A Human-System Interface Risk Assessment Method Based on Mental Models

Abstract:

In many safety-critical systems, it is necessary to maintain operators' situation awareness at a high level to ensure the safety of operations. Today, in many such systems, operators have to rely on the principles and design of human-system interfaces (HSIs) to observe and comprehend the overwhelming amount of process data. Thus, poor HSIs may cause serious consequences, such as occupational accidents and diseases including stress, and they have therefore been considered an emerging risk. Despite the importance of this, very few methods have as yet been developed to assess the risk of HSIs. This paper presents a new risk assessment method that relies upon operators' mental models, human reliability analysis (HRA) event tree, and the situation awareness global assessment technique (SAGAT) to produce a risk profile for the intended HSI. In the proposed method, the operator's understanding (i.e. mental models) about possible abnormal situations in the intended plant is modeled on the basis of the capabilities of Bayesian networks. The situation models are combined with the HRA event tree, which paves the way for the incorporation of operator responses in the assessment method. Probe questions in line with the SAGAT through simulated scenarios in a virtual environment are then administrated to gather operator responses. Finally, the proposed method determines a risk level for the HSI by assigning the operator responses to the developed situational networks. The performance of the proposed method is investigated through a case study at a chemical plant.

Keywords: Risk assessment, Situation awareness, Situation awareness measurement, Human-system interfaces, Mental models.

1. Introduction

Following several high impact disasters such as those at Three Mile Island, Bhopal and Chernobyl, many high-hazard industries have focused on different contributing factors to reduce their accident rates as much as possible. In most industrial accidents, there is a chain of organizational conditions and human errors which show that 70-80% of such accidents are attributable to human-factor causes (Isaac et al., 2002; Sneddon et al., 2006). Among those causes, the ability of operators to maintain an adequate understanding of their worksite situations is a critical factor in preventing accidents. This cognitive ability is referred to as situation awareness (SAW); it indicates a high level of awareness of task and environmental conditions, as well as the ability to predict how these conditions may change in the near future to aid understanding of how situations will develop (Nazir et al., 2012; Nazir et al., 2014b). To date, several SAW models such as Taylor (1990), Endsley (1995b), Adams et al. (1995), and Bendy and Meister (1999), have been developed; however, Endsley's model has undoubtedly received the most attention. This information processing-based model describes SAW 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". It introduces SAW as a product that has three levels: Level 1, the perception of relevant elements in the task environment; Level 2, the comprehension of the elements

with regard to the goals; and Level 3, the projection of the state of those elements in the near future (Endsley, 1995b).

In many safety-critical systems today, 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. Human-system interfaces (HSIs) should therefore support operators by helping them to understand situations and act more effectively and less ambiguously. Poor HSI can have serious consequences, such as occupational accidents and diseases including stress, therefore HSI has recently been considered an emerging risk which may jeopardize safety (Flaspoler et al., 2009; Jovanovic and Balos, 2012). To design an adequate HSI, the specific properties and qualities of human factors as well as the working environment must be taken into account, but very few methods and tools have as yet been developed to assess this kind of risk in the design of HSIs, despite its importance. Fuchs-Frohnhofen et al. (1996) proposed a methodology to incorporate users' mental models in a HSI for a CNC system. Carvalho et al. (2008) suggested several principles based on human factors to improve an interface screen, alarm system, and procedure guidelines in a nuclear power plant simulator. Ha and Seong (2009) proposed a difficulty evaluation method in information search, based on two measures: Fixation-to-importance ratio and selective attention effectiveness. Lee and Seong (2013) recently developed a computational situation assessment model to design HSIs in nuclear power plants based on SAW.

This paper argues that a range of methods and techniques are required for evaluating the safety of HSIs from the human factor perspective. It may be argued that human error is best examined from a cognitive perspective, as traditional reliability engineering techniques do not appear to fit well with human factor concerns. Therefore, it may be more appropriate to quantify safety from a human factor perspective in terms of the level of SAW acquired through the interface. In this sense, the paper considers operators' behavior when they are confronted with abnormal situations in a safety-critical environment. To achieve this, the operators' mental models with regard to possible abnormal situations in the intended plant are first modeled by exploiting the capabilities of Bayesian networks (BNs). Secondly, the aspects of the situation that are important for operators' SAW are determined using a cognitive task analysis called goal-directed task analysis (GDTA) methodology. Thirdly, online probe questions based on identified SAW requirements and in line with the situation awareness global assessment technique (SAGAT) are administrated in a simulation environment where operators' responses are collected and assigned to developed BN-based situational networks as evidence to form the assessment result.

The paper is organized as follows. Section 2 presents the operators' cognitive activities. Section 3 describes the operators' mental models. Measuring SAW is explained in Section 4. The HSI risk assessment method is presented in Section 5. The performance of the proposed method is investigated in Section 6 in which a residue treater unit at a chemical plant is used for demonstration. The conclusion and future work are outlined in Section 7.

2. Operators' Cognitive Activities

Large-scale technological systems usually 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, 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 the ability to intervene or tackle abnormal situations as such systems are usually designed for routine operating conditions (Nazir et al., 2013; Nazir et al., 2014a). Therefore, any attempt to develop operator support systems should consider both normal and abnormal situations.

