, and SLS), which can be inferred from their contributor objects, are modelled. Their contributor objects, which are physical or conceptual, are determined as shown in Tables 7.6.

Table 7.6: The ink vehicle mix tank situations

Objects	Symbol	Failure Probability
SHT		
Sensor	S	0.0400
Pneumatic Unit	PU	0.2015
Temperature Control System	TCS	OR gate
Operator	O	0.0200
Manual Steam Valve	MSV	0.0243
Manual Temperature Control	MTC	OR gate
SBV		
Belt	B	0.0500
Fan	F	0.0100
Inadequate Ventilation	V	0.0150
Duct Plugging	DP	0.0010
SLS		
Drain Valve	DV	0.0013
Transfer Piping	T	0.0049
Transfer System	TS	AND gate
Leak	L	0.0001

According to the ASM method, these objects have two states (i.e. failure and success) and the prior probabilities of basic objects are determined based on data recorded by the CCPS (1989), and OREDA (2002).

The CPTs of intermediate objects and focal objects are based on AND and OR gates definition. The CPTs of SHT, SBV, and SLS are shown in Tables 7.7–7.9; the CPTs of intermediate objects are omitted because they are set in a similar way.

Table 7.7: **CPT of P(SHT | MTC, TCS)**.

MTC	TCS	SHT=Hazardous	SHT=Safe
Failure	Failure	1	0
Failure	Success	0	1
Success	Failure	0	1
Success	Success	0	1

Table 7.8: **CPT of P(SLS | L, TS)**

L	TS	SLS=Hazardous	SLS=Safe
Failure	Failure	1	0
Failure	Success	1	0
Success	Failure	1	0
Success	Success	0	1

Table 7.9: CPT of P(SBV| DP, F, B, V)

DP	F	B	V	SIV=Hazardous	SIV=Safe
Failure	Failure	Failure	Failure	1	0
Failure	Failure	Failure	Success	1	0
Failure	Failure	Success	Failure	1	0
Failure	Failure	Success	Success	1	0
Failure	Success	Failure	Failure	1	0
Failure	Success	Failure	Success	1	0
Failure	Success	Success	Failure	1	0
Failure	Success	Success	Success	1	0
Success	Failure	Failure	Failure	1	0
Success	Failure	Failure	Success	1	0
Success	Failure	Success	Failure	1	0
Success	Failure	Success	Success	1	0
Success	Success	Failure	Failure	1	0
Success	Success	Failure	Success	1	0
Success	Success	Success	Failure	1	0
Success	Success	Success	Success	0	1

7.3.3 SITUATIONAL NETWORK DEVELOPMENT

The higher level situation (i.e. SAV), which can be inferred from the independent situations, has three physical objects which are safety barriers in the environment, as shown in Table 7.10; the states and prior probabilities of these objects are set in the same way as the basic objects of the independent situations. In addition, SAV has a consequence node, which has several states representing probable accidents, as shown in Table 7.11. Because of the lack of historical data, the CPT of SAV is set using expert judgment, as shown in Table 7.12. The expert judgment has been made by an expert with good knowledge and experience in the oil industry. The prior probability of the higher level situation, i.e. SAV, is set to 1 for Safe state and 0 for Hazardous state, and it is assumed that the environment is initially safe.

Table 7.10: SAV objects and symbols

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

Table 7.11: The consequences of SAV

Consequence	Symbol	Loss ($)	Probability
Explosion	C1	5E+06	6.76E-08
Fire with low death and high property damage	C2	3E+06	5.19E-05
Fire with high death and moderate property damage	C3	4E+06	1.62E-06
Fire with low death and moderate property damage	C4	2E+06	0.001246
Vapour cloud with possibility of ignition	C5	1E+05	0.011693
Safe state	C6	0	0.987008

Table 7.12: CPT of P(SAV| SAV, SBV, SHT, SLS)

SAV	SLS	SBV	SHT	SAV=Hazardous	SAV=Safe
Hazardous	Hazardous	Hazardous	Hazardous	1	0
Hazardous	Hazardous	Hazardous	Safe	1	0
Hazardous	Hazardous	Safe	Hazardous	0.6	0.4
Hazardous	Hazardous	Safe	Safe	0.05	0.95
Hazardous	Safe	Hazardous	Hazardous	0.98	0.02
Hazardous	Safe	Hazardous	Safe	0.6	0.4
Hazardous	Safe	Safe	Hazardous	0.6	0.4
Hazardous	Safe	Safe	Safe	0.05	0.95
Safe	Hazardous	Hazardous	Hazardous	0.98	0.02
Safe	Hazardous	Hazardous	Safe	0.95	0.05
Safe	Hazardous	Safe	Hazardous	0.5	0.5
Safe	Hazardous	Safe	Safe	0.05	0.95
Safe	Safe	Hazardous	Hazardous	0.95	0.05
Safe	Safe	Hazardous	Safe	0.05	0.95
Safe	Safe	Safe	Hazardous	0.5	0.5
Safe	Safe	Safe	Safe	0.01	0.99

A temperature controller reports the temperature of the inside of the tank and a temperature sensor reports the temperature of the production unit. In addition, there is a sensor which shows the temperature of the outside environment. SHT can be inferred by the sensor which reports the temperature of the inside of the tank, and SBV can be inferred by the sensor which reports the temperature of the production unit; however the temperature of the production unit is affected by the outside temperature. Therefore, the appropriate connection between situations and observable variables are set as shown in Figure 7.9.

The situational network illustrated in Figure 7.9 shows that the situations of interest in which higher level situations are coloured red and first level situations are coloured blue, the objects are shown in yellow, and observable variables are depicted in green. The time difference of one time step is set to one minute. The temporal arc points to the SAV situation itself, as it is assumed that the situation is formed after a time interval which is longer than one minute. The interpretation is that the vapour accumulates when the high temperature persists for a while inside the tank, or there is a large spill from the storage system and operation of the ventilation system is unable to disperse the vapour.

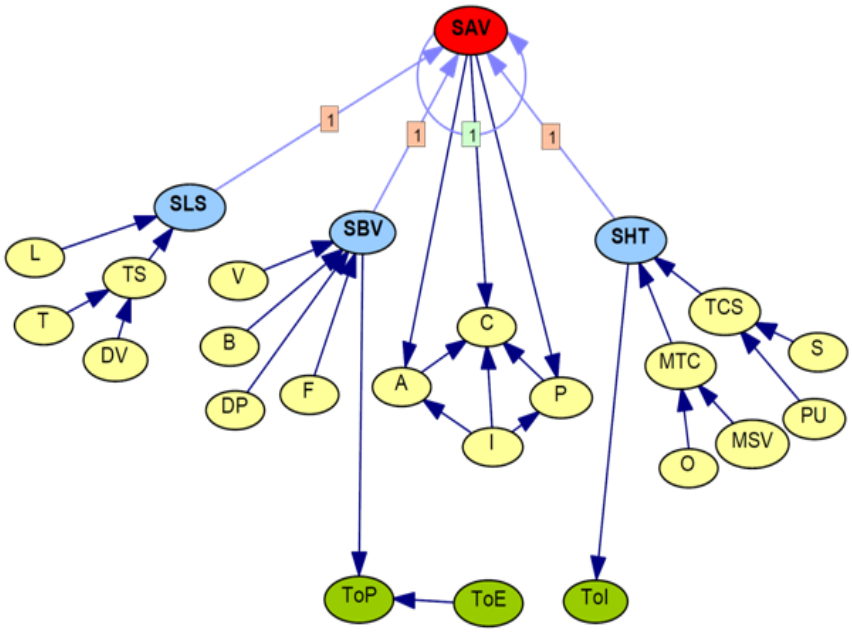


Figure 7.9: The ink vehicle mix tank situational network

7.3.4 Situational Network Evaluation

The sensitivity analysis is conducted to evaluate the developed situational network. Examination of the model at time *t* reveals that when the failure probability of S is set to 1 (i.e. failure of sensor), this results in a revised failure probability of 1 from 0.23 for TCS, and a hazardous probability of 0.04 from 0.01 for SHT. Similarly, at time *t*, when the failure probability of MSV is set to 1 (i.e. failure), the posterior probability of MTC and SHT is

increased to 1 from 0.04 and 0.043 respectively. Both these failures result in a hazardous probability of 0.5 from 0.01 for SAV at time *t+1* (temporal dependency). Likewise, when at time *t* the failure probability of F is set to 1, this results in an increased hazardous probability of 1 from 0.07 for SBV, and in a hazardous probability of 0.95 from 0.5 for SAV at time *t+1*. Equally, when at time *t* the failure probability of L is set to 1, the probabilities of SLS and SAV are increased to 1 and 0.98 from 0.001 and 0.95.

7.3.5 The SASS Performance

On 22 November 2006, the temperature of the mixing tank and the production unit started to increase; the former deviated from normal value at 9:10 AM and the latter deviated from normal value at 9:15 AM. The temperature of the outside environment was steady at 12 °C. The trend of observable variables for 60 minutes is illustrated in Figure 7.10, together with the fuzzy partitioning values of ToI and ToP. The fuzzy partitioning value of ToE is omitted because it was steady in its normal range. These data can be interpreted as ground truth data to evaluate the performance of the proposed system.

