

DEVELOPING A DATABASE TO ALLEVIATE THE PRESENCE OF MUTUAL MISCONCEPTIONS BETWEEN DESIGNERS AND OPERATORS OF PROCESS PLANTS

B.P.Das[1], P.W.H.Chung, J.S.Busby* and R.E.Hibbered*
Department of Computer Science, Loughborough University, Loughborough, UK.
* Department of Mechanical Engineering, University of Bath, Claverton Down, Bath, UK.

In this paper the development work concerning a novel system – *Mutual Misconception Database* is reported. The term *misconception* for this paper refers to the possession of an incorrect belief by the individual about some aspect of the complex system. Marine and process plant (off-shore and on-shore) accident case histories, which are available in public domain, are used in developing the system. It is based on the premise that mutual misconceptions occur between designers and operators. Prior to the commencement of this work, the authors could not locate any tools designed specifically for the identification of mutual misconceptions in accidents. This prompted the development of a mutual misconceptions database system, which should eventually assist in the elimination of the presence of these mutual misconceptions. In the body of this paper, the rationale that underlies the development of the database, the manner in which accidents were analysed, together with an example accident analysis including brief description of the database system are presented. Many interesting observations are made relating to misconceptions at appropriate places of the paper. The paper concluded with an examination of the potential uses of the database system that has been developed particularly as the starting point for the developing intelligent agenda-setting mechanisms that are integrated with other computer-based systems.

Keywords: Accident, Database, Design, Misconception, Mitigation, System

INTRODUCTION AND OVERVIEW OF THE PAPER

Researchers at Loughborough University and the University of Bath have begun a project to investigate the role of mutual misconceptions in marine and process plant (off-shore and on-shore) accidents. The project is based on the premise that mutual misconceptions occur between designers and operators. In other words, designers may have specific beliefs about the manner in which operators can and will behave, whilst operators possess beliefs about the behaviours that designers wish them to enact.

In this project, the term ‘operators’ does not simply refer to those individuals who are engaged in the manipulation of complex systems’ user interfaces. It includes all other personnel involved in the operation of the complex system, such as maintenance personnel and managers. Further, the project does not constrain itself solely to investigation of errors that arise in the control room of a complex system. Rather, consideration is given to both the artefacts, such as storage vessels that comprise a complex system, and the procedures, such as permit-to-work systems, which dictate its operation.

This research hopes to identify the types of mutual misconceptions that arise and can suggest means by which to alleviate the occurrence of these misconceptions. It is also expected that a computer-based system can be developed which would promote the application of lessons learnt from previous accidents to novel situations and previously unused artefacts.

Prior to the development of such a system, it is necessary to identify and classify those misconceptions that have been found to contribute to accidents in complex systems. To

[1] Corresponding author. Email: B.P.Das@lboro.ac.uk

achieve this goal, a database has been developed, and it is this, which is the subject of this paper.

In order to provide insight into the development of this database, this paper is composed of a further five sections. The following section will introduce the rationale that underlies the development of the database. Following this, the manner in which accidents were analysed will be described, together with an example accident analysis. Consideration will then be given to the data that is considered to be significant in this analysis and that should inform the development of the database system. This database system will be described in the following section. The paper will conclude with an examination of the potential uses of the database system that has been developed.

THE NEED FOR A MUTUAL MISCONCEPTION DATABASE SYSTEM

In this paper, the term *misconception* refers to the possession of an incorrect belief by the individual about some aspect of the complex system. This may include misconceptions about those who design or operate the system, the environment in which the complex system can and should be used, the processes and activities enacted, and the properties of materials employed within the system. Such mutual misconceptions may arise from the manner in which the artefacts within the complex system communicate with the operator, the knowledge possessed by the operator, and the perceptions held of the dispositions of those responsible for the design and operation of the complex system.

The accident analyses conducted by (King, Hirst and Evans)[1] indicated the significant role of mutual misconceptions in accident causation. However, prior to the commencement of this project, there were no tools designed specifically for the identification of mutual misconceptions in accidents. This prompted the development of a mutual misconceptions database system, which should eventually assist in the elimination of the presence of these mutual misconceptions. It is envisaged that the database can form the basis for a tool that would assist designers in identifying potential sources of mutual misconceptions. This tool would provide strategies for reducing the presence of mutual misconceptions and would be used at crucial decision-processes during the design process.