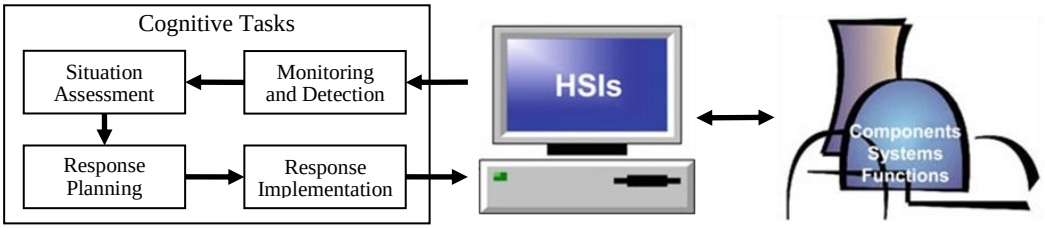
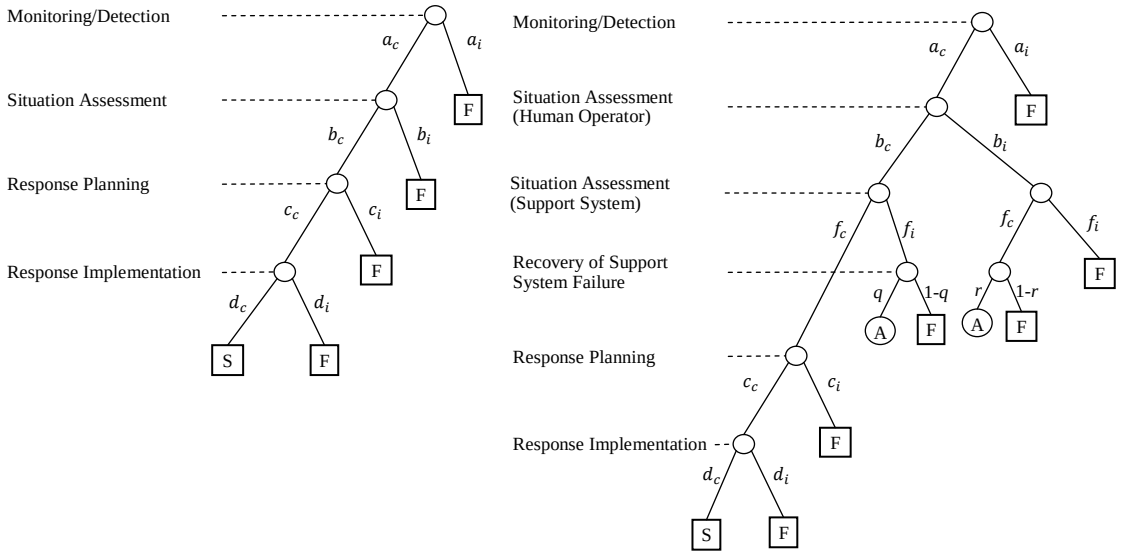


Figure 1: General cognitive tasks.

Generally, the cognitive tasks that operators perform to carry out their roles and responsibilities include monitoring and detection, situation assessment, response planning, and response implementation (O'Hara and Persensky, 2011), as illustrated in Figure 1. Any breakdown in these generic tasks can lead to human error. Therefore, a balanced automated system that avoids an excessive workload for its operators and keeps them in the loop of decision-making, taking action, and updating related information will benefit the intended industry. The activities involved in extracting information from the environment are referred to as 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' achieving perception or SAW level 1. Situation assessment is the evaluation of current conditions to determine whether they are acceptable, or to discover the underlying causes of abnormalities. Situation assessment which underlies the achievement of SAW is therefore critical to taking appropriate human action. The HSI must thus provide additional support for assessing the situation besides providing alarms and displays that are used to obtain information to support situation assessment. This development corresponds to SAW levels 2 and 3, which enable 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 and Persensky, 2011).

The human reliability analysis (HRA) event tree is a technique that shows that the final operation result is correct if the components of all four cognitive tasks have been carried out correctly. Figure 2, a_c and a_i indicates the probability of an operator reading an indicator correctly or incorrectly. As can be seen, the basic event tree does not include a decision support system. If a decision support system is used in any step, new branches are added to the basic event tree. For instance, f_c and f_i refer to the probability that the support system will generate correct or incorrect results. q represents the probability that the operator will recognize incorrect diagnosis results produced by the support system, while r indicates the recovery probability that an operator who has assessed the situation incorrectly will make a decision change based on correct results delivered by the support system (Lee et al., 2008). As in this paper, a simulated environment is used to show the performance of the HSI risk assessment method, the first three layers–monitoring, situation assessment, and response planning– are just considered.



(I) Basic HRA event tree (II) HRA event tree with a support system

Figure 2: Basic and extended HRA event trees.

3. Operators' Mental Models

The concept of mental models has a very long tradition in applied cognition. Mental models are mechanisms that enable humans to generate descriptions of system purpose and explanations of system functioning (Endsley, 2000b). Mental models embody stored long-term knowledge about systems that can be called upon to interact 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 to achieve SAW 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 SAW can provide the operator with quick retrieval of actions from memory (Pridmore, 2007).

Mental models have often been used in studies trying to model 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 SAW model. However, they believe that mental models are not a state but sets of processes. Endsley's representations provide a context for some form of judgment and contribute to SAW in the form of references to prior experience. Her approach presents mental models as default information that helps to form higher levels of SAW 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 SAW. Mental models (formed by training and experience) are used to facilitate the achievement of SAW 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).

A situation model can be developed not only by observing the world, but also by being influenced by the operator's underlying mental models. 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). For example, an operator may perceive several dynamics in the flow lines (considered to be important elements according to the mental model) as being 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 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 SAW, the operator is then able to select suitable actions that will prevent their formation of mental models.

4. Measuring Situation Awareness

Situation awareness measures determine the degree to which design concepts and new technologies improve or degrade an operator's SAW. They are therefore a critical part of any system and procedural design process, and evaluation efforts to assure that SAW is improved and not degraded by new systems, interfaces or procedures is essential (Endsley, 1995a). Unfortunately, difficulties arise when trying to measure SAW because there is no universally accepted model. Measures of SAW, in general, try to infer it from other constructs that are easier to assess (i.e. indirect measures), or obtain it directly. Endsley's research shows that direct SAW measurements, including subjective and objective measures, are the best way to evaluate a system design (Endsley et al., 2003); however, even the most successful measures are not able to assess operators' SAW during real operations (Jones and Endsley, 2004). The Situation

Awareness Global Assessment Technique (SAGAT), which is a popular freeze probe technique, was developed to assess pilots' SAW based on Endsley's three level model (Endsley and Garland, 2000). It has been widely used in a variety of domains, such as air traffic control (Endsley, 2000a), commercial and military aviation (Endsley et al., 1998), nuclear power plant operations (Jenkins et al., 2012), and simulated air traffic management (Paige Bacon and Strybel, 2013). Operators training with SAGAT execute the experimental scenarios, during which several freezes occur at randomly selected intervals. The freezes are not predictable by the operators. At the time of each freeze, the displays are blanked and the simulations are suspended. The operators' responses are scored 1 for correct answers and 0 for incorrect answers, and final SAGAT scores are calculated by summing all correct responses for each participant.

5. A HSI Risk Assessment Method

A situation is defined as a set of circumstances in which a number of objects may have relationships with one another and the environment, and 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 (Naderpour et al., 2014c). 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 and Seong, 2006).