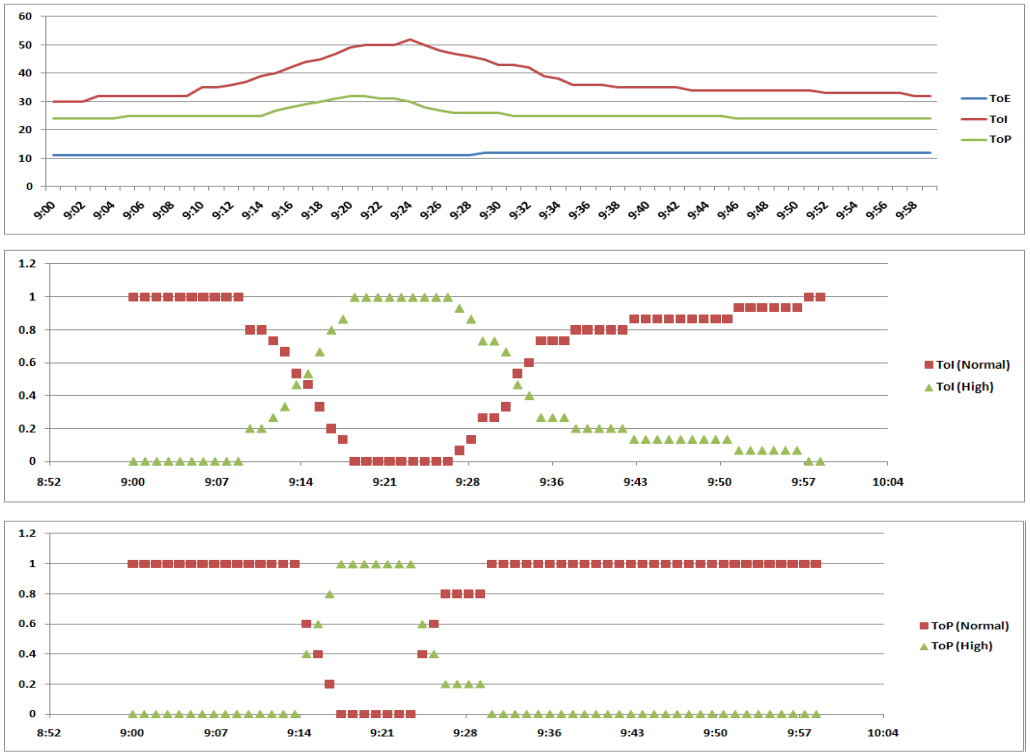


Figure 7.10: The observable variables and their fuzzy partitioning values

By assigning the primary probabilities to the DBN-based situational network, one minute after the start of the period, i.e. 9:01 AM, the probability of SAV is 0.01 and the probabilities of the consequence states are calculated as shown in Table 7.11. As can be seen, the safe state is the most probable consequence of SAV. The total loss of SAV, i.e. its severity, can be calculated by multiplication of the probabilities and losses of consequence, which are about \$3.82E+03. Therefore the estimated risk level of SAV is 1.3, which means that the current risk level of SAV is acceptable. It is worth noting that for first level situations, i.e. SHT, SBV and SLS , the accumulated vapour can be considered as their consequence, in which the degree of loss is about \$1E+05.

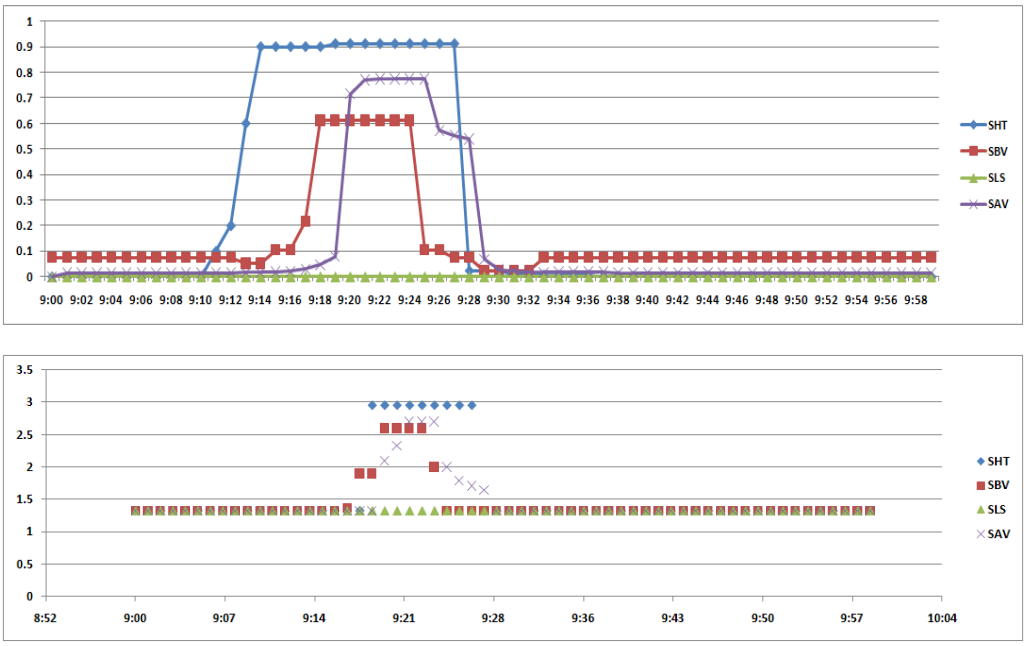


Figure 7.11: The posterior probabilities and risk levels of situations

By assigning the fuzzy soft evidence which the data preparation component provides for the situation assessment component, the posterior probabilities of the situations are updated during the period as well as their risk levels, as shown in Figure 7.11. As can be seen, the risk level of S^{HT} is TNA from minutes 15 to 27 and the risk level of S^{BV} is TNA from minutes 20 to 24. The risk level of S^{LS} is acceptable during this period. The risk level of S^{AV} is TNA from minutes 22 to 25 exactly after increasing the risk level of S^{BV}, which is because

of the assumption that the local and area ventilation systems have the ability to disperse the vapour. However, there was a one minute delay because of the temporal definition. After minutes 24, the risk level of SAV has been reduced to an acceptable level because the risk level of SBV has been decreased to an acceptable level.

The system is set to trigger an alarm for every situation which has a risk level more than 2.5, i.e. tolerable not acceptable. At 9:16 AM when the risk level of SHT 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 PU. New evidence (success of the PU system) showed that the failure of the tank's sensor was the most probable factor. Considering the result of the situation assessment, maintenance decisions were made to recover the situation. The proposed approach helps the operator in hazardous situation to prevent accidents, but it can present the factors which contribute to the creation of an accident or a specific consequence as well. For instance, if at 9:26 AM a fire with low death and moderate property damage (C4) is reported, the posterior probability updating from this evidence shows that the tank sensor failure or leakage from the transfer piping and belt failure cause the accumulated vapour, and the failure of the ignition barrier creates the fire.

7.4 SUMMARY

This chapter investigated the performance of the SASS in two chemical mixing tank environments in one of which because of poor operator's SA a tragic explosion killed one person, injured two employees, and caused significant assets loss. As has been shown, the results demonstrate that the SASS provides a mathematically consistent system for dealing with incomplete and uncertain information to help operators maintain the risk of dynamic situations at an acceptable level.

Chapter 8:

A MULTI–PERSPECTIVE SITUATION AWARENESS EVALUATION APPROACH

8.1 INTRODUCTION

As explained in Chapter 4, the SASS has been partially validated by a sensitivity analysis technique carried out to evaluate the situation models. The aim of this chapter is to fully and systematically evaluate the performance of the SASS based on related SA measures. SA measures determine the degree to which design concepts and new technologies improve or degrade an operator's SA (Endsley 1995a). SA measures are therefore a critical part of a system and procedural design process, and such evaluation efforts ensure that new systems, procedures or interfaces have improved SA rather than degraded it.

Unfortunately, due to the lack of a universally accepted SA model, there are difficulties when trying to measure SA. Measures of SA, in general, try to infer SA from other factors that are easier to assess (i.e. indirect measures), or attempt to obtain it directly. Indirect measures approach the issue by inferring how much SA an operator has acquired by assessing the cognitive processes that contribute to the development and maintenance of SA, or by assessing relevant aspects of performance in relation to the interaction between operators and systems. Behavioural, performance and process measures may thus be relied

on to make these assessments; however, because the quality of decision making and task execution, independent of SA, may be influenced by many factors, the use of indirect measures alone to assess SA are not recommended (Endsley, Bolté & Jones 2003). Unlike indirect measures, direct metrics try to measure SA by comparing operators' responses with the real world, or by asking an expert to assess the quality of operators' SA during a time interval. Endsley believes that workload assessment, human/system performance analysis, and objective SA measurements are the best ways to evaluate system design (Endsley, Bolté & Jones 2003); however, even the most successful measures are not able to assess operators' SA during real-time operations (Jones & Endsley 2004). Endsley et al. use SAGAT[1], which is a direct objective technique, and SART[2], which is a direct subjective technique, to assess air traffic controllers' SA using a traditional Air Traffic Control (ATC) display and an enhanced ATC display (Endsley & Garland 2000). They then compare the sensitivity and validity of both techniques with the results of a real-time probe approach. The results show that the on-line probe approach and SART are not sensitive to changes in conditions, whereas the SAGAT scores are sensitive to interface changes. In another study, Endsley et al. utilize SAGAT and SART in the assessment of fighter pilots' SA. Because there is no correlation between measures, they conclude that the objective SA assessment by SAGAT is not related to the subjective SA assessment by SART (Endsley, Selcon, et al. 1998a). Salmon et al. also utilize SAGAT and SART to assess participants' SA during a military planning task (Salmon, Stanton, Walker, Jenkins, Ladva, et al. 2009). They conclude that different SA measures assess different aspects of SA. The literature review reveals that the majority of SA measurement applications are limited to aviation and military domains and their usefulness in evaluating safety-critical decision support systems has not been studied sufficiently.

[1] Situation Awareness Global Assessment Technique

[2] Situation Awareness Rating Technique

In this chapter, a multi-perspective evaluation approach considering three SA metrics is proposed to address the suitability of the SASS. The approach includes two direct SA measures, SAGAT and SART, and one workload measure called NASA-TLX[1] which is a multi-dimensional scale to estimate the workload of operators. The evaluation process of the SASS is conducted through the participation of ten operators who investigate abnormal situations in a chemical plant using a virtual plant user interface, both with and without the support of the SASS.

8.2 INTENDED SAFETY-CRITICAL ENVIRONMENT

The residue treater unit explained in Chapter 6 is considered, and routine operation is chosen for the evaluation. The plant has a traditional virtual user interface that it is used for leading the operation. In addition, the human-computer interface of the SASS for this plant has been developed based on the capabilities of OOBNs.

8.2.1 VIRTUAL PLANT USER INTERFACE

The virtual plant user interface, shown in Figure 8.1, displays the necessary information for operators to monitor the operation of the residue treater unit and manipulate the components. Flow directions are indicated by vertical and horizontal lines between components. Instantaneous values, such as pressure, flow rate, liquid level and temperature are displayed as gauge values adjacent to their respective components. If the values exceed high or low limits, the system triggers an alarm and indicates to the user that the values that appeared as a flashing value have fallen outside of their allowable range. By mouse-clicking any component, the user interface provides a pop-up window that represents the available options to deactivate the alarm or turn the system pumps on and off, as well as offering maintenance suggestions.