THE CONDUCT OF ACCIDENT ANALYSES

Given that the aim of this project is to identify and classify the mutual misconceptions that underlie specific accidents, it is necessary to analyse specific accidents for their presence. It is impossible to predict *a-priori* when an accident will occur, therefore accident analysis can only be conducted retrospectively. Fortunately, researchers such as (Kletz)[2] have recognised this, and collated case-histories of accidents. Their intentions have been to identify the specific factors that contributed to a specific accident and remove them in some manner or mitigate their effects. These case histories form the foundation for the authors' database system.

Conduct of the causal analysis allows the identification of both the goals adopted by operators, and also the actions enacted to attain these goals. Causal analysis can identify those actions and goals that were inappropriate in relation to specific process plants. Further, an understanding of the reasons why the operators goals or actions were inappropriate can also identify the mutual misconceptions that arose from designers inappropriate beliefs about the manner in which the process plant would be used, or the manner in which it could be used.

Whilst identification of a root cause may provide a means to identify a specific inappropriate action from operators that the designer can avoid, the analysis of mutual misconceptions provides a means by which to understand why both designers and operators failed to consider the presence or consequences of specific actions. In the next section of the paper, attention will be given to the analysis procedure that was adopted for the identification of mutual misconceptions.

REQUIREMENTS FOR A MUTUAL MISCONCEPTIONS DATABASE SYSTEM

THE METHOD EMPLOYED FOR ANALYSIS

The mutual misconceptions database system relies upon a methodology that allows the identification of the mutual misconceptions that contributed to a specific accident. This procedure requires the identification of a specific outcome, and the immediate cause of this. Following from this it may be possible to further identify subsidiary causes that contributed to the immediate cause. The identification of subsidiary causes continues until the root causes presented within the case-history are identified, which may constitute either active errors, actions committed by operators, or latent errors, causal factors arising from decisions taken during the design of a particular process plant (Reason)[3]. Once root causes have been identified it is then possible to consider the mutual misconceptions that may have contributed to this specific accident. This data can then be included within the fields of the mutual misconceptions database system.

ILLUSTRATION OF THE MANNER IN WHICH ANALYSIS IS CONDUCTED

In order to illustrate the analysis procedure that has been used, an accident case-history available in the public domain, in (Kletz)[2] is first presented in Table 1. It looks at an *explosion* that took place in a process plant's batch reactor circulating system. Based on this case-history first of all an overall analysis is done as shown in Table 2. It leads to identify consequences of incident/accident and assists in finding answers to the subsequent question of "*Why*". Next causation analysis of all the consequences of incident/accident as identified from the previous stage is carried out which is briefly shown in Figure 1. It eventually leads to misconceptions held by an individual. The last part of the procedure develops the misconceptions in a concise manner as shown in Table 3.

There are six main misconceptions included in the causation of this accident, four of which arise from the beliefs held by the designer of the system, two of which arise from the operators beliefs. The first of these misconceptions was the designers' expectation that the operator would not make use of the system unless all alarms and instruments were operating in an appropriate manner. This presumed that the operator was able to identify the state of alarms and instruments, and that they would not be subject to external pressures that would encourage use of the system when it was in a non-functional state.

Another misconception held by the designer, was the expectation that the operator would heed all warning signs and would be able to conduct appropriate diagnosis of the state of the system. Further, the designer did not perceive any reason for providing a means to directly measure the physical properties of the system. The ability to directly measure the properties may have encouraged the operator to test their hypotheses about the state of instruments within the system. The last misconception held by the designer, was that explosion couldn't occur in a reactor because of their robust design. Probably the designer was not aware of an incident like this.

It is possible to identify two main misconceptions held by the operators of the plant. The management assume that it is unnecessary to monitor the state of key instruments within the system. In this case, the management appeared ignorant of the importance of ensuring that there are properly functioning instruments monitoring the performance of the system.

The operator demonstrates another misconception, which suggests ignorance of the consequences of their actions upon the state of the system. In this case it is apparent that the operator lacks strategies for effective diagnosis of system state or for simulating the consequences of their actions. Such actions may reflect a belief that the designer would provide a means to prevent them from conducting inadvisable actions, that the system would not fail in a catastrophic manner, or that the system had adequate defences to alleviate the consequences of inadvisable actions.