In the context of automation systems, an operator's mental model will be greatly influenced by the system design being employed, and this is especially pertinent now that operators are increasingly physically removed from the process. The visible aspects of the system, the actions that seem applicable and the prior experience of the operator combine to 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 paper assumes that the operator's mental model can be modeled using BNs as a representation of static cause–effect relationships between objects in the situation, administering freeze probe questions in simulated scenarios in regard to SAGAT, calculating a HSI risk level for every operators by introducing their responses to probe questions as evidence into developed BN-based mental models, and forming an overall risk level by averaging individuals. The core idea of the proposed method is illustrated in Figure 3 and explained in the sections that follow.

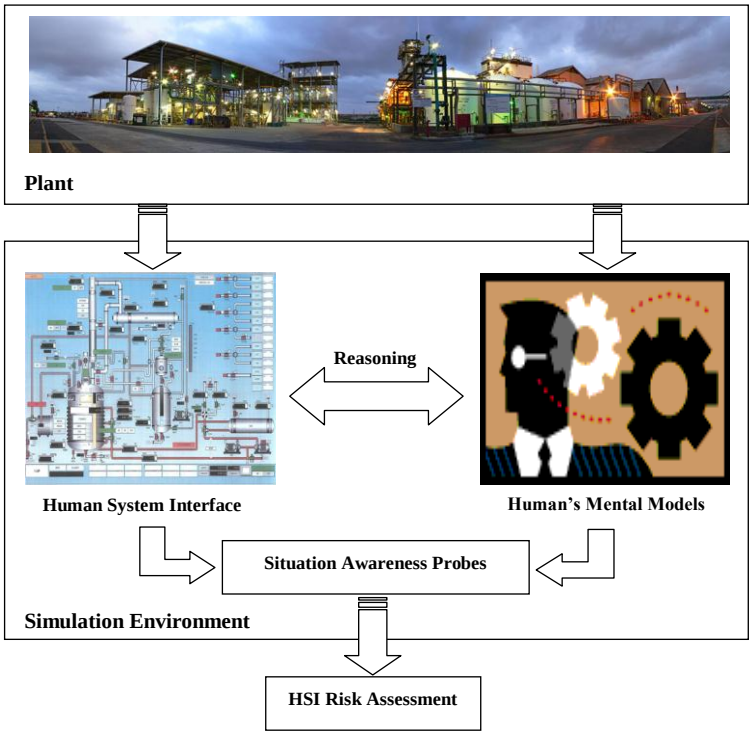


Figure 3: A human-system interface risk assessment method.

5.1. Identifying Situation Awareness Requirements

This paper considers the safety assessment of HSIs when operators are confronted with abnormal situations (i.e. not routine operation situations) in which process optimization is a concern. The GDTA methodology is a method to determine the aspects of a situation that are important for a particular user's SAW requirements, and the main goal is to eliminate or reduce the risks to a level that is as low as reasonably practicable (ALARP). According to the ALARP principle, 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). The other elements of GDTA are shown in Table 1. The main goal is supported by two sub-goals: risk determination and risk reduction. The major decisions that need to be made in association with each sub-goal are identified, and the SAW requirements for making these decisions and fulfilling each sub-goal are determined.

Table 1: Safety goals, decisions and SAW requirements.

Goal: Eliminate or reduce the risks to a level that is as low as reasonably practicable
Subgoal 1: Determine the risks
Decision 1-1: Hazardous situation identification
• *L1 Observable variable states*
• *L1: Alarm status*
• *L2: Objects and relationships which contribute to creating a hazardous situation*
• *L2: Situations and relationships which contribute to creating a hazardous situation*
Decision 1-2: Probability determination
• *L1: Objects which are relevant to the hazardous situation*
• *L1: Observable variables which are relevant to the hazardous situation*
• *L2: Prior probability of the hazardous situation*
• *L3: Posterior probability of the hazardous situation*
Decision 1-3: Severity determination
• *L2: Possible consequences of the hazardous situation*
• *L3: Degree of loss*
Decision 1-4: Risk level estimation
• *L2: Probability of the hazardous situation* (*Decision 1-2*)
• *L2: Severity of the hazardous situation* (*Decision 1-3*)
• *L3: Current level of risk*
Subgoal 2: Reduce the risks
Decision 2-1: Choosing practical options
• *L2: Available reduction and containment options*
Decision 2-2: Options impact prediction
• *L2: The severity of the hazardous situation*
• *L3: Projecting the new probability of the hazardous situation*
• *L3: New level of risk*

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

5.2. Modeling of Mental Models

Learning, education, training, and other experiences enable operators to form mental models on plant components in their long-term memories. Bayesian networks offer nodes, arcs, and CPTs that can be used to encode an operator's knowledge about a plant and is thus an appropriate method for modeling a causal process with uncertainty. As modeling complex systems may lead to complicated models, a particular class of BNs, the object oriented Bayesian networks (OOBNs) has been defined to avoid this phenomenon. The authors have developed an abnormal situation modeling (ASM) method that tries to represent operators' mental models in regard to abnormal situations (Naderpour et al., 2015a). 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 situation models should be determined, and how they should be connected to each other to create the situational networks. As a situation of interest can be inferred by observable variables in the environment, the ASM method explains how situations can be connected to observable variables.

In this paper, the ASM method is modified by adding nodes (i.e. Monitoring/Detection (MD), Situation Assessment (SA), and Response Planning (RP)) related to the HRA event tree to incorporate the operators' responses to the SAGAT probe questions. For example, consider a vessel that needs to be

maintained at a defined temperature for production and safety purposes. The vessel has an automatic cooling system (ACS) to remove excess heat generated by the exothermic decomposition of substances inside the vessel. The cooling system includes a temperature sensor (TS), automatic water valve (AWV), and recirculation pump (RPU) which provides steady state recirculation, and there is a flow transmitter (F) that measures the flow of liquid through the recirculation pipeline. The operator's mental model of a situation of abnormal recirculation (SAR), as demonstrated in Figure 4, can be described as follows: A SAR exists if the FT is out of order and the ACS is not working properly (i.e. AND gate). The ACS is also failed if any of TS, AWV, or TS is out of order (i.e. OR gate). In addition, as the SAR can be inferred from F, there is a relationship between the SAR node and the F node.

Several situations can generally exist in parallel, and the complete modeling of their dependencies results in one or more networks of situations. This may also include 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 or other situations.