[1] NASA Task Load Index

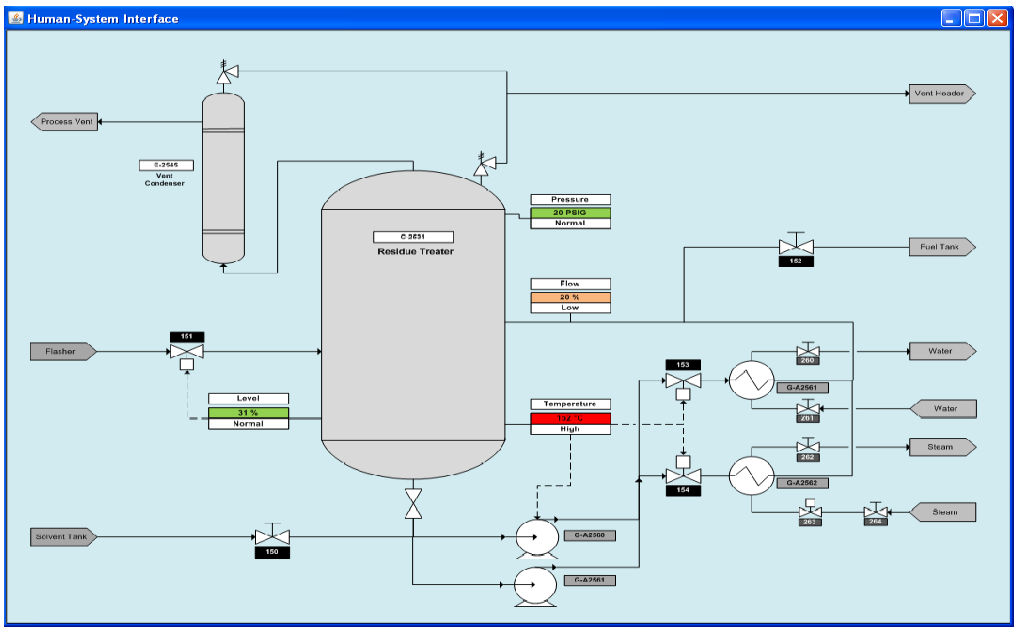


Figure 8.1: **Virtual plant user interface**.

8.2.2 The Human–Computer Interface of the SASS

Because modelling the situational network for the residue treater led to complex models, OOBNs were used to develop the SASS interface. Based on OOBN characteristics, the situational network is simplified as instance nodes in Figure 8.2, while its collapsed form is represented in Figure 8.3. The human-computer interface of the SASS is shown in Figure 8.4.

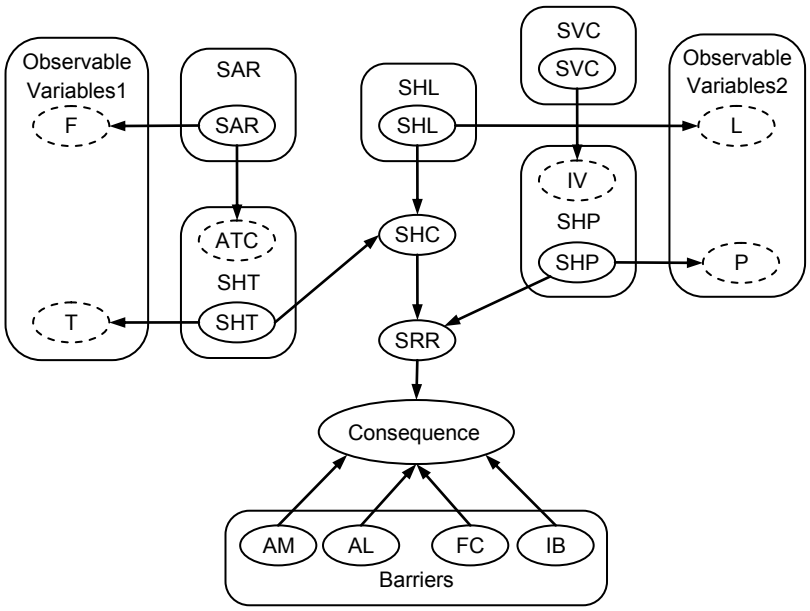


Figure 8.2: **The residue treater situational network based on OOBN characteristics**

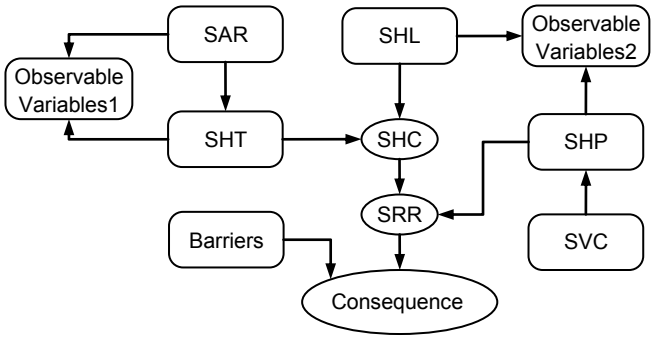


Figure 8.3: Collapsed form of the residue treater situational network

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 for the hazardous situation.

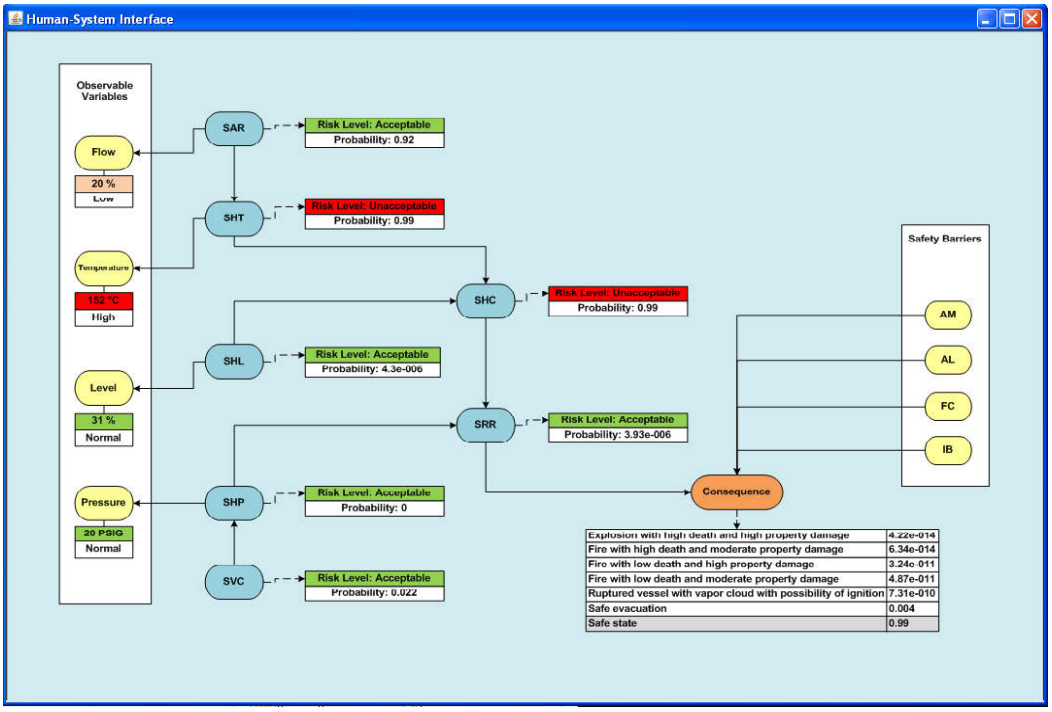


Figure 8.4: The human-computer interface of the SASS

8.3 A Multi-Perspective SA Evaluation Approach

Our multi-perspective evaluation approach, illustrated in Figure 8.5, consists of SAGAT, SART and NASA-TLX metrics to measure different aspects of an operator's SA.

SAGAT is used in this study as an objective means by which to quantify SA. Subjective measures of SA are not sufficient because of limitations in the veracity of self-ratings and observer ratings of SA. Self-ratings of SA may not be truly representative of actual SA because operators are limited to their own perceptions of the task environment and may not have an accurate picture of reality by which to judge the completeness or correctness of their perceptions (Endsley 1995b). Observer ratings of SA are limited by the fact that trained observers often have information about the simulation and reality, but may have only limited knowledge of an operator's concept of a situation. The SAGAT assesses SA by comparing the real-time conditions of the environment with the SA reported by the operator. Operators are queried about aspects of the environment and their responses are compared with reality. To achieve this, operator-in-the-loop simulation exercises are managed by a personal computer (PC) that employs the design concepts of interest, in this case the virtual user interface alone in one monitor and the human-computer interface of the SASS in an adjacent monitor. The simulation activity suspends at randomly selected intervals, the displays are blanked, and queries are administered to the participant. Data collected by the PC are used to score the participant's responses as correct or incorrect based on what was actually happening in the scenario at that time.

SART assesses SA by asking operators to rate the quality of their SA during a specified period. This rating is then used to compare the quality of SA when the virtual user interface is used alone and when it is used with the SASS. The SART is inexpensive, easy to perform, simple to analyse, and employable without the performance being disrupted. However, it may include inaccuracies due to operator self-reporting as explained before. Therefore, the use of SART in conjunction with SAGAT can engender confidence that the levels of operator SA provided are accurate.

In addition to the SAGAT and SART, the approach includes NASA-TLX to represent the workload of operators when they are managing situations with both systems. This subjective measure of workload was selected because of its demonstrated reliability and

sensitivity as an overall workload measure in empirical investigation. It was chosen over other potential objective secondary task and physiological measures of workload because of concerns regarding the obtrusiveness (primary task interference) and sensitivity of these measures. In addition, workload effects must be indirectly inferred from differences revealed through physiological measures. To perform this assessment, the operators answer questions regarding their experience with the systems. The results are used to determine which aspects of the work contribute the most to operators' perceived workload. Computerized SART and NASA-TLX questionnaires are administered post-trial using the PC.

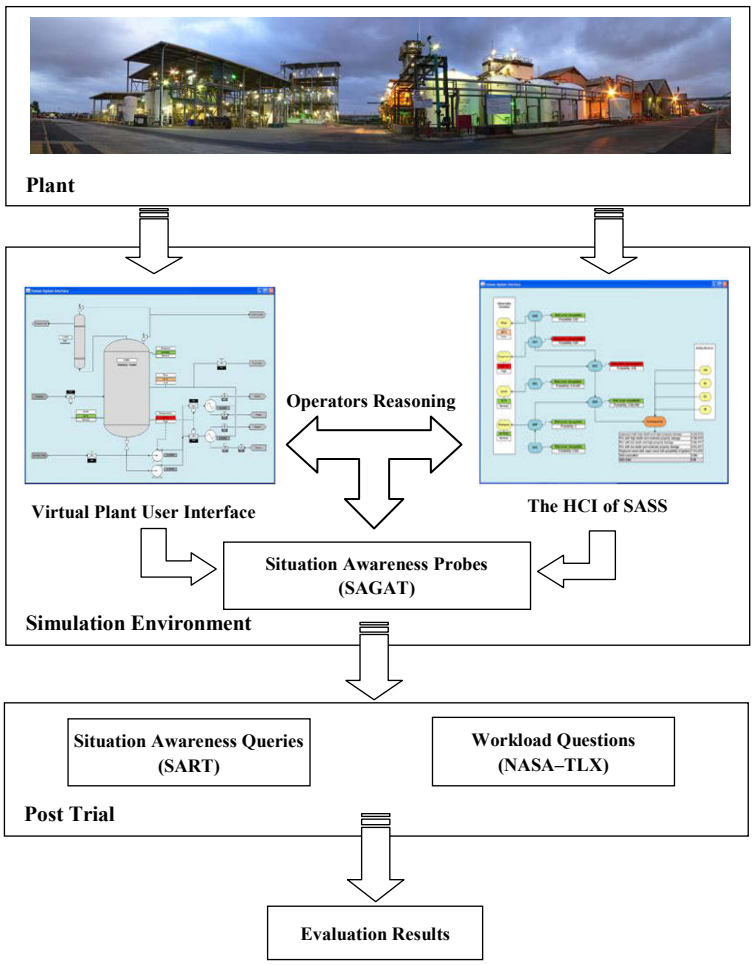


Figure 8.5: A multi-perspective evaluation approach.