GENERAL CONCLUSIONS FROM THE ANALYSES

In this section, consideration is given to some of the conclusions that can be drawn from the analysis of these cases. In all we have studied 50 cases that are related to the operation of complex systems. These have been acquired from a number of sources including (Crowl and Louvar)[4], (Kletz)[2], the Marine Accident Investigation Board's Safety Digest amongst other sources. This study covers accidents that occurred with a variety of artefacts, failure modes, process operations and personnel. For example, artefacts examined included marine vessel auto-pilots, pipelines, reactors and valves amongst others. Process operations examined included preparation for maintenance, process control, amongst others. The analyses also included a variety of personnel including designers, managers, maintenance personnel, operators and supervisors.

Given the nature of the data presented in the case-histories analysed, it was difficult to find evidence of the actual psychological processes that underlie operator performance. For example, in the case-history presented in the previous section, the operator's decision to open the valve at the base of the reactor may have been simply because the operator forgot the appropriate procedure for the operation of this reactor. It may also have been the case that the operator lacked specific knowledge about the relationships between the components of the system and the dynamics of the reaction being controlled. However, these case-histories do allow the identification of the mutual misconceptions that could have potentially contributed to a specific accident. They allow us to identify what should have been known to ensure that these forms of accidents are not repeated.

In many of the case-histories that were studied, it was possible for the operator to overlook the recommended operating procedures. Related to this was the possession of inappropriate knowledge by operators, typically they appeared to lack an understanding of the relationships between the components of the system they were using, procedural models instead of structural models (Preece, Rogers, Sharp, Benyon, Holand and Carey)[5]. The nature of the system may also allow modelling of inappropriate behaviours by other personnel. That is an accident may not necessarily arise from the use of a non-recommended procedure, and this provides reinforcement for its use (Bandura)[6,7]. Further, there may be conflicting goals pursued by operators, safety goals being usurped by production goals (Reason)[3]. Indeed, there are many other psychological biases that may suggest means by which inappropriate behaviours are enacted, and by which mutual misconceptions develop.

The question arises as to why these mutual misconceptions should develop. It is possible that there are limitations to the degree to which designers can recall appropriate knowledge about the environment in which the artefact is to be used, possibly through lack of access to appropriate individuals (Katz and Khan)[8]. Further, both operators and designers may

have differing expectations about the manner in which the others would perceive them. That is there may be projection of specific attitudes and values held by one group of individuals onto the other (Katz and Khan)[8]. The manner in which these mutual misconceptions arise is however addressed elsewhere.

DESCRIPTION OF THE MUTUAL MISCONCEPTIONS DATABASE SYSTEM

THE SYSTEM AND FUNCTIONS

Following analysis and collation of required information from accident reports, the Mutual misconception database system is developed using the Microsoft Access database management system. Currently the user interface of the Mutual misconception database system, (Figure 2) provides six menu options: (1) View case list (2) View case details (3) View Misconceptions (4) View reports (5) View notes (6) Quit the system.

The first menu option gives a choice of viewing accident cases by type of complex system involved, namely; (a) *Marine accidents* (b) *Offshore platform accidents* (c) *Process plant accidents*. For each category, it provides facilities to view full list of cases, the corresponding sources and the casual network of causation leading to primary consequences of an accident (Figure 3).

The second menu option of the system also gives the user a choice of viewing accident case details by type of complex system involved. For each category, the *source* of the case, the *narrative* containing brief description of the accident, the *causation* of the accident in the form of two dimensional *step* diagram linking consequences and corresponding causes can be viewed through this option (Figure 4). It also provides further facility to look into the corresponding misconceptions that were identified from the analysis of the case.

The third menu option of the system provides the facility of looking at the complete list of misconceptions associated with the subjects possessing those misconceptions, whether designer or operator. Each misconception is described in a short sentence. Again by clicking a particular misconception with a mouse pointer the user can view the *subject*, *object*, *description* relating to the misconception, *lessons learnt* from the incident and the *remedy* prescribed (Figure 5).

The fourth menu option of the system provides a formatted report of all the misconceptions available within the system. This report is generated automatically and is dynamic in nature. The user has the option of viewing them on the screen or to obtain a hard copy for detailed analysis. Finally, the fifth and sixth menu options allow the user to access a blank note pad facility and to exit the database system.

THE RESULT

Varieties of reports can be generated out of this system depending on user's requirements. A typical report containing list of misconceptions, the lessons learnt and remedy is given in Table 4.

CONCLUSIONS

This research has investigated the means by which to develop a database that provides data on a hitherto ignored contributor to accident causation in complex systems. It suggests a means by which to structure case-histories of accident causation that provides analyses that can be universally applied for a variety of design tasks.