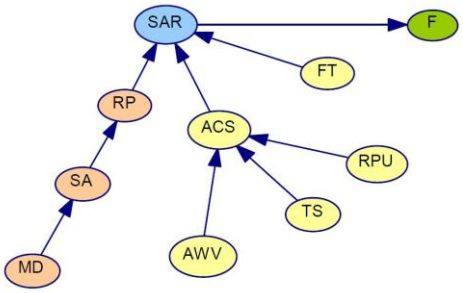


Figure 4: A combined situation model and HRA event tree.

5.3. Probabilistic Risk Assessment

The developed BN-based situational networks discussed in the previous section are able to provide the prior and posterior probabilities of situations and objects. A quantitative analysis can be conducted by the forward method (or predictive analysis) to compute the posterior probability distribution of any situation given the observation of a set of evidence. The proposed HSI risk assessment method uses operators' responses to the probe questions of SAGAT as evidence and assigns them to the situational networks. Thus, a risk level can be calculated as a multiplication of the posterior probability and severity of consequences. The severity of each consequence can be determined in a common currency in which human loss, asset loss, and environmental loss are converted to money to provide a coherent view of the totality of loss associated with an abnormal situation. Table 2 provides an example in AUD.

Risk profiles may provide designers with a clearer vision of how the risk profile may change due to variations in the parameters, information, or supplementary materials provided. Appropriate efforts can therefore be effectively applied to reduce or maintain the risk within defined acceptance criteria for the majority of operators.

Table 2: Estimated damage of consequences.

Consequence	Symbol	Damage (AUD)
Safe	C1	0
Near miss	C2	5,000
Incident	C3	50,000
Accident	C4	1,000,000
Major accident	C5	10,000,000

6. A Case Study

On 28 August 2008, a runaway chemical reaction at a residue treater unit caused an explosion, and two employees who were investigating why the residue treater pressure was increasing were killed (Naderpour et al., 2014a). Several factors, including deviation from the written start-up procedures and bypassing of critical safety devices, contributed to the accident. In addition to these precursors, a poor newly-installed process mimic screen which could not provide adequate SAW for the board operator was another important contributing factor (CSB, 2011). In this case, the new control system significantly changed the interactions between the board operators and the DCS[1] interface. The new visual displays and modified command entry method, which changed from a keyboard to a mouse, influenced the usability of the HSI and impaired human performance. The new workstation had five display screens available to monitor the processes and one display screen dedicated to process alarms. Routine activities such as starting a reaction or troubleshooting alarms required operators to move between multiple screens to complete a task. It can therefore be concluded that it was very difficult to interpret the data or to detect deviation from safety set points. In addition to identified level 1 SAW errors, several level 2 SAW errors that could occur were determined. Firstly, a good mental model was lacking, particularly in respect of the new automated system, as the facility's management failed to provide operators with comprehensive formal training and practice in the use of the new DCS. Secondly, it is worth noting that the wrong mental model or the mental model of a similar system, i.e. the methomyl unit adjacent to the residue treater, could have been used to interpret information, leading to an incorrect diagnosis or understanding of the situation. Thirdly, over-reliance on defaults in the mental models might be another problem (Naderpour et al., 2015b).

6.1. 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 starts with the production of methylthioacetaldoxime (MSAO) by reacting chloroacetaldoxime with sodium methyl mercaptide. The MSAO then reacts with MIC to produce methomyl. The crystallizers remove excess MIC from the methomyl-solvent solution by adding an anti-solvent that causes the methomyl to become crystallized. Lastly, a centrifuge separates the crystallized methomyl from the solvents. The methomyl cake is dried,

[1] Distributed Control System

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

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, called "flasher bottoms", includes unvaporized solvents and impurities containing up to 22 percent 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 percent by weight. This rate is essential for environmental and processing considerations (CSB, 2011).

The incoming flasher bottoms are diluted in a 4500-gallon pressure vessel (50 psig is the maximum allowable operating pressure) called the residue treater. The concentration of methomyl in the flasher bottom stream will be below 0.5 percent 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 vapour are removed from vapour generated in the methomyl decomposition reaction when it exits through the vent condenser to the process vent system (CSB, 2011).

6.2. Observable Variables

There are several transmitters in the environment that provide the online condition for the residue treater. The discrete states of observable variables are determined in terms of operation and safety set-points, as shown in Table 3.

Table 3: Discrete states of observable variables.

Observable variable	States	Definition
Liquid Level (L)	Low	$L < 30$
	Normal	$30 \leq L \leq 50$
	High	$50 < L$
Recirculation Flow (F)	Very low	$F < 20$
	Low	$20 \leq L \leq 60$
	Normal	$60 < L$
Temperature (T)	Low	$T < 130$
	Normal	$130 \leq T \leq 135$
	High	$135 < T$
Pressure (P)	Normal	$P \leq 20$
	High	$20 < P \leq 25$
	Very high	$25 < P$

6.3. Situation Models

Seven abnormal situations in the environment were 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), and situation of runaway reaction (SRR). The objects are presented in Table 4, but the CTPs are omitted as the details can be found in (Naderpour et al., 2015a). The situational network is then modified by the HRA event tree, as shown in Figure 5. The focal objects representing situations are colored blue, the basic objects are yellow, the observable variables are green and the HRA event tree nodes are orange. The consequence node is red. As can be seen, in the abnormal situations that are not directly inferable from observable variables, the MD node of the HRA event tree is removed.

Table 4: Abnormal situations and their objects.

Situation/Objects	Symbol	Failure Probability
SVC		
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
SHL		
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
SAR		
Flow transmitter	FT	7.13E-06
Recirculation pump	RP	4.00E-02
Temperature sensor in recirculation	TS	4.00E-02
Automatic water valve	AWV	8.68E-06
Automatic cooler system	ACS	OR gate
SHP		
Pressure transmitter	PT	1.64E-01
Automatic relief valve (mechanical failure)	ARV	3.40E-01
Automatic pressure control	APC	OR gate
Failure of 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
SHT		
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
SHC		
Situation of high liquid level	SHL	Independent situation
Situation of high temperature	SHT	Dependent situation
SRR		
Situation of high pressure	SHP	Dependent situation
Situation of high concentration of methomyl	SHC	Dependent situation
Air monitor system	AM	0.18E-06
Fire alarm	FA	1.30E-03
Fire cannon	FC	4.00E-01
Ignition barrier	IB	1.00E-01
Consequence	Consequence	NA