8.3.1 PARTICIPANTS

Ten operators currently involved in the operation of an oil refinery served as participants. All participants became familiar with the simulation software and features of the SASS used in the present study (M=5.40 yrs, SD=1.42). It is assumed that the operators are decision makers in the residue treater unit, where the current states of processing components are displayed in the GUI. Based on observed values, they have to identify abnormal situations and the actions required to address those abnormal situations. The test people are introduced to the characteristics of abnormal situations in the environment before the evaluation.

8.3.2 SCENARIO DEVELOPMENT

To prepare for a routine operation, the vessel is filled with solvent and heated. Methomyl is added to the residue treater and a normal recirculation loop flow is activated to mix the concentrated methomyl feed with preheated solvent in the residue treater. The operator opens the feed control valve and begins feeding flasher bottoms into the vessel. At normal flow rate, it takes approximately 10 minutes to fill the residue treater to 50%, the normal operating level. The recirculation pump is then started. Two 40-min scenarios are defined. Table 8.1 shows the timeline of Scenario 1. In this scenario, the residue treater liquid level reaches approximately 51% after 17 minutes and the temperature ranges between 130 and 135 °C. The pressure is 22 psig. The temperature begins to rise steadily about 2 degrees per minute when the recirculation flow suddenly drops to zero after 30 minutes. In less than three minutes, the temperature is at 147 °C, the highest safe operating limit.

Table 8.1: **Scenario 1 timeline**.

Time into scenario (min)	Event
00:00	Scenario is started
05:00	Level reaches 30%.
07:00	Flow is steady at normal rate and temperature is about 130°C.
09:00	Automatic feed valve is opened and flasher bottoms are introduced into the vessel.
17:00	Level reaches 51% and the pressure is 22 psig.
18:00	Automatic feed valve is closed.
23:00	The temperature begins to rise steadily about 2 degrees per minute.
30:00	The recirculation flow suddenly drops to zero.
31:00	The temperature is at 147 °C, the highest safe operating limit.
31:00	The estimated risk level of SAR increases from 1.32 (acceptable) to 2.95 (tolerable not acceptable).
32:00	The risk level of SHP is steady and acceptable.
32:00	The risk level of SHT and SHC increases from acceptable (i.e. 1.32 and 1.65 respectively) to tolerable not acceptable (i.e. 2.95 and 3 respectively).
37:00	The risk level of SRR remains acceptable.
39:00	Scenario is ended.

8.3.3 OBJECTIVE MEASUREMENT

Situation awareness is first measured applying SAGAT. The operators execute the experimental scenarios twice, once using the virtual plant user interface without the SASS and once with the SASS. Five freezes occur at randomly selected intervals and they are unpredictable by the operators. At the time of the freeze, the displays are blanked and the simulations are suspended. Each freeze lasts approximately 2 minutes. The thirteen questions summarized in Table 8.2 are derived from the GDTA results shown in Table 5.1.

Responses to all the queries are collected at each stop via an on-line questionnaire system adjacent to the operator's station. All responses are scored as 1 for a correct answer and 0 for an incorrect answer. The total SAGAT scores are calculated by summing all the correct responses for each participant, giving a total possible score of 13. Table 8.3 shows the SAGAT scores under different interfaces.

Table 8.2: Probe questions for Scenario 1.

Time into scenario (min)	SA level	Question
07:00	Level 1	What is the current level of temperature? (Low, Normal, High)
07:00	Level 1	What is the current level of flow? (Very low, Low, Normal)
18:00	Level 1	Climbing, decreasing, or steady: Which is correct for liquid level?
24:00	Level 2	Which abnormal situation threatens the unit? (SHL, SVC, SAR)
24:00	Level 2	What is the most probable explanation? (Failure of the recirculation pump, Failure of cooling water isolation valve, Failure of automatic level control)
24:00	Level 3	What is the current level of risk of the abnormal situation? (Acceptable, Tolerable acceptable, Tolerable not acceptable, Not acceptable)
31:00	Level 1	Climbing, decreasing, or steady: Which is correct for temperature?
31:00	Level 2	Which abnormal situations threaten the unit? (SHT, SHC, SRR)
31:00	Level 2	What are the best actions for reduction or containment of risk?
31:00	Level 3	What will be the level of risk? (Acceptable, Tolerable acceptable, Tolerable not acceptable, Not acceptable)
32:00	Level 3	What are the risk levels of SHT and SHC? (Acceptable, Tolerable acceptable, Tolerable not acceptable, Not acceptable)
32:00	Level 2	What are the best actions for reduction or containment of risk? (Temperature transmitter, Manual water valve, Automatic feed valve)
32:00	Level 3	Is SRR abnormal? (Yes, No)

Table 8.3: The SAGAT scores under different interfaces.

Virtual system	SA level							
	Perception		Comprehension		Projection		Overall	
	M	*SD*	*M*	*SD*	*M*	*SD*	*M*	*SD*
Virtual plant user interface	3.10	0.76	0.60	0.48	0.80	0.17	4.50	2.27
Virtual plant user interface plus SASS	3.80	0.17	4.50	0.27	3.30	0.45	11.60	1.37

The mean total SAGAT score without using SASS is 4.50 (SD =2.27). The highest total SAGAT score is 7 and the lowest score is 3. The mean overall SAGAT score for level 1 SA probes is 3.10 (SD = 0.76) while it is 0.60 (SD = 0.48) and 0.80 (SD =0.17) for levels 2 and 3, respectively. As can be seen, the SAGAT scores for levels 2 and 3 are much lower in comparison with level 1. The mean total SAGAT score with support of the SASS is 11.60 (SD =1.37). The highest total SAGAT score is 13 and the lowest SAGAT score is 9. The SAGAT score decomposition corresponding to SA levels is 3.80 (SD = 0.17) for level 1,

4.50 (SD = 0.27) for level 2, and 3.30 (SD = 0.45) for level 3. Analysis of variance (ANOVA) shows that the SAGAT rating of SA is significantly higher with the support of SASS than without $F(1,18)=137.90$ $p<0.001$. The results particularly indicate the improvement of SA in levels 2 and 3 with the support of the SASS.

8.3.4 SUBJECTIVE MEASUREMENT

Situation awareness is also measured using the SART. The SART questionnaire requires participants to use a 1-7 scale (1=Low and 7=High) and to rate 10 factors (shown in Table 8.4) in three categories: understanding of the situation, demand on attention resources, and supply of attention resources. Responses to the SART questions result in a score for each of the three major factors, as well as an overall score for SA. The overall SART score is calculated as SA=U-(D-S) where U is a sum for understanding, D is summation of attention demand, and S is the summation of attention supply.

The SART rating of SA is inferred to be significantly higher with SASS than without it, $F(1,18)=228.57$, $p<0.001$. The mean overall SART score when using the virtual plant user interface alone is 19.2 (SD=1.51) while the mean overall SART score in obtaining support of SASS is 27.2 (SD=1.28). The highest and lowest overall SART scores for the former are 21 and 17, and for the latter, 29 and 24. Participant scores are examined for each SART dimension and these show that the result is mainly attributed to differences in subject rating of understanding ($p<0.001$).

Table 8.4: The SART factors.

Domain	Construct	Definition
Understanding	Information quantity	The amount of knowledge that an operator receives and understands
	Information quality	The goodness degree of knowledge that an operator gains
	Familiarity with situation	The degree of being familiar with the situation
Attention Demand	Instability of situation	The situation is unstable and likely to change suddenly
	Variability of situation	The number of variables in the situation that are changing
	Complexity of situation	The situation is complicated or straightforward
Attention Supply	Arousal	The degree of alertness that the operator has for doing the activity
	Spare mental capacity	The amount of mental ability that the operator has for new variables
	Concentration of attention	The number of aspects in the situation that demand the operator's concentration
	Division of attention	The extent to which the operator's attention is divided

8.3.5 WORKLOAD MEASUREMENT

The NASA-TLX consists of six independent sub-scales: Mental, Physical, Temporal Demands, Frustration, Effort, and Performance. Users are asked to rate the perceived workload on a continuous scale (one scale per dimension) with three anchors (low, medium, and high). The results of these tools can be displayed as individual workload dimensions, or as overall workload scores. The five questions shown in Table 8.5 were asked.

Table 8.5: The NASA-TLX questions.

Domain	Question
Mental Demand	How mentally demanding was the task?
Temporal Demand	How temporally demanding was the task?
Performance	How successful were you in accomplishing what you were asked to do?
Effort	How hard did you have to work to accomplish your level of performance?
Frustration	How insecure, discouraged, irritated, stressed, and annoyed were you?

The participants' answers are scaled to the range of 0 to 100 as shown in Figure 8.6. As can be seen, working with the SASS produces better results than working without it in four domains. In just one domain, performance, the results are lower when the operators use the support system. The average of the results from the five questions is also depicted in Figure

8.6. It can be concluded that working with the proposed SASS for this specific environment results in a lower workload for decision makers than when they work without it.