The development of this database requires the involvement of individuals with appropriate expertise. In the case of this project, there is a need to gain the involvement of those with expertise in process operations, process plant design, psychology, and user-interface design. It is preferable that each case-history is analysed by as many members of the group as is possible. Such an approach allows the identification of ambiguities in the case-history and allows the identification of invalid conclusions.

The analyses that have been conducted suggest that in any accident there may be a number of mutual misconceptions operating. Further, the identity of the mutual misconceptions that caused different personnel to make errors may differ. This suggests a need to present specific remedies according to the different groups involved in the design and operation of complex systems. Further, it is recognised that identification of a specific mutual misconception does not in itself suggest any means by which to remedy it. Consequently, within the database, consideration has been given to the specific lessons that can be learned from specific case-histories and also to the remedies that these suggest.

It is expected that in the future, this type of database could provide a starting point for the development of intelligent agenda-setting mechanisms that are integrated with other computer-based systems. For example, it may be possible to integrate this type of database with computer-aided design tools and indicate to the designer where assumptions are based on an unrealistic view of the operator. Similarly, the database could be integrated with permit-to-work systems to ensure that operators are conducting work that does not assume an unrealistic model of the designer. However, such development is as yet only a future possibility, and relies upon further development upon the analyses that have been presented in this paper.

REFERENCES

1. King, R., Hirst, R. and Evans, G., 1998, King's Safety In The Process Industries. Second Edition, Arnold: London, UK
2. Kletz,T., 1998, *What Went Wrong? Case Histories of Process Plant Disasters*. Fourth Edition, Gulf Publishing Company: Houston, Texas, USA
3. Reason, J., 1991, *Human Error*. Cambridge University Press: Cambridge, UK
4. Crowl, D. A. and Louvar, J. F., 1990, *Chemical Process Safety Fundamentals with Applications*. Prentice Hall: New Jersey, USA
5. Preece, J., Rogers, Y., Sharp, H., Benyon, D., Holland, S. and Carey, T., 1994, *Human-Computer Interaction*. Addison-Wesley: Harlow, UK
6. Bandura, A., 1965, Influence of model's reinforcement contingencies on the acquisition on imitative responses. *Journal of Personality and Social Psychology*, **1**: 589-595
7. Bandura, A., 1965, 'Vicarious processes: A case of no-trial learning' in L. Berkowitz (Ed.) *Advances in Experimental Social Psychology* (*Vol. 2*), Academic Press: New York, USA
8. Katz, D. and Khan, R.L., 1978, *The Social Psychology of Organizations* (*2nd. Edn.*), Wiley: New York, USA

Table 1. Example accident case-history

(Kletz)[2] described an accident that took place in a batch reactor circulating system. This system consists of ethylene oxide feed pump, reactor, circulation pump, heat exchanger and catalyser forming a closed loop including associated control instruments such as pressure indicator, temperature indicators, flow indicator alarm and trip initiator. In short the material first flows through the reactor then through the circulation pump into the heat exchanger and finally into the catalyser from where it goes back to the reactor again.

The process starts with a batch of glycerol, which is placed in the reactor and then circulates through the heat exchanger and the catalyser. The heat exchanger of the system acts both as a heater and a cooler. At the beginning of the process, this heat exchanger acts as a heater, its role being to raise the temperature of the glycerol in the reactor to 115° Celsius. Once the glycerol reaches this temperature, ethylene oxide is then added to the reactor through the ethylene oxide feed pump. The reaction of the glycerol and the ethylene oxide is exothermic, and it is at this stage that the heat exchanger is used as a cooler to cool the reaction.

There are three conditions that has to be met before ethylene oxide could be added to the reactor. Firstly, the circulation pump must be running. Secondly, the temperature of the reactor's contents has to exceed 115° Celsius. If this condition is not met there would be no reaction between the glycerol and the ethylene oxide. Thirdly, temperature must be kept below 125° Celsius; else the reaction would be potentially explosive.

Although, the three conditions above identify three conditions that should ensure safe production using this batch reaction system, in this case-history an explosion did occur. In this case-history, the operator was confronted with a pressure indicator that showed rising pressure within the reactor, which indicated that there was no reaction between the ethylene oxide and the glycerol. On the basis of this indicator, the operator decided that the indicated temperature was reading too low, and so added more heat to encourage the start of the reaction. The trip setting was manually adjusted to allow this, and the indicated temperature was allowed to rise to 200° Celsius. However, the pressure reading indicated that the reaction had still not begun.