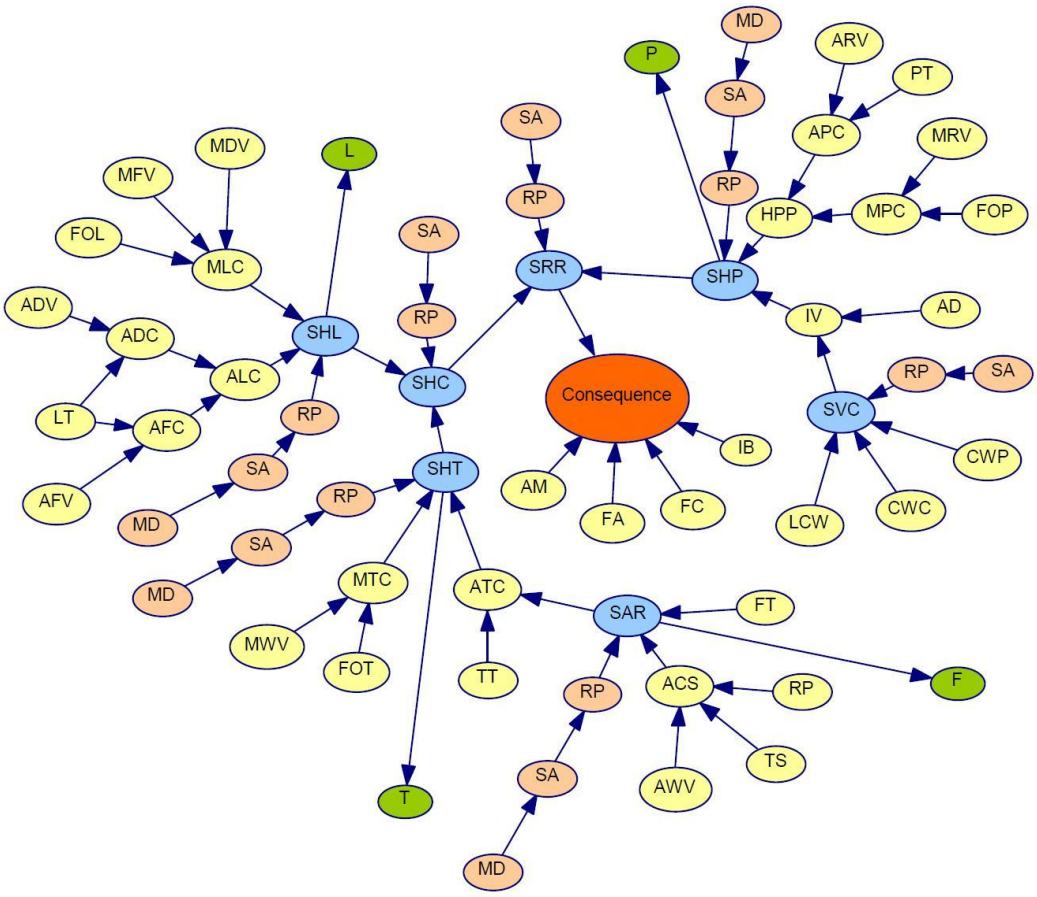


Figure 5: The combined situational network of the residue treater with HRA event trees.

6.4. The Intended Human-System Interface

The simulation environment consists of a HSI that displays the necessary information for operators to monitor the residue treater operation and manipulate the components, as shown in Figure 6. Flow directions are indicated by vertical and horizontal lines between components. Instantaneous values, i.e. 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 appearing as a flashing value have fallen outside of their allowable range. The interface also provides a pop-up window, accessible by mouse-clicking any component, giving the available options to deactivate the alarm, turn the system pumps on and off, and maintenance suggestions.

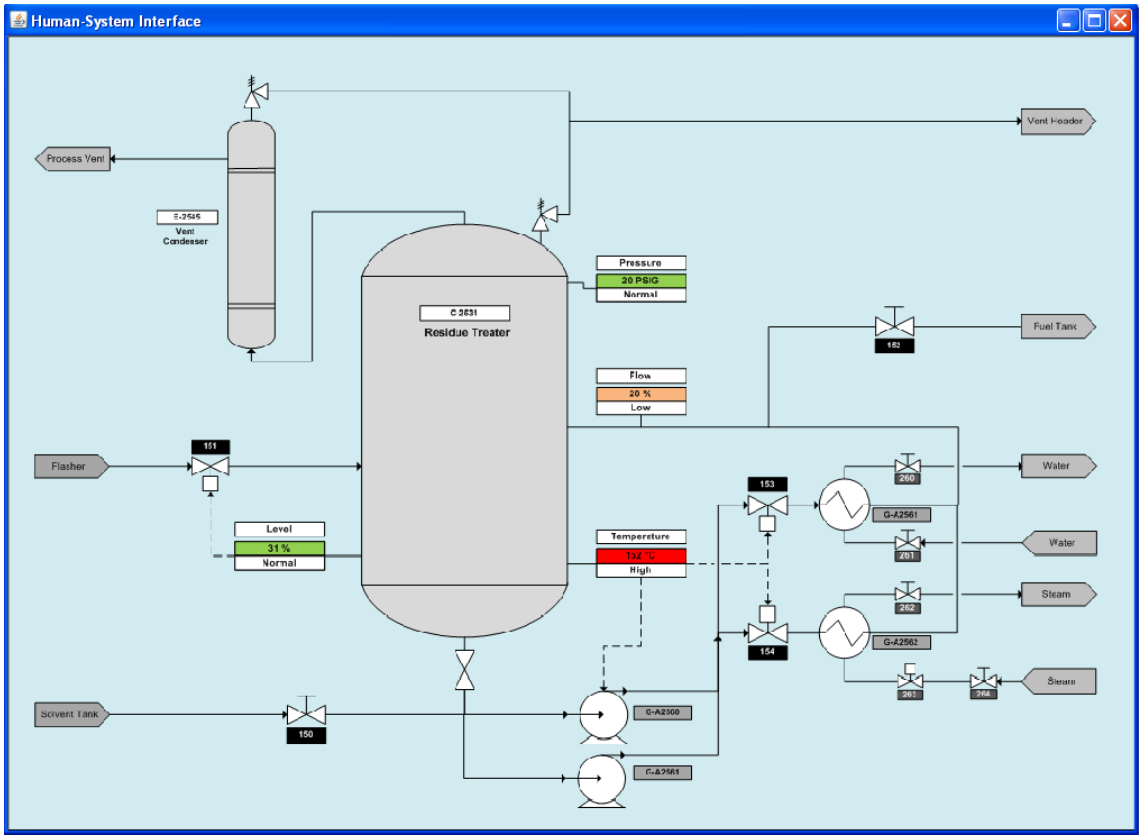


Figure 6: The human-system interface of a simulated residue treater plant.