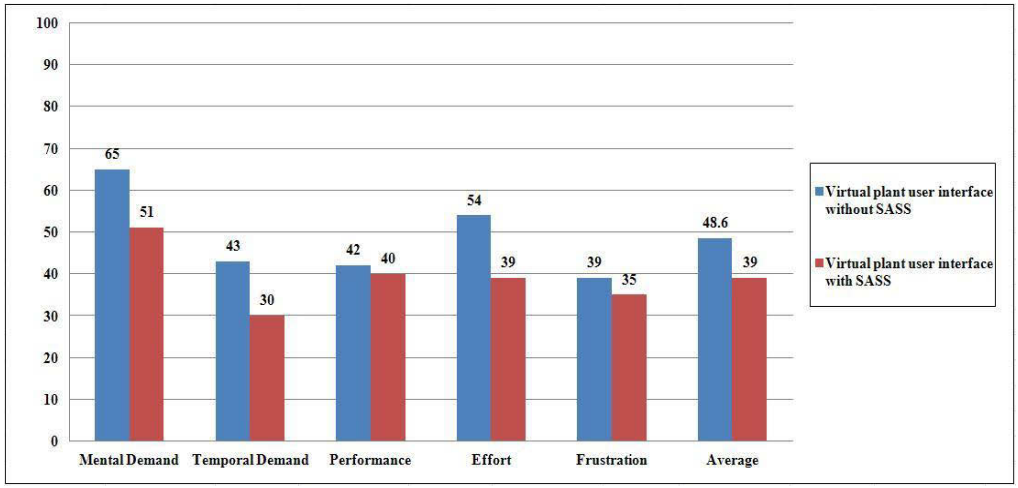


Figure 8.6: NASA Task Load Index results.

8.3.6 CORRELATION BETWEEN SA MEASURES

The analysis of the correlation between SAGAT and SART is presented in Table 8.6. As can be seen, there are no significant correlations between the participants' SA scores assessed by these two measures. This fact shows that the SART and SAGAT measurements evaluate different items in respect of SA during the study. In other words, they view SA differently and measure different elements of operator awareness.

Table 8.6: SAGAT and SART correlations.

	SART	SART U	SART D	SART S
SAGAT	-0.26681 *Not Sig*	0.285942 *Not Sig*	-0.1122 *Not Sig*	-0.60033 *Not Sig*
SAGAT Level 1	-0.37139 *Not Sig*	0.149256 *Not Sig*	0.234261 *Not Sig*	-0.37139 *Not Sig*
SAGAT Level 2	-0.37139 *Not Sig*	-0.0995 *Not Sig*	-0.37139 *Not Sig*	-0.37139 *Not Sig*
SAGAT Level 3	0.058001 *Not Sig*	0.481736 *Not Sig*	-0.21951 *Not Sig*	-0.52201 *Not Sig*

If $\alpha = 0.05$ is chosen, the ANOVA analysis reveals that there is no significant effect in the use of the virtual plant interface, with or without SASS, for this specific environment. It can generally be concluded that to demonstrate that a better workload is produced for operators, the SASS should be validated through a variety of scenarios in different environments with more participants. In addition, as the results strongly depend on the

visualization of the user interface, the system should be evaluated by using a range of visualization techniques for the recognized situations.

8.4 SUMMARY

The importance of cognitive decision support systems for managing abnormal situations in safety-critical environments has been highlighted and the situation awareness support system (SASS) that assists operators to understand and project situations in such environments has been developed in Chapter 5. In addition, the SASS has been partially validated by a sensitivity analysis that is carried out to evaluate the knowledge-base of the system. To fully and systematically evaluate the SASS, it needs to be empirically tested to identify any unforeseen issues that might negatively impact operator SA. Therefore, appropriate measures must be employed to assess the level of operator SA in interaction with the SASS. This chapter demonstrated the multi-perspective approach for this purpose. The approach consists of two direct SA measurements, SAGAT and SART, and a workload metric called NASA-TLX. SAGAT narrowly focuses on questions and is not sensitive to SA changes. In contrast, it is sensitive to system manipulation, automation manipulation, expertise differences, and changes in task load and factors affecting operator attention. SART is also a measure that is sensitive to task difficulty, operator experience and SA changes. Ten experienced operators participated in this study to respond to the simulation scenarios using a virtual plant user interface, with and without the support of the SASS. The results show that the SASS improves operator SA, particularly in levels 2 and 3. No significant correlations between the participants' SA scores have been found. In addition, it is concluded that the SASS reduces the workload of operators, although further investigations in different environments with a larger number of participants have been suggested.

Chapter 9:

CONCLUSION AND FUTURE WORK

9.1 CONCLUSIONS

Today, in many safety-critical systems the role of operators has shifted from manual controllers to supervisors or decision-makers who are responsible for extensive cognitive tasks (Ha & Seong 2009). Operators are often moved to a control room far away from the physical process and have to rely on human computer interaction (HCI) principles to observe and comprehend the overwhelming amount of rapidly changing data for processing. For instance, in the 1970s, a typical operator manually controlled approximately 45 control valves in one process unit. Today, an operator controls, on average 175 control valves through an automation system interface. More specifically, the number of observable process variables in the power distribution sector grew from 200,000 to 700,000 between the years 1990 and 2000 (Burmester, Komischke & Wust 2000). It is widely accepted that more data does not equate to more information. In many cases automation has only worsened the problem (Endsley & Kiris 1995), and operators are required to handle more data and more responsibility. Although experienced users tend to filter through the over-abundance of data to generate information and acquire good SA, even the most expert operator can become swamped by the excessive amount of data provided by new

technologies. This has led to a huge gap between the massive amount of data produced and disseminated and the operator's ability to effectively assimilate the required data and to make a timely, accurate decision (Endsley & Garland 2000).

In the presence of all these data, complex interfaces, and dynamic situations, human error could be a serious cause of accidents in these environments. It has been found that in most industries, 70-90% of accidents are attributed to human error (Isaac, Shorrock & Kirwan 2002). Traditionally, there are two approaches to prevent human error during operation of safety-critical systems. The first approach focuses on the provision of better training programs for operators, and the second one aims to improve operator support systems (Lee & Seong 2014). However, it has been shown that in abnormal time pressure situations, ordinary training does not improve the quality of decision making (Zakay & Wooler 1984), therefore the role of cognitive support systems to assist operators in such situations is highlighted (Naderpour, Lu & Zhang 2014b). This study introduced a new system for SA enhancement called the Situation Awareness Support System (SASS). This chapter summarizes the conclusions of this research and nominates some future research directions.

This research has been motivated by this fact that the SA, a cognitive human factor, has been recognized as an important contributing factor in recent accidents of safety-critical systems. It has also been realized that the SA is a critical factor in managing abnormal situations when operators are under time pressure to make quick and accurate decisions. This research makes the following main contributions:

(1) It proposes a new definition for abnormal situations. It defines the situation as a set of circumstance in which a number of objects may have relationships with one another and the environment, and a hazardous situation as a possible circumstance immediately before harm is produced by a hazard. Therefore, an abnormal situation is defined as a hazardous situation if its risk is not acceptable. In abnormal situations, a well-trained operator should comprehend a malfunction in real time by analyzing

alarms, assessing values, and recognizing unusual trends indicated by multiple instruments. In such a situation, many alarms from different systems are frequently triggered at the same time, making it difficult for the operator to make a decision within a very short time frame. If several abnormal situations occur at once, decisions have to be made in even less time. Operators are usually unable to judge which situation should be given priority when confronted with complex abnormal situations such as these (Hsieh et al. 2012; Jou et al. 2011). Based on the proposed definition, 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).

(2) It develops an abnormal situation modelling method by exploiting the specific capabilities of BNs. The ASM method models the operators' mental model using BNs to represent these cause–effect relationships between objects in a situation. It also describes how the states and CPTs of objects in the models should be determined, and how they should be connected to each other to create the situational networks. As the situations of interest can be inferred by some observable variable distributed in the environment, the ASM method explains how the situations can be connected to observable variables.

(3) It develops a situation assessment method that employs a fuzzy logic system to resemble human thinking when it assesses a situation. The use of linguistic variables allows operators to express their knowledge in the form of related imprecise inputs and outputs. As has been shown, the 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.

(4) It develops a cognition-driven DSS called the Situation Awareness Support System. Some types of DSS, such as model-driven, data-driven, communication-driven, document-driven, and knowledge-driven have achieved increased popularity in various domains. Model-driven DSSs are complex systems that help to analyse decisions or choose between different options. Data-driven DSSs are used to query a database or data warehouse to seek specific answers for specific purposes. Most communications-driven DSSs are targeted at internal teams, including partners. Their purpose is to help the conduct of a meeting, or for users to collaborate. Document-driven DSSs, which are more common, are utilized to search web pages and find documents on a specific set of keywords or search terms. Knowledge-driven DSSs are a catch-all category covering a broad range of systems covering users within the organization setting it up, but may also include others interacting with the organization (Niu, Lu & Zhang 2009). Unlike these DSSs, cognitive DSSs have not been researched sufficiently, albeit they have long been recognized as being worthy of consideration (Chen & Lee 2003). Just as a cognitive process refers to an act of human information processing, so a cognition-driven DSS refers to assisting operators in their decision–making from a human cognition perspective. The SASS consists of five major components: 1) knowledge base, 2) situation data collection, 3) situation assessment, 4) situation recovery, and 5) human-computer interface.

(5) It illustrates the performance of the SASS in three safety-critical environments that have accidents with grave consequences in US recent history. The case studies included: a residue treater at a methomyl production unit, a tank equipped with steam coils at a chemical plant, and an ink vehicle insulated mix tank at a paint manufacturing company. The use of case studies could add a sense of urgency or

reality to the proposed system, and showed how the system works. In addition, they provided real applications of the proposed system and helped to validate its performance.

(6) It develops a multi-perspective evaluation approach for full and systematic validation of the SASS. The approach consists of three SA metrics: the Situation Awareness Global Assessment Technique, the Situation Awareness Rating Technique, and the NASA Task Load Index. The first two metrics are used for direct objective and subjective measurement of SA, while the third is used to estimate the workload of operators. A computerized system was developed in order to implement the approach.

9.2 FUTURE WORKS

Future directions of this research can be summarized in the following perspectives:

(1) Due to the significant presence of teams in contemporary organizational systems, the construct of team SA is currently receiving increased attention from the human factors community. A team can be defined as consisting of two or more people, dealing with multiple information resources, who work to accomplish some shared goal. Distributed teams comprise members interacting over time and space via technology mediated communication. Team performance itself comprises two components of behaviour, teamwork (team members working together) and task-work (team members working individually). 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. Coordination is accomplished using a chain of command and internal communications systems to relay status to the appropriate decision makers. These team members have a common goal and perform specific roles in their interaction with elements in the task environment. The first future direction of the research, therefore, is to extend the proposed system to a distributed system that applies the team/distributed situation awareness concept.