The operator then began to suspect that this theory about the state of the batch reactor could be wrong. At this point, the operator looked at other potential hypotheses to explain the present state of the reactor, and realised that a valve at the base of the reactor was shut. In order for the reaction to occur, the operator recalled that this valve needed to be opened, and so opened this valve. The resulting reaction from the two chemicals at a temperature that was in excess of 125° Celsius burst the reactor and released a plume of escaping gas. As a result two other operators were injured, one by flying reactor debris, the other by being blown off from the top of a tank truck.

Subsequent investigation indicated that at the time of accident key instruments were not kept in working order.

Table 2. Overall analysis of example accident case-history

Operation:
Operator started the addition of ethylene oxide in a reactor, so that the reaction with a batch of glycerol can take place.
What happened:
An explosion occurred in the reactor.
What is the immediate cause of accident:
Human error; Misdiagnosis of the state of the reactor.
How it happened:

a. Increase in reactor pressure indicated that no reaction was taking place between the ethylene oxide and glycerol.
b. Operator attempted to promote reaction by raising the temperature in the reactor by altering the trip setting.
c. Opened the valve at the base of the reactor to promote reaction when the temperature of the reactor's contents was in excess of 125º Celsius.

What are the consequences of the accident:

a. Explosion ruptures reactor.
b. Gas ejected from reactor.
c. Two men injured as a result of flying debris and escaping gas.

What are the causes of the accident:

a. A pump was running with a closed suction valve, got hot and the heat affected the temperature measuring point of the reactor which was outside as well as close to the circulation pump.
b. The operator opened the valve at the base of the reactor at wrong time.
c. A violent uncontrolled reaction occurred as unreacted ethylene oxide together with glycerol passed through the heat exchanger and catalyser of the system.

Who are involved (direct):
An Operator
Who are involved (indirect):
The Designer of the system and the Manager of the plant.

Table 3. Misconceptions as developed from causation analysis of example accident case-history

By Designer:

1. The designer failed to foresee that if an alarm does not operate, the system must stop automatically, otherwise operator might attempt to operate the system manually.

2. The designer failed to foresee that operator could fail to heed warning sign and try his own remedial process through his own thought process, which might cause and fail to provide adequate safeguard.

3. The designer failed to foresee importance of direct measurement of physical properties of the system at the crucial points and consequently made no provision.

4. The designer failed to foresee that an explosion can happen around the reactor and failed to provide adequate explosion guard for flying debris, blown off by high-pressure burnt gas.

By Manager:

1. The manager failed to foresee the importance of keeping key instruments in working order and prevent operator to operate the system without them.

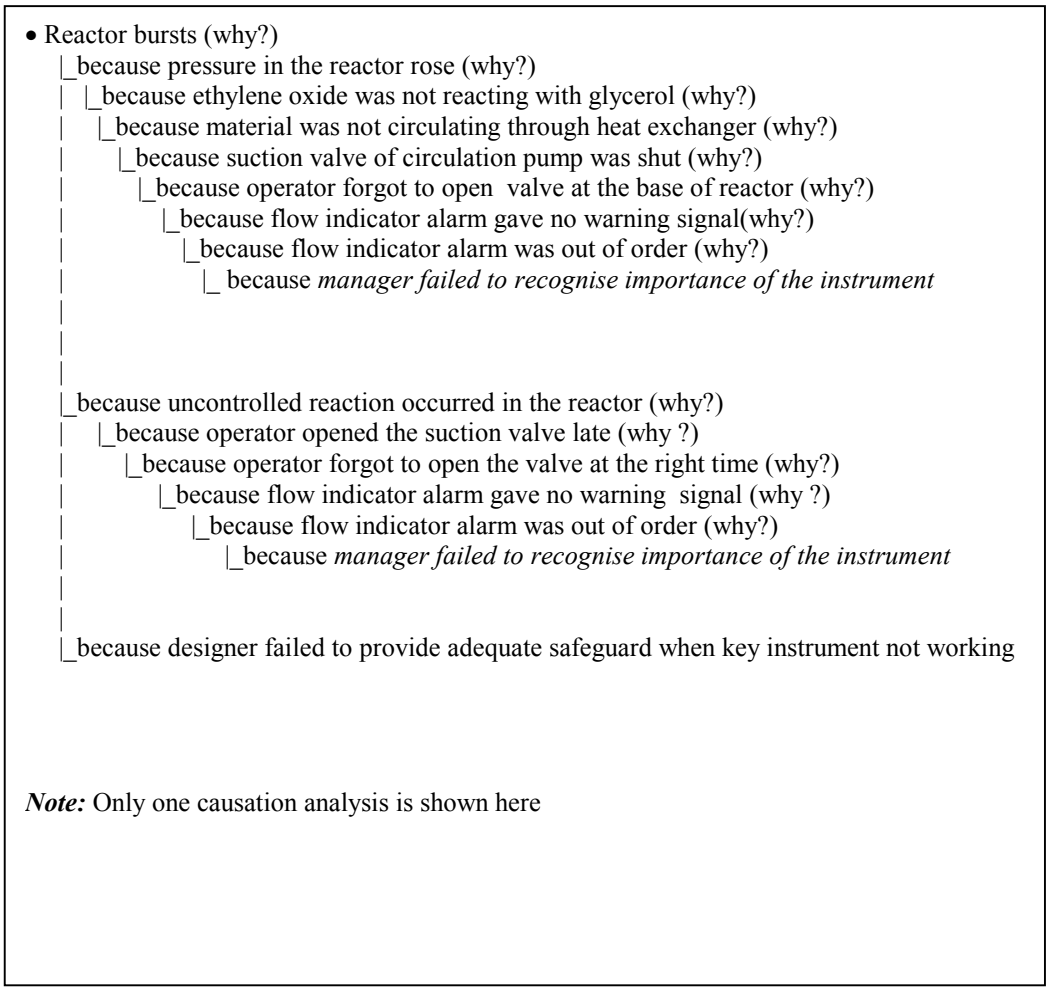
By Operator:

1. The operator failed to understand the severity of making wrong decision in adjusting interlock settings and the designer failed to prevent the operator in making such decision.

Table 4. List of misconceptions, the lessons learnt and remedy

fragment	291
description	The designer failed to foresee that an explosion can happen and failed to provide adequate explosion guard for flying debris which might be blown off by high pressure burnt gas.
misconception	explosion can not happen in a reactor
subject	designer
object	operator
lessons learnt	explosion can happen in a reactor and debris will scatter across the plant causing damage to equipment and plant personnel.
remedy	In order to contain debris flying all over the place of the plant and causing damage, a reactor must be provided with explosion guard or located outside the main plant in an explosion proof building.

Figure 1. Causation analysis of the example accident case-history



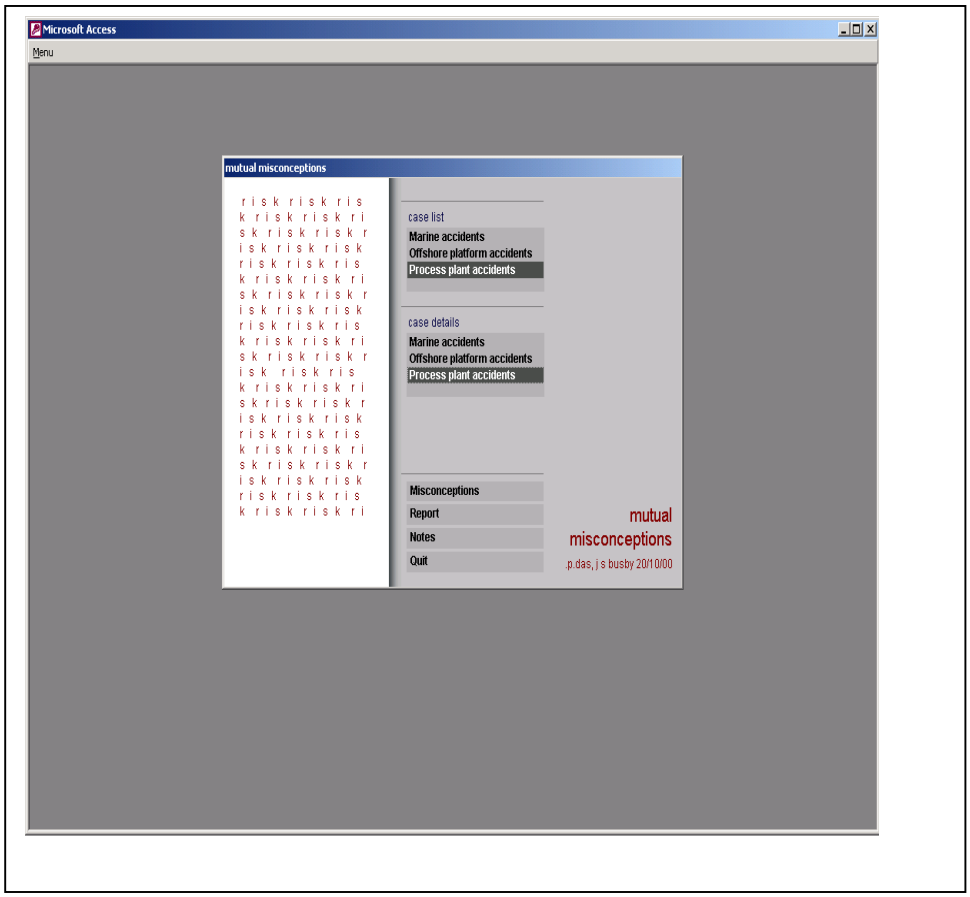


Figure 2. User Interface of the Mutual Misconception Database System

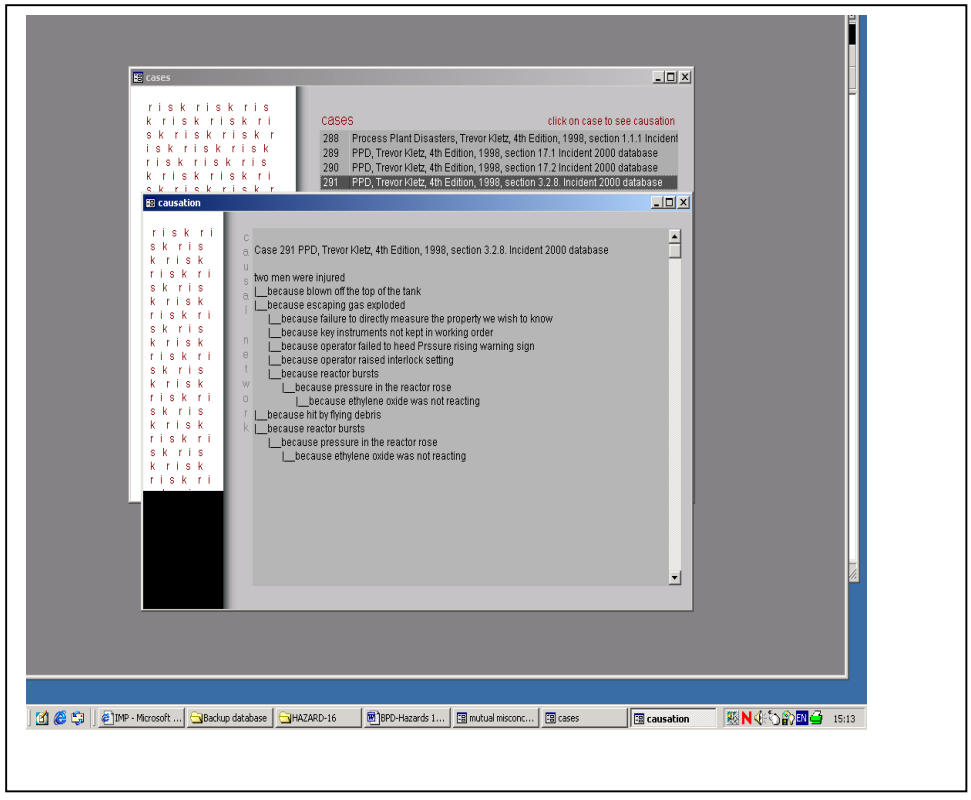


Figure 3. A view of the case list of the Mutual Misconception Database

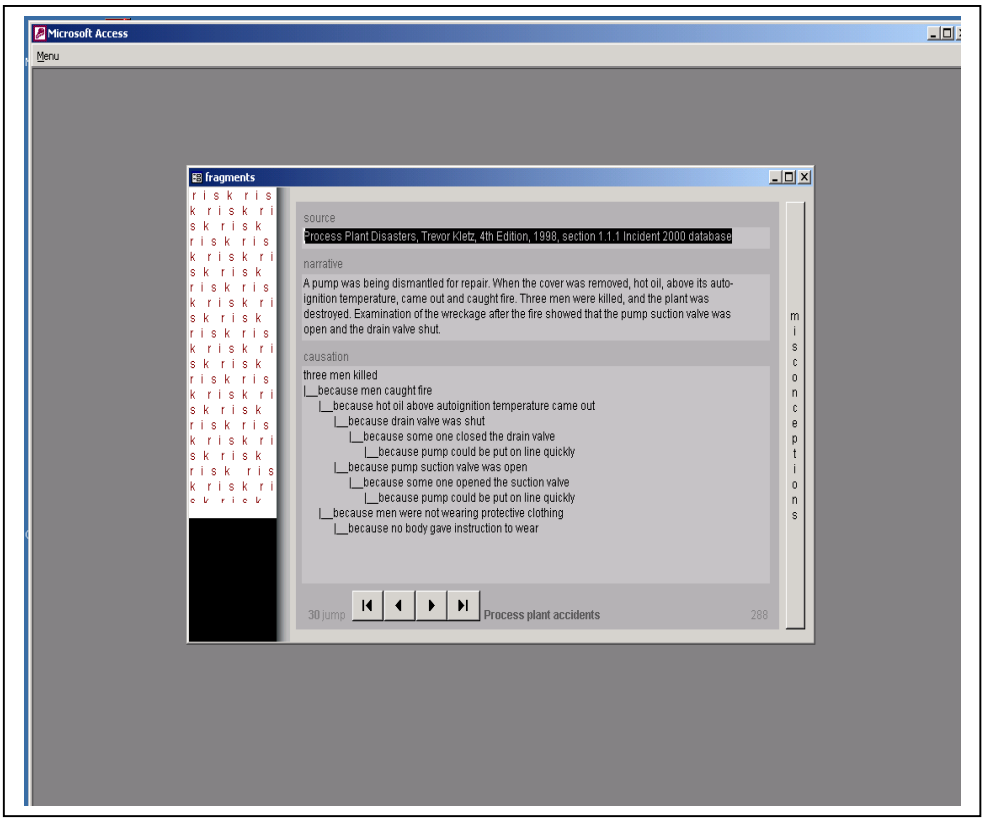


Figure 4. A view of the case details of the Mutual Misconception Database System

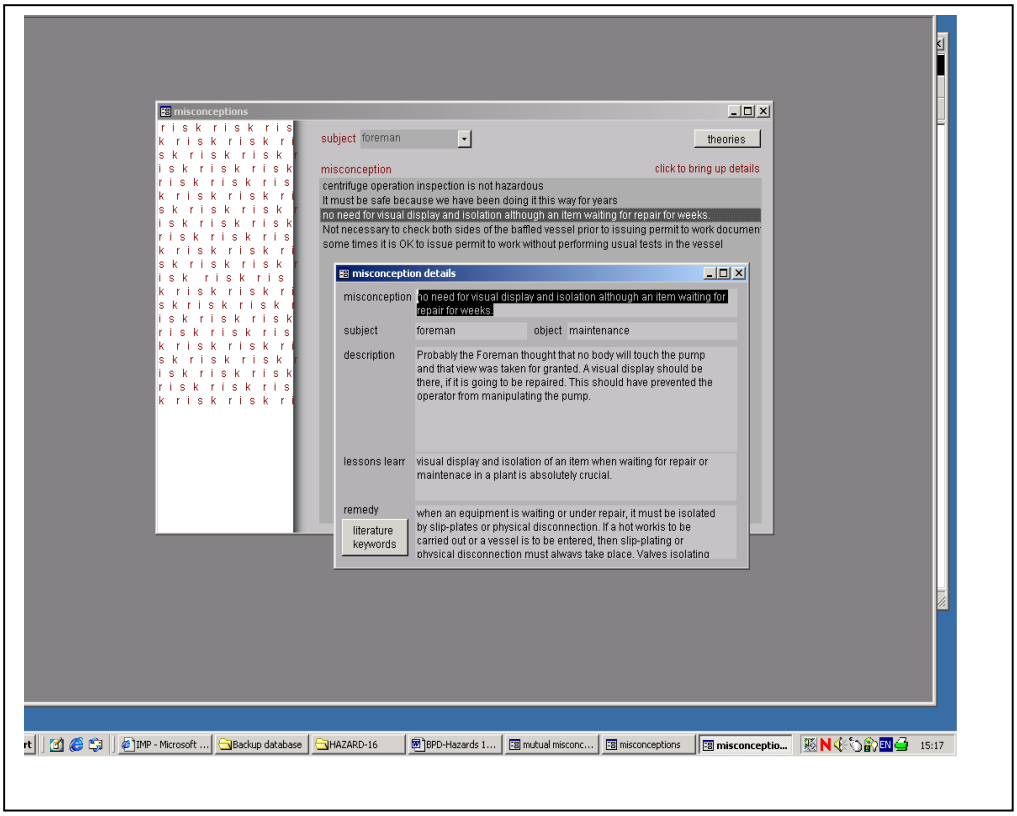


Figure 5. A view of the misconception details of the Mutual Misconception Database System