6.5. Risk Assessment

Ten experienced operators (*M*=5.40 yrs, *SD*=1.42) currently involved in the operation of an oil refinery took part in the risk assessment. All participants became familiar with the characteristics of abnormal situations and the simulation environment and features of the HSI. During the simulated scenarios, they observed variables, heard alarms, identified abnormal situations, answered probe questions, and took the actions necessary to recover the abnormal situations. Two kinds of operation for a residue treater can be considered: Startup and Routine. During startup, the residue treater is manually pre-filled with solvent to a minimum level of about 30 percent. 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 the routine operation is started. The current study considers the routine operation.

6.5.1. Scenarios

Two 40-min counterbalanced scenarios are defined. In Scenario 1, the vessel is filled with solvent and heated. Methomyl is added to the residue treater, and a normal recirculation loop flow is ensured to mix the concentrated methomyl feed with preheated solvent in the residue treater. The field operator opens the feed control valve and begins to feed flasher bottoms into the vessel. At normal flow rate, it takes approximately 10 minutes to fill the residue treater to 50 percent, the normal operating level. The recirculation pump is then started. Table 5 shows the timeline of Scenario 1 in which, after 17 minutes,

the residue treater liquid level reaches approximately 51 percent, the temperature ranges between 130 and 135 °C, and the pressure is at 22 psig. The temperature begins to rise steadily about two degrees per minute when the recirculation flow suddenly drops to zero in 30 minutes. In less than three minutes, the temperature is at 147 °C, the highest safe operating limit.

Table 5: 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 50% and the pressure is at 22 psig.
18:00	Automatic feed valve is closed and recirculation pump is then started
23:00	The temperature begins to rise steadily about two 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.
32:00	Cooling water isolation valve is plugged.
35:00	Field operator fails to operate water valve.
37:00	Automatic relief valve fails.
39:00	Scenario is ended.

6.5.2. Probe Questions

Five freezes occur at randomly selected intervals, and they are not predictable by the operators. At the time of the freeze, the HSI is blanked and the simulation is suspended. Each freeze lasts approximately two minutes. The 13 questions, summarized in Table 6, are derived from the GDTA results. Responses to all the questions are collected at each stop via a pop-up window displayed in the HSI. The correct answers are not shown to the operators at freeze times; however, they will be able to see the scenario, probe questions, and their correct answers at the end of the trial.

Table 6: Probe questions for Scenario 1.

Time into scenario (min)	SAW 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, SAR)
24:00	Level 2	What is the most probable explanation? (Failure of the recirculation pump, Failure of automatic level control)
24:00	Level 3	What is the current state of the abnormal situation? (Hazardous, Safe)
31:00	Level 1	Climbing, decreasing, or steady: Which is correct for temperature?
31:00	Level 2	Is SHT abnormal? (Yes, No)
31:00	Level 2	What are the best actions for reduction or containment of risk? (Replace temperature transmitter, Manually control the temperature)
31:00	Level 3	What will be the level of risk? (Acceptable, Tolerable acceptable, Not acceptable)
37:00	Level 1	What is the current level of pressure? (Low, Normal, High)
37:00	Level 2	What are the best actions for reduction or containment of risk? (Automatic relief valve needs maintenance, Field operator should remove accumulating deposits at vent condenser piping)
39:00	Level 3	Is SRR abnormal? (Yes, No)

6.5.3. Results

The conditions of the scenarios along with the operator's responses are assigned to the situational network. For example, if the operator has answered question 1 correctly (i.e. in relation to the actual state of the simulation environment), the success state of the desired object (i.e. failure of control room operator to notice the temperature changes) will have been selected as evidence. If the answer is incorrect,

the failure state will have been selected. If the operator was unable to recognize the abnormal situation, the failure state of the desired object (i.e. failure of control room) will have been selected. If the operator was unable to determine the cause of situation, then the failure state of the desired object (i.e. failure of control room to take appropriate action) will have been selected. Apart from the human responses, the scenario conditions at the determined time are manipulated into the situational network; for example, at min 30, 'failure' is chosen as the state of the recirculation pump.

Both the SAGAT scores and risk assessment results are considered. The final SAGAT scores are calculated by summing all the correct responses for each participant, giving them a possible total score of 13 each. Figure 7 shows the results obtained from Scenario 1.

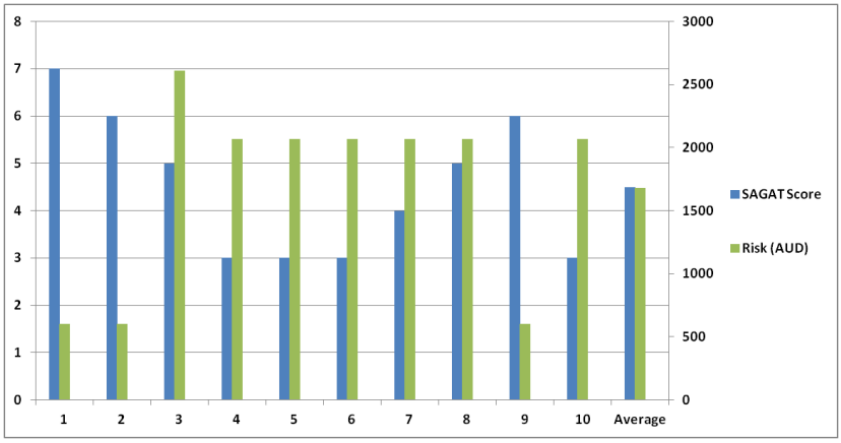


Figure 7: The SAGAT score and risk profile for Scenario 1 using HSI.

It can be seen that, as the SAW scores obtained from the SAGAT for the HSI decrease, the risk profiles significantly increase. The mean total SAGAT score for using the HSI is 4.50 (*SD* =2.27) while the mean risk profile is 16.82E+2. The highest total SAGAT score is 7 and the lowest score is 3. The mean overall SAGAT score for level 1 SAW 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. Clearly, the SAGAT scores for levels 2 and 3 are really low compared to level 1.