(2) Most of traditional SA measurement studies are conducted through qualitative analysis methods. Qualitative techniques cannot be satisfactorily used to achieve quantitative SA measurements; thus, quantitative techniques based on statistical models (Kirlik & Strauss 2006) and inference models (Ma & Zhang 2008) have been merged. However, a common drawback is that these quantitative techniques completely replace qualitative information with numeric values. The existence of uncertainty is another reality of most operational human–machine systems. In the course of processing information, one applies background knowledge (forms a mental model of the situation) and uncertainty reasoning to handle perceptions with uncertainty (referred to as situation models). Therefore, in developing any SA measurement, two important aspects should be considered: 1) independently measuring the contribution of technology to SA, and 2) measuring the contribution of environmental uncertainty to SA (Kirlik & Strauss 2006). In addition, research on linguistic decision making indicates that using linguistic terms is an efficient way to describe uncertain qualitative information. Therefore, in the light of research on linguistic information decisions, a SA measurement method that combines a qualitative information process and quantitative computation should be developed for evaluating SA systems.

(3) Another future study should consider automation systems with a multiple screen design. This research was designed with only one main operating screen. Future research is needed with multiple screen processes to further conceptualizations the results of the present study, to get a clearer picture of the effect of the SASS on operators' performance.

(4) Today, in many safety-critical systems, the advanced control rooms are equipped with many automated systems; however operators are still responsible for accident diagnosis and mitigation. Thus information acquisition and decision making are emphasized more than manual manipulation. Therefore HCIs should support them

to know and do more effectively and less ambiguously. The poor HCI can bring serious consequences, such as occupational accidents and diseases including stress, therefore the HCI is recently considered as an emerging risk (Flaspoler et al. 2009; Jovanovic & Balos 2012) which may jeopardize safety. Therefore, to design an adequate HCI, the specific properties and qualities of human factors as well as the working environment must be taken into account. Despite this importance, very few methods and tools have as yet been developed to assess this kind of risk in the design of HCIs. Another future research direction is to develop a new risk assessment method to evaluate HCIs in safety-critical systems. In this sense, the operators' mental models in regard to possible abnormal situations in the simulation environment along with operators' responses when they are working with the system can be utilized for proposing a new interface risk assessment methodology.

REFERENCES

Adams, M.J., Tenney, Y.J. & Pew, R.W. 1995, 'Situation awareness and the cognitive management of complex systems', *Human Factors*, vol. 37, no. 1, pp. 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 ', paper presented to the *The 18th International Conference on Automated Reasoning with Analytic Tableaux and Related Methods*, Oslo, Norway, July 6-10.

Banbury, S. & Tremblay, S. 2004, *A Cognitive Approach to Situation Awareness: Theory and Application*, Ashgate, Aldershot, UK.

Bangso, O. & Wuillemin, P. 2000, 'Top-down specification and compact representation of repetitive structures in Bayesian networks', paper presented to the *The 13th International Florida Artificial Intelligence Research Symposium Conference*, Orlando, USA, 21-23 May.

Bedny, G. & Meister, D. 1999, 'Theory of activity and situation aewareness', *International Journal of Cognitive Ergonomics*, vol. 3, no. 1, pp. 63-72.

Bobbio, A., Portinale, L., Minichino, M. & Ciancamerla, E. 2001, 'Improving the analysis of dependable systems by mapping fault trees into Bayesian networks', *Reliability Engineering & System Safety*, vol. 71, no. 3, pp. 249-60.

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*, vol. 22, no. 3, pp. 316-25.

Broughton, E. 2005, 'The Bhopal disaster and its aftermath: A review', *Environmental Health: A Global Access Science Source*, vol. 4, pp. 1-6.

Burkolter, D. & Kluge, A. 2012, 'Process control and risky decision-making: moderation by general mental ability and need for cognition', *Ergonomics*, vol. 55, no. 11, pp. 1285-97.

Burmester, M., Komischke, T. & Wust, L. 2000, 'Innovative User Interfaces in Automation Engineering by Application of Usability Engineering Methods Shown by the Example of a Three-Dimensional Plant Representation', *International Journal of Human-Computer Interaction*, vol. 12, no. 3-4, pp. 359-73.

Center for Chemical Process Safety (CCPS) 1989, *Guidelines for Process Equipment Reliability Data with Data Tables*, The American Institute of Chemical Engineers.

Chai, H. & Wang, B. 2011, 'A hierarchical situation assessment model based on fuzzy Bayesian network', paper presented to the *International Conference on Artificial Intelligence and Computational Intelligence*, Taiyuan, China.

Chan, H. 2005, 'Sensitivity analysis of probabilistic graphical models', University of California, Los Angeles.

Chatzimichailidou, M.M., Protopapas, A. & Dokas, I.M. 2015, 'Seven Issues on Distributed Situation Awareness Measurement in Complex Socio-technical Systems', *Complex Systems Design & Management*, Springer, pp. 105-17.

Chen, J.Q. & Lee, S.M. 2003, 'An exploratory cognitive DSS for strategic decision making', *Decision Support Systems*, vol. 36, no. 2, pp. 147-60.

Chemical Safety Board (CSB) 2006, *Sterigenics*, 2004-11-I-CA Washington, DC.

Chemical Safety Board (CSB) 2007, *Mixing and heating a flammable liquid in an open top tank* 2006-08-I-IL Washington, DC.

Chemical Safety Board (CSB) 2008, *Confined vapor cloud explosion*, 2007-03-I-MA, Washington, DC.

Chemical Safety Board (CSB) 2011, *Pesticide Chemical Runaway Reaction Pressure Vessel Explosion*, 2008-08-I-WV, Washington, DC.

Darwiche, A. 2008, 'Bayesian networks', *Handbook of Knowledge Representation*, vol. 3, pp. 467-509.

Das, S., Grey, R. & Gonsalves, P. 2002, 'Situation assessment via Bayesian belief networks', paper presented to the *The Fifth International Conference on Information Fusion*, Maryland, USA, July 8-11

Dekker, S.W.A. 2013, 'On the epistemology and ethics of communicating a Cartesian consciousness', *Safety Science*, vol. 56, pp. 96-9.

Dubois, D. & Prade, H. 1978, 'Operations on fuzzy numbers', *International Journal of Systems Science*, vol. 9, no. 6, pp. 613-26.

Durso, F.T., Dattel, A.R. & Banbury, S. 2004, 'SPAM: The real-time assessment of SA', in S. Banbury & S. Tremblay (eds), *A cognitive approach to situation awareness: Theory and application*, Ashgate, Aldershot, UK, pp. 137-54.

Endsley, M. 1995a, 'Measurement of situation awareness in dynamic systems', *Human Factors: The Journal of the Human Factors and Ergonomics Society*, vol. 37, no. 1, pp. 65-84.

Endsley, M.R. 1995b, 'Toward a theory of situation awareness in dynamic systems', *Human Factors: The Journal of the Human Factors and Ergonomics Society*, vol. 37, no. 1, pp. 32-64.

Endsley, M.R. 1997, 'Supporting situation awareness in aviation systems', paper presented to the *The IEEE International Conference on Systems, Man and Cybernetics*, Orlando, USA, October 12-15

Endsley, M.R. 2000a, 'Direct measurement of situation awareness: Validity and use of SAGAT', in M.R. Endsley & D.J. Garland (eds), *Situation awareness analysis and measurement*, Lawrence Erlbaum Associates, Mahwah, NJ, pp. 147-73.

Endsley, M.R. 2000b, 'Situation models: An avenue to the modeling of mental models', *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 44, SAGE Publications, pp. 61-4.

Endsley, M.R. 2006, 'Situation awareness', in G. Salvendy (ed.), *Handbook of human factors and ergonomics*, John Wiley and Sons, pp. 528–42.

Endsley, M.R., Bolté, B. & Jones, D. 2003, *Designing for situation awareness: an approach to user-centered design*, Taylor & Francis.

Endsley, M.R. & Connors, E.S. 2008, 'Situation awareness: State of the art', *IEEE Power and Energy Society General Meeting: Conversion and Delivery of Electrical Energy in the 21st Century, PES*.

Endsley, M.R., Farley, T.C., Jones, W.M., Midkiff, A.H. & Hansman, R.J. 1998, *Situation awareness information requirements for commercial airline pilots*, International Center for Air Transportation, ICAT-98-1.

Endsley, M.R. & Garland, D.J. 2000, *Situation awareness: analysis and measurement*, Lawrence Erlbaum, Mahwah, NJ.

Endsley, M.R. & Jones, W.M. 2001, 'A model of inter-and intra-team situation awareness: Implications for design, training and measurement', in E.S. M. McNeese, & M. R. Endsley (ed.), *New trends in cooperative activities: Understanding system dynamics in complex environments*, Human Factors and Ergonomics Society, Santa Monica, CA, pp. 46–67.

Endsley, M.R. & Kiris, E.O. 1995, 'The out-of-the-loop performance problem and level of control in automation', *Human Factors: The Journal of the Human Factors and Ergonomics Society*, vol. 37, no. 2, pp. 381–94.

Endsley, M.R., Selcon, S.J., Hardiman, T.D. & Croft, D.G. 1998a, 'A comparative analysis of SAGAT and SART for evaluations of situation awareness', *Proceedings of the human factors and ergonomics society annual meeting*, vol. 42, SAGE Publications, pp. 82–6.

Endsley, M.R., Selcon, S.J., Hardiman, T.D. & Croft, D.G. 1998b, 'A comparative analysis of SAGAT and SART for evaluations of situation awareness', *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 42, SAGE Publications, pp. 82–6.

Farahbod, R., Avram, V., Glasser, U. & Guitouni, A. 2011, 'Engineering situation analysis decision support systems', paper presented to the *European Intelligence and Security Informatics Conference (EISIC)*, Athens, Greece, September 12–14.

Fischer, Y., Bauer, A. & Beyerer, J. 2011, 'A conceptual framework for automatic situation assessment', *IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)*, pp. 234–9.

Flaspoler, E., Hauke, A., Pappachan, P., Reinert, D., Bleyer, T., Henke, N. & Beeck, R. 2009, 'The human machine interface as an emerging risk', European Agency for Safety and Health at Work.

Gallupe, R.B. 2007, 'The tyranny of methodologies in information systems research', *SIGMIS Database*, vol. 38, no. 3, pp. 20–8.

Garland, D.J., Wise, J.A. & Hopkin, V.D. 1999, *Handbook of aviation human factors*, Lawrence Erlbaum, Mahwah, NJ.

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*, vol. 50, no. 6, pp. 632-45.

Ha, J.S. & Seong, P.H. 2009, 'A human-machine interface evaluation method: A difficulty evaluation method in information searching (DEMIS)', *Reliability Engineering & System Safety*, vol. 94, no. 10, pp. 1557-67.

Hessami, A. 2010, 'A systems framework for strategic approach to risk in e-business', *International Journal of Information Science and Management*, no. Special, pp. 89-121.

Hsieh, M.-H., Hwang, S.-L., Liu, K.-H., Liang, S.-F.M. & Chuang, C.-F. 2012, 'A decision support system for identifying abnormal operating procedures in a nuclear power plant', *Nuclear Engineering and Design*, vol. 249, no. 0, pp. 413-8.

Hu, Y., Zhang, X., Ngai, E.W.T., Cai, R. & Liu, M. 2013, 'Software project risk analysis using Bayesian networks with causality constraints', *Decision Support Systems*, vol. 56, pp. 439–49.

Isaac, A., Shorrock, S.T. & Kirwan, B. 2002, 'Human error in European air traffic management: the HERA project', *Reliability Engineering & System Safety*, vol. 75, no. 2, pp. 257-72.

Jakobson, G., Buford, J., Lewis, L., Popovich, V.V., Schrenk, M. & Korolenko, K.V. 2007, 'Situation Management: Basic Concepts and Approaches Information Fusion and Geographic Information Systems'Springer Berlin Heidelberg, pp. 18-33.

Jenkins, D.P., Stanton, N.A. & Walker, G.H. 2012, *Distributed situation awareness: Theory, measurement and application to teamwork*, Ashgate Publishing, Ltd.

Jones-Lee, M. & Aven, T. 2011, 'ALARP: What does it really mean?', *Reliability Engineering & System Safety*, vol. 96, no. 8, pp. 877-82.

Jones, B., Jenkinson, I., Yang, Z. & Wang, J. 2010, 'The use of Bayesian network modelling for maintenance planning in a manufacturing industry', *Reliability Engineering & System Safety*, vol. 95, no. 3, pp. 267-77.

Jones, D.G. & Endsley, M.R. 2004, 'Use of real-time probes for measuring situation awareness', *International Journal of Aviation Psychology*, vol. 14, no. 4, pp. 343-67.

Jones, R., Connors, E., Mossey, M., Hyatt, J., Hansen, N. & Endsley, M. 2011, 'Using fuzzy cognitive mapping techniques to model situation awareness for army infantry platoon leaders', *Computational & Mathematical Organization Theory*, vol. 17, no. 3, pp. 272-95.

Jones, R.E.T., Connors, E.S. & Endsley, M.R. 2011, 'A framework for representing agent and human situation awareness', *IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support*, pp. 226-33.

Jou, Y.-T., Yenn, T.-C., Lin, C.J., Tsai, W.-S. & Hsieh, T.-L. 2011, 'The research on extracting the information of human errors in the main control room of nuclear power plants by using Performance Evaluation Matrix', *Safety Science*, vol. 49, no. 2, pp. 236-42.

Jovanovic, A.S. & Balos, D. 2012, 'iNTeg-Risk project: concept and first results', *Journal of Risk Research*, pp. 1-17.

Juricek, B.C., Seborg, D.E. & Larimore, W.E. 2001, 'Predictive monitoring for abnormal situation management', *Journal of Process Control*, vol. 11, no. 2, pp. 111-28.

Kaber, D.B. & Endsley, M.R. 1998, 'Team situation awareness for process control safety and performance', *Process Safety Progress*, vol. 17, no. 1, pp. 43-8.

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*, vol. 5, no. 2, pp. 113-53.

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*, vol. 91, no. 1-2, pp. 46-53.

Khakzad, N., Khan, F. & Amyotte, P. 2013, 'Quantitative risk analysis of offshore drilling operations: A Bayesian approach', *Safety Science*, vol. 57, no. 0, pp. 108-17.

Kim, M.C. & Seong, P.H. 2006a, 'An analytic model for situation assessment of nuclear power plant operators based on Bayesian inference', *Reliability Engineering & System Safety*, vol. 91, no. 3, pp. 270-82.

Kim, M.C. & Seong, P.H. 2006b, 'A computational method for probabilistic safety assessment of I&C systems and human operators in nuclear power plants', *Reliability Engineering & System Safety*, vol. 91, no. 5, pp. 580-93.

Kim, Y.J. & Hoffmann, C.M. 2003, 'Enhanced battlefield visualization for situation awareness', *Computers & Graphics*, vol. 27, no. 6, pp. 873-85.

Kirlik, A. & Strauss, R. 2006, 'Situation awareness as judgment I: Statistical modeling and quantitative measurement', *International Journal of Industrial Ergonomics*, vol. 36, no. 5, pp. 463-74.

Klashner, R. & Sabet, S. 2007, 'A DSS Design Model for complex problems: Lessons from mission critical infrastructure', *Decision Support Systems*, vol. 43, no. 3, pp. 990-1013.

Kokar, M.M., Matheus, C.J. & Baclawski, K. 2009, 'Ontology-based situation awareness', *Information Fusion*, vol. 10, no. 1, pp. 83-98.

Korb, K.B. & Nicholson, A.E. 2003, *Bayesian Artificial Intelligence*, Taylor & Francis.

Kwakernaak, H. 1978, 'Fuzzy random variables I: definitions and theorems', *Information Sciences*, vol. 15, no. 1, pp. 1-29.

Decision Support Laboratory 1998, 'SMILE (Structural Modeling, Inference, and Learning Engine)', library of C++ University of Pittsburgh, <http://genie.sis.pitt.edu/>.

Laskey, K.B. 1995, 'Sensitivity analysis for probability assessments in Bayesian networks', *IEEE Transactions on Systems, Man and Cybernetics*, vol. 25, no. 6, pp. 901-9.

Lee, S. & Seong, P. 2014, 'Design of an Integrated Operator Support System for Advanced NPP MCRs: Issues and Perspectives', in H. Yoshikawa & Z. Zhang (eds), *Progress of Nuclear Safety for Symbiosis and Sustainability*, Springer Heidelberg, Tokyo, pp. 11-26.

Li, P.c., Chen, G.h., Dai, L.c. & Zhang, L. 2012, 'A fuzzy Bayesian network approach to improve the quantification of organizational influences in HRA frameworks', *Safety Science*, vol. 50, no. 7, pp. 1569-83.

Lu, J., Liu, B., Zhang, G., Hao, Z. & Xiao, Y. 2008, 'A situation assessment approach using support vector machines as a learning tool', *International Journal of Nuclear Knowledge Management*, vol. 3, no. 1, pp. 82-97.

Lu, J., Yang, X. & Zhang, G. 2008, 'Support vector machine-based multi-source multi-attribute information integration for situation assessment', *Expert Systems with Applications*, vol. 34, no. 2, pp. 1333-40.

Ma, J. & Zhang, G. 2008, 'Team Situation Awareness measurement using group aggregation and implication operators', paper presented to the *The 3rd International Conference on Intelligent System and Knowledge Engineering (ISKE)*, Xiamen, China, November 17-19.

Mamdani, E.H. 1977, 'Application of fuzzy logic to approximate reasoning using linguistic synthesis', *IEEE Transactions on Computers*, vol. C-26, no. 12, pp. 1182-91.

Markowski, A.S., Mannan, M.S., Kotynia, A. & Pawlak, H. 2011, 'Application of fuzzy logic to explosion risk assessment', *Journal of Loss Prevention in the Process Industries*, vol. 24, no. 6, pp. 780-90.

Matthews, M.D., Martinez, S.G., Eid, J., Johnsen, B.H. & Boe, O.C. 2005, 'A Comparison of observer and incumbent ratings of situation awareness', *Human Factors and Ergonomics Society Annual Meeting*, vol. 49, SAGE Publications, pp. 548-51.

McGuinness, B. & Foy, L. 2000, 'A subjective measure of SA: the Crew Awareness Rating Scale (CARS)', *Proc. of Human Performance, Situation Awareness and Automation: User-Centered Design for the New Millenium*.

Melchers, R.E. 2001, 'On the ALARP approach to risk management', *Reliability Engineering & System Safety*, vol. 71, no. 2, pp. 201-8.

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

Nachreiner, F., Nickel, P. & Meyer, I. 2006, 'Human factors in process control systems: The design of humanâ€“machine interfaces', *Safety Science*, vol. 44, no. 1, pp. 5-26.

Naderpour, M. & Lu, J. 2012a, 'A fuzzy dual expert system for managing situation awareness in a safety supervisory system', paper presented to the *21st IEEE International Conference on Fuzzy Systems*, Brisbane-Australia, June10-15.

Naderpour, M. & Lu, J. 2012b, 'Supporting situation awareness using neural network and expert system', paper presented to the *10th International FLINS Conference on Uncertainty Modeling in Knowledge Engineering and Decision Making*, Istanbul-Turkey, August 26-29.

Naderpour, M. & Lu, J. 2014, 'A Situation Analysis Decision Support System Based on Dynamic Object Oriented Bayesian Networks', *Journal of Software*, vol. 9, no. 8, pp. 2194-9.

Naderpour, M., Lu, J. & Kerre, E. 2011, 'A Conceptual Model for Risk-Based Situation Awareness', paper presented to the *International Conference on Intelligent Systems and Knowledge Engineering (ISKE)*, Shanghai, China.

Naderpour, M., Lu, J. & Zhang, G. 2014a, 'The explosion at Institute: Modeling and analyzing the situation awareness factor', *Accident Analysis & Prevention*, vol. 73, no. 0, pp. 209-24.

Naderpour, M., Lu, J. & Zhang, G. 2014b, 'An intelligent situation awareness support system for safety-critical environments', *Decision Support Systems*, vol. 59, pp. 325-40.

Nazir, S., Colombo, S. & Manca, D. 2012, 'The role of situation awareness for the operators of process industry', *Chemical Engineering Transactions*, vol. 26, pp. 303-8.

Nazir, S., Kluge, A. & Manca, D. 2014, 'Automation in Process Industry: Cure or Curse? How can Training Improve Operator's Performance', in P.S.V. Jiří Jaromír Klemeš & L. Peng Yen (eds), *Computer Aided Chemical Engineering*, vol. Volume 33, Elsevier, pp. 889-94.

Nazir, S., Sorensenb, L.J., Øvergårdb, K.I. & Manca, D. 2014, 'How Distributed Situation Awareness Influences Process Safety ', *Chemical Engineering Transactions*, vol. 36, pp. 409-14.

Niu, L., Lu, J. & Zhang, G. 2009, *Cognition-driven decision support for business intelligence: Models, techniques, systems and applications*, vol. 238, Springer-Verlag, Berlin Heidelberg.

Niu, L., Lu, J., Zhang, G. & Wu, D. 2013, 'FACETS: A cognitive business intelligence system', *Information Systems*, vol. 38, pp. 835-62.

O'Hara, J.M. & Persensky, J. 2011, 'Human Performance and Plant Safety Performance', *Simulator-based Human Factors Studies Across 25 Years*, Springer, pp. 91-106.