6.5.4. The HSI with a Decision Support System

To perform Scenario 2, the HSI was used with the support of a decision support system named the situation awareness support system (SASS), developed by the authors (Naderpour et al., 2014b). The HSI of the SASS is shown in Figure 8. The SASS incorporates the collapsed form of mental models into the display by applying the characteristics of OOBNs. 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 current situation.

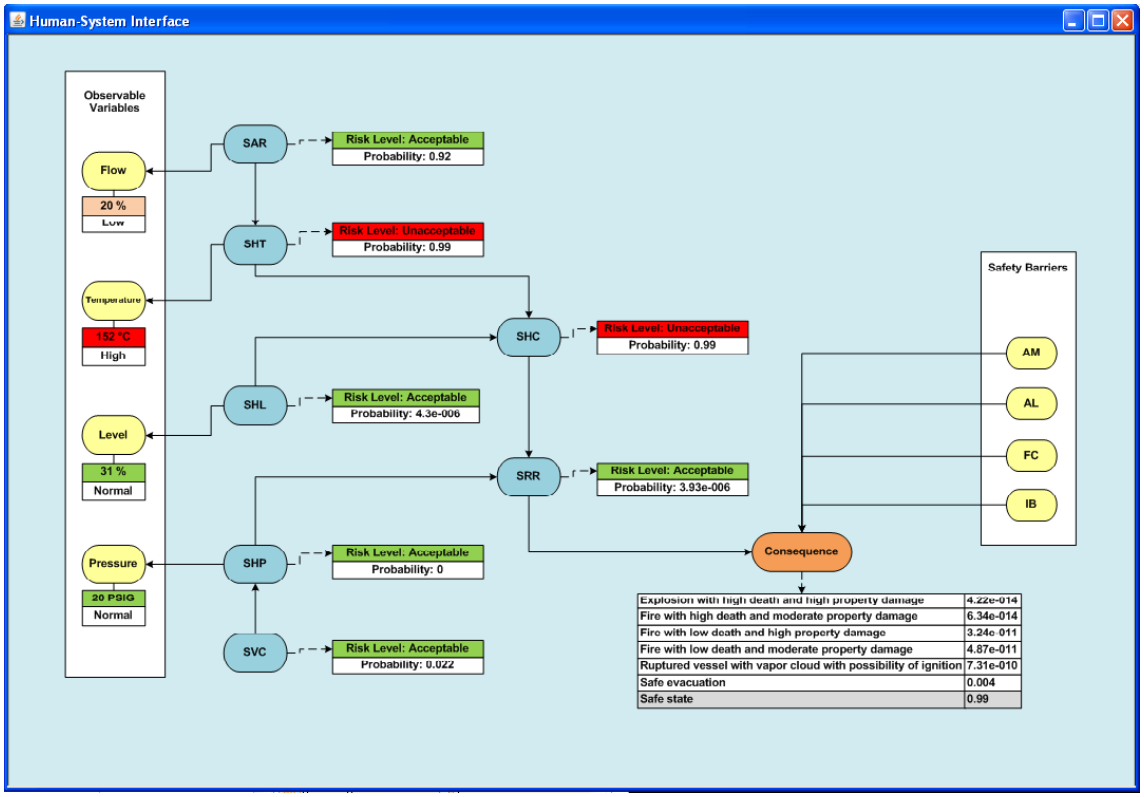


Figure 8: The human-system interface of the SASS.

The mean risk profile for the HSI with the support of SASS is 570.6 as shown in Figure 9 that in comparison with the original HSI, is lower. Analysis of variance (ANOVA) shows that the new risk level is significantly lower with the use of SASS $F(1,18)=18.13$ $p<0.001$.

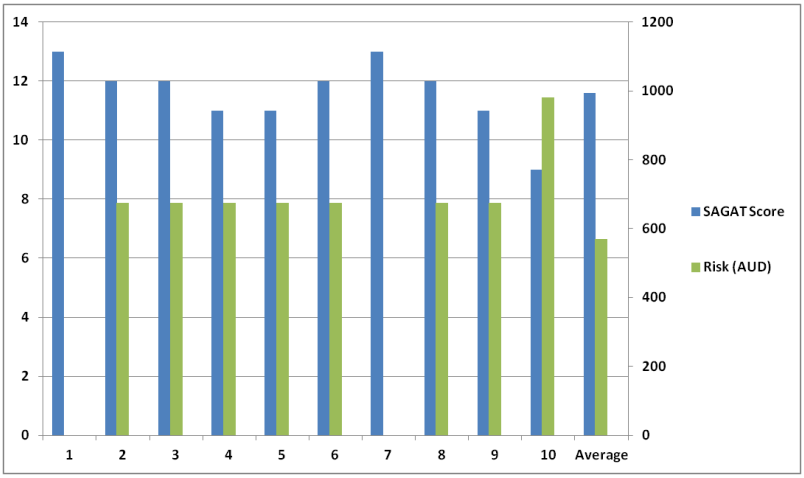


Figure 9: The SAGAT score and risk profile for Scenario 2 with support of SASS.

Table 7 shows the SAGAT scores under different interfaces. The mean total SAGAT score for the modified HSI 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 SAW 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. ANOVA shows that the SAGAT rating of SAW

is significantly higher with the use of the modified HSI $F(1,18)=137.90$ $p<0.001$. The results particularly indicate the improvement in SAW in levels 2 and 3 with the modified HSI.

Table 7: The SAGAT scores under different systems.

Interfaces	SAW level							
	Perception		Comprehension		Projection		Overall	
	M	*SD*	*M*	*SD*	*M*	*SD*	*M*	*SD*
HSI	3.10	0.76	0.60	0.48	0.80	0.17	4.50	2.27
HSI with SASS	3.80	0.17	4.50	0.27	3.30	0.45	11.60	1.37

7. Conclusion and Future Work

In many safety-critical systems today, humans increasingly share the control of systems with automation, rely on HSIs, and move into positions of higher-level decision making. Many recent accidents blamed on operator error could therefore more accurately be labeled as resulting from flawed system and interface design. This paper considers the HSI as an emerging risk issue in such complex systems. The core idea of this paper is formed on the basis of the fact that by designing HSIs that support all levels of SAW, effective and efficient systems that support decision making and performance are more likely to be developed. Mental models play a key role in how information is interpreted, comprehended and used to make projections. Therefore, a HSI risk assessment method is proposed based on operators' mental models, and SAGAT to evaluate HSIs in simulated environments. The performance of the proposed method was investigated through a case study at a case study concerning a residue treater at a virtual chemical plant. Ten experienced operators participated in this study to interact with the HSI and respond to the online probe questions, and a risk level was produced by taking into account the operators' responses as evidence in the BN-based situation models. The results show that the proposed method can be successfully used in the design and evaluation processes of HSIs of dynamic systems.

Attention and working memory decay are also important factors that affect operators' SAW. The future direction of this study will take both these factors into account in the risk assessment process, along with the mental workload, to provide more realistic results.

Acknowledgment

The work presented in this paper was supported by the Australian Research Council (ARC) under Discovery Project DP140101366. In addition, the authors sincerely thank those who took part in this study.

References

Adams, M.J., Tenney, Y.J., Pew, R.W., 1995. Situation awareness and the cognitive management of complex systems. Human Factors 37, 85-104.
Bedny, G., Meister, D., 1999. Theory of activity and situation aewareness. International Journal of Cognitive Ergonomics 3, 63-72.
Carvalho, P.V.R., dos Santos, I.L., Gomes, J.O., Borges, M.R.S., Guerlain, S., 2008. Human factors approach for evaluation and redesign of human-system interfaces of a nuclear power plant simulator. Displays 29, 273-284.
Chemical Safety Board, 2011. Pesticide Chemical Runaway Reaction Pressure Vessel Explosion, Washington, DC.
Endsley, M., 1995a. Measurement of situation awareness in dynamic systems. Human Factors: The Journal of the Human Factors and Ergonomics Society 37, 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 37, 32-64.
Endsley, M.R., 2000a. Direct measurement of situation awareness: Validity and use of SAGAT, In: Endsley, M.R., Garland, D.J. (Eds.), Situation awareness analysis and measurement. Lawrence Erlbaum Associates, Mahwah, NJ, pp. 147-173.

Endsley, M.R., 2000b. Situation models: An avenue to the modeling of mental models, Proceedings of the Human Factors and Ergonomics Society Annual Meeting. SAGE Publications, pp. 61-64.
Endsley, M.R., Bolté, B., Jones, D., 2003. Designing for situation awareness: an approach to user-centered design. Taylor & Francis.
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.
Endsley, M.R., Garland, D.J., 2000. Situation awareness: analysis and measurement. Lawrence Erlbaum, Mahwah, NJ.
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.
Fuchs-Frothnhofen, P., Hartmann, E.A., Brandt, D., Weydandt, D., 1996. Designing human-machine interfaces to match the user's mental models. Control Engineering Practice 4, 13-18.
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 94, 1557-1567.
Isaac, A., Shorrock, S.T., Kirwan, B., 2002. Human error in European air traffic management: the HERA project. Reliability Engineering & System Safety 75, 257-272.
Jenkins, D.P., Stanton, N.A., Walker, G.H., 2012. Distributed situation awareness: Theory, measurement and application to teamwork. Ashgate Publishing, Ltd.
Jones, D.G., Endsley, M.R., 2004. Use of real-time probes for measuring situation awareness. International Journal of Aviation Psychology 14, 343-367.
Jovanovic, A.S., Balos, D., 2012. iNTeg-Risk project: concept and first results. Journal of Risk Research, 1-17.
Kim, M.C., Seong, P.H., 2006. An analytic model for situation assessment of nuclear power plant operators based on Bayesian inference. Reliability Engineering & System Safety 91, 270-282.
Lee, H.-C., Koh, K.-Y., Seong, P.-H., 2013. Application of a computational situation assessment model to human system interface design and experimental validation of its effectiveness. Annals of Nuclear Energy 56, 158-171.
Lee, S.J., Kim, M.C., Seong, P.H., 2008. An analytical approach to quantitative effect estimation of operation advisory system based on human cognitive process using the Bayesian belief network. Reliability Engineering & System Safety 93, 567-577.
Melchers, R.E., 2001. On the ALARP approach to risk management. Reliability Engineering & System Safety 71, 201-208.
Naderpour, M., Lu, J., Zhang, G., 2014a. The explosion at Institute: Modeling and analyzing the situation awareness factor. Accident Analysis & Prevention 73, 209-224.
Naderpour, M., Lu, J., Zhang, G., 2014b. An intelligent situation awareness support system for safety-critical environments. Decision Support Systems 59, 325-340.
Naderpour, M., Lu, J., Zhang, G., 2014c. A situation risk awareness approach for process systems safety. Safety Science 64, 173-189.
Naderpour, M., Lu, J., Zhang, G., 2015a. An abnormal situation modeling method to assist operators in safety-critical systems. Reliability Engineering & System Safety 133, 33-47.
Naderpour, M., Nazir, S., Lu, J., 2015b. The role of situation awareness in accidents of large-scale technological systems. Process Safety and Environmental Protection.
Nazir, S., Colombo, S., Manca, D., 2012. The role of situation awareness for the operators of process industry. CHEMICAL ENGINEERING TRANSACTIONS 26, 303-308.
Nazir, S., Colombo, S., Manca, D., 2013. Minimizing the Risk in the Process Industry by Using a Plant Simulator: a Novel Approach. CHEMICAL ENGINEERING TRANSACTIONS 32, 109-114.
Nazir, S., Kluge, A., Manca, D., 2014a. Automation in Process Industry: Cure or Curse? How can Training Improve Operator's Performance, In: Jiří Jaromír Klemeš, P.S.V., Peng Yen, L. (Eds.), Computer Aided Chemical Engineering. Elsevier, pp. 889-894.
Nazir, S., Sorensenb, L.J., Øvergårdb, K.I., Manca, D., 2014b. How Distributed Situation Awareness Influences Process Safety CHEMICAL ENGINEERING TRANSACTIONS 36, 409-414.
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.
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 56, 89-95.
Pridmore, J.L., 2007. Designing for the improvement of operator situation awareness in automation systems. Auburn University, Alabama, U.S.
Rouse, W.B., Morris, N.M., 1986. On looking into the black box: Prospects and limits in the search for mental models. Psychological bulletin 100, 349–363.
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 9, 297-323.
Sneddon, A., Mearns, K., Flin, R., 2006. Situation awareness and safety in offshore drill crews. Cognition, Technology & Work 8, 255-267.
Taylor, R.M., 1990. Situational Awareness Rating Technique (SART): the development of a tool for aircrew systems design, Situational Awareness in Aerospace Operations, pp. 1-17.