OREDA 2002, *Offshore Reliability Data Handbook*, SINTEF Industrial Management.

Paige Bacon, L. & Strybel, T.Z. 2013, 'Assessment of the validity and intrusiveness of online-probe questions for situation awareness in a simulated air-traffic-management task with student air-traffic controllers', *Safety Science*, vol. 56, no. 0, pp. 89-95.

Papadopoulos, Y. & McDermid, J. 2001, 'Automated safety monitoring: A review and classification of methods', *International journal of COMADEM*, vol. 4, no. 4, pp. 14-32.

Pedrycz, W. 1994, 'Why triangular membership functions?', *Fuzzy sets and Systems*, vol. 64, no. 1, pp. 21-30.

Pierce, R.S., Strybel, T.Z. & Vu, K.-P.L. 2008, 'Comparing situation awareness measurement techniques in a low fidelity air traffic control simulation', *Proceedings of the 26th International Congress of the Aeronautical Sciences (ICAS), Anchorage, AS*.

Pollino, C.A., Woodberry, O., Nicholson, A., Korb, K. & Hart, B.T. 2007, 'Parameterisation and evaluation of a Bayesian network for use in an ecological risk assessment', *Environmental Modelling & Software*, vol. 22, no. 8, pp. 1140-52.

Power, D.J. & Sharda, R. 2007, 'Model-driven decision support systems: Concepts and research directions', *Decision Support Systems*, vol. 43, no. 3, pp. 1044-61.

Pridmore, J.L. 2007, 'Designing for the improvement of operator situation awareness in automation systems', PhD thesis, Auburn University, Alabama, U.S.

Qian, Y., Xu, L., Li, X., Lin, L. & Kraslawski, A. 2008, 'LUBRES: An expert system development and implementation for real-time fault diagnosis of a lubricating oil refining process', *Expert Systems with Applications*, vol. 35, no. 3, pp. 1252-66.

Roth, E.M., Multer, J. & Raslear, T. 2006, 'Shared Situation Awareness as a Contributor to High Reliability Performance in Railroad Operations', *Organization Studies*, vol. 27, no. 7, pp. 967-87.

Rouse, W.B. & Morris, N.M. 1986, 'On looking into the black box: Prospects and limits in the search for mental models', *Psychological bulletin*, vol. 100, no. 3, pp. 349–63.

Roy, J. 2001, 'From data fusion to situation analysis', paper presented to the *The 4th International Conference on Information Fusion*, Montreal, Canada, 7-10 August.

Salerno, J., Hinman, M. & Boulware, D. 2004, 'Building a framework for situation awareness', paper presented to the *Seventh International Conference on Information Fusion*, Stockholm Sweden, 28 June - 1 July.

Salmon, P., Stanton, N., Walker, G. & Jenkins, D. 2009, 'Distributed situation awareness: advances in theory, measurement and application to teamwork'.

Salmon, P.M. & Stanton, N.A. 2013, 'Situation awareness and safety: Contribution or confusion? Situation awareness and safety editorial', *Safety Science*, vol. 56, pp. 1-5.

Salmon, P.M., Stanton, N.A., Walker, G.H., Baber, C., Jenkins, D.P., McMaster, R. & Young, M.S. 2008, 'What really is going on? Review of situation awareness models for individuals and teams', *Theoretical Issues in Ergonomics Science*, vol. 9, no. 4, pp. 297-323.

Salmon, P.M., Stanton, N.A., Walker, G.H., Jenkins, D., Ladva, D., Rafferty, L. & Young, M. 2009, 'Measuring situation awareness in complex systems: Comparison of measures study', *International Journal of Industrial Ergonomics*, vol. 39, no. 3, pp. 490-500.

Salmon, P.M., Stanton, N.A., Walker, G.H., Jenkins, D.P. & Rafferty, L. 2009, 'Is it really better to share? Distributed situation awareness and its implications for collaborative system design', *Theoretical Issues in Ergonomics Science*, vol. 11, no. 1-2, pp. 58-83.

Schmidt, K.W. & Boutalis, Y.S. 2012, 'Fuzzy discrete event systems for multiobjective control: Framework and application to mobile robot navigation', *IEEE Transactions on Fuzzy Systems*, vol. 20, no. 5, pp. 910-22.

Seong, P.H. 2009, *Reliability and risk issues in large scale safety-critical digital control systems*, Springer.

Shapiro, A.F. 2009, 'Fuzzy random variables', *Insurance: Mathematics and Economics*, vol. 44, no. 2, pp. 307-14.

Shrivastava, P. 1992, *Bhopal: anatomy of a crisis*, P. Chapman Pub., Ballinger, Cambridge, MA.

Smart, P.R., Russell, A., Shadbolt, N.R. & Carr, L.A. 2007, 'Aktivesa: A technical demonstrator system for enhanced situation awareness', *The Computer Journal*, vol. 50, no. 6, pp. 703-16.

Smith, K. & Hancock, P. 1995, 'Situation awareness is adaptive, externally directed consciousness', *Human Factors: The Journal of the Human Factors and Ergonomics Society*, vol. 37, no. 1, pp. 137-48.

Sneddon, A., Mearns, K. & Flin, R. 2006, 'Situation awareness and safety in offshore drill crews', *Cognition, Technology & Work*, vol. 8, no. 4, pp. 255-67.

Sneddon, A., Mearns, K. & Flin, R. 2013, 'Stress, fatigue, situation awareness and safety in offshore drilling crews', *Safety Science*, vol. 56, no. 0, pp. 80-8.

Stanton, N. 2005, *Human Factors Methods: A Practical Guide for Engineering and Design*, Ashgate, Aldershot, UK.

Stanton, N.A., Chambers, P.R.G. & Piggott, J. 2001, 'Situational awareness and safety', *Safety Science*, vol. 39, no. 3, pp. 189-204.

Stanton, N.A., Salmon, P.M., Walker, G.H. & Jenkins, D.P. 2010, 'Is situation awareness all in the mind?', *Theoretical Issues in Ergonomics Science*, vol. 11, no. 1-2, pp. 29-40.

Stanton, N.A., Stewart, R., Harris, D., Houghton, R.J., Baber, C., McMaster, R., Salmon, P., Hoyle, G., Walker, G. & Young, M.S. 2006, 'Distributed situation

awareness in dynamic systems: theoretical development and application of an ergonomics methodology', *Ergonomics*, vol. 49, no. 12-13, pp. 1288-311.

Su, X., Bai, P., Du, F. & Feng, Y. 2011, 'Application of Bayesian networks in situation assessment', in R. Chen (ed.), *Intelligent Computing and Information Science*, vol. 134, Springer-Verlag Berlin Heidelberg, pp. 643-8.

Sugeno, M. 1985, *Industrial applications of fuzzy control*, Elsevier Science Inc.

Taylor, R.M. 1990, 'Situational Awareness Rating Technique (SART): the development of a tool for aircrew systems design', *Situational Awareness in Aerospace Operations*, vol. 3, pp. 1-17.

University of California, Los Angeles (UCLA) 2004, 'SamIam: Sensitivity Analysis, Modeling, Inference and More', <http://reasoning.cs.ucla.edu/samiam/>.

Van den Broek, A.C., Neef, R.M., Hanckmann, P., Van Gosliga, S.P. & Van Halsema, D. 2011, 'Improving maritime situational awareness by fusing sensor information and intelligence', *Proceedings of the 14th International Conference on Information Fusion (FUSION)*, pp. 1-8.

Vincenzi, D.A., Mouloua, M. & Hancock, P.A. 2004, *Human performance, situation awareness and automation: current research and trends : HPSAA II*, L. Erlbaum Associates.

Waag, W.L. & Houck, M.R. 1994, 'Tools for assessing situational awareness in an operational fighter environment', *Aviation, Space, and Environmental Medicine*, vol. 65, no. 5 Suppl, pp. A13-9.

Walker, P.D., Cammy, N.E., Ellis, B.J. & Seibert, K.D. 2011, 'Operations Skills for the 21st Century', *National Petrochemical & Refiners Association (NPRA) Annual Meeting, Paper AM-11-68*.

Wang, L.-X. 1999, *A course in fuzzy systems*, Prentice-Hall press, USA.

Zadeh, L.A. 1965, 'Fuzzy sets', *Information and Control*, vol. 8, no. 3, pp. 338-53.

Zadeh, L.A. 1975, 'The concept of a linguistic variable and its application to approximate reasoning—I', *Information Sciences*, vol. 8, no. 3, pp. 199-249.

Zakay, D. & Wooler, S. 1984, 'Time pressure, training and decision effectiveness', *Ergonomics*, vol. 27, no. 3, pp. 273-84.

APPENDIX: ABBREVIATIONS

ALARP	As Low As Reasonably Practicable
ASM	Abnormal Situation Modeling
BN	Bayesian Network
CPT	Conditional Probability Tables
DAG	Directed Acyclic Graph
DAG	Directed Acyclic Graph
DBN	Dynamic Bayesian Network
DCS	Distributed Control System
DSA	Distributed Situation Awareness
DSS	Decision Support System
EO	Ethylene Oxide
FDA	Food And Drug Administration
FLS	Fuzzy Logic System
FMEA	Failure Mode and Effect Analysis
GDTA	Goal-Directed Task Analysis
GUI	Graphical User Interface
HSWA	Health and Safety at Work Act
MIC	Methyl Isocyanate
MSAO	Methylthioacetaldoxime
NASA-TLX	NASA Task Load Index
NPP	Nuclear Power Plant
OOBN	Object Oriented Bayesian Network
SA	Situation Awareness
SABARS	Situation Awareness Behavioural Rating Scale
SAGAT	Situation Awareness Global Assessment Technique

SAL	Situation of Abnormal Liquid Level
SAR	Situation of Abnormal Recirculation
SARS	Situational Awareness Rating Scale
SART	Situation Awareness Rating Technique
SASS	Situation Awareness Support System
SA-SWORD	Situation Awareness-Subjective Workload Dominance Technique
SAT	Situation of Abnormal Temperature
SAV	Situation of Accumulated Vapour in the Production Building
SBV	Situation of Building Ventilation System Malfunction
SCADA	Supervisory Control And Data Acquisition
SFAIRP	So Far As Is Reasonably Practicable
SHC	Situation of High Concentration of Methomyl
SHP	Situation of High Pressure
SHT	Situation of High Temperature Inside the Tank
SIV	Situation of Inadequate Building Ventilation
SLS	Situation of Large Spill from Storage System
SME	Subject Matter Expert
SPAM	Situation Present Assessment Method
SRR	Situation of Runaway Reaction
SVC	Situation of Vent Condenser Failure