Korean J. of Chem. Eng., **11**(3), 153-161 (1994)

SAFETY ANALYSIS USING AN EXPERT SYSTEM IN CHEMICAL PROCESSES

Heeyeop Chae, Yeo Hong Yoon and En Sup Yoon†

Dept. of Chem. Eng., Seoul National University, Seoul 151-742, Korea

(Received 19 July 1993 • accepted 24 March 1994)

Abstract—A knowledge-based expert system for hazard and operability study (HAZOP) is developed. HAZOP study is regarded as one of the most systematic and logical qualitative hazard identification methodologies. But, it requires a multidisciplinary team and is very time-consuming and repetitious task in nature. By developing an computer-aided automation system, these drawbacks of HAZOP study can be overcome. Considerable manpower and time can be reduced and even past experiences of engineers and existing checklists can be stored for future use in the form of knowledge base. The developed knowledge-based HAZOP expert system has a frame-based knowledge structure for equipment failures and process properties, and rule networks for consequence reasoning which uses both forward and backward chaining. The system is open-ended and modular in structure to make it easy to implement wide process knowledge for future expansion. LPG storage and fractionation process has taken as example to test the applicability of the developed system as an automated HAZOP study system. The result shows that savings more than 50% of the required manpower and time for HAZOP studies can be achieved, and the system is very efficient and reliable, too.

INTRODUCTION

To prevent and eliminate hazards is one of the main concerns for various chemical processes from the design to the operation stage and there are many hazard identification techniques at each project stage.

Generally, two steps are required for complete safety analysis in chemical industries. The first step is hazard identification of a process and qualitative analysis is carried out in this step. Scenarios for the propagation of hazardous events can be found at the step by various qualitative hazard identification methods - checklists, safety audit, Dow and Mond hazard indices, preliminary hazards analysis, What-If analysis, failure modes, effects and criticality analysis (FMECA), and hazard and operability study (HAZOP) [1]. Among them, HAZOP have been regarded as the most widespread and systematic methodology for hazard identification during the last two decades.

The second step is risk assessment of the scenario produced in the previous step, and quantitative analysis is performed. A risk assessment procedure that determines probabilities is frequently called probabilistic risk assessment - fault tree analysis (FTA) and event tree analysis (ETA) [4]. The probabilistic techniques require a data base of frequencies of occurrences for specific accident scenarios. Consequence analysis is also required for risk assessment because risk is defined as the product of the probabilities of occurrences of an events and their consequences. Consequence analysis is site-specific and must consider the type of hazard involved, site-location, population density and prevailing weather patterns. When the consequences of an undesired event are calculated, both health and economic effects should be considered.

Hazard identification is more deterministic for process design than risk assessment because it provides scenarios to risk assessment and contains many process knowledge about safety and design. This work has focused on the hazard identification of safety analysis with HAZOP using an expert system approach. This work enables process designer to consider safety factors and something to be improved with the developed system.

HAZOP (HAZARD AND OPERABILITY STUDY) AND THE MODIFICATION FOR THE EXPERT SYSTEM

HAZOP studies should be carried out by a multidis-

†To whom all correspondences to be addressed.

Table 1. Guide words and their meanings

Guide words	Meaning
No	Negation of intention
Less	Quantitative decrease
More	Quantitative increase
Part of	Qualitative decrease
As well as	Qualitative increase
Reverse	Logical opposition of intention
Other than	Complete substitution

ciplinary team through brainstorming meetings when the design is fairly firm. A typical HAZOP team consists of process engineers, instrument engineers, safety engineers, chemists, maintenance personnel. HAZOP begins with a full description of the process with process flow diagram (PFD), piping and instrumentation diagram (P&ID), and operation manuals. To study systematically, they have to divide the process into small processes called study nodes. It is an important aspect of the procedure of HAZOP study to divide the process, because how to divide the process determines the scope of the problem to be studied. After the determination of study nodes, the multidisciplinary team starts brainstorming meeting. They examine every part of the process to discover what kind of deviations from the intention of the design can occur and what their causes and consequences may be. This is done systematically by applying suitable guide words [5]. The key elements of the study are:

(1) Intention
(2) Deviation (Using guide words and parameters)
(3) Causes
(4) Consequences (Hazard and operating difficulties)
(5) Recommendations

The procedure for the HAZOP studies is to apply a number of guide words to various parts of the process design intention. These guide words and their meaning are shown in Table 1.

The process parameters which represent the state of the process include flow, temperature, pressure, level, composition, and instrumentation. The deviations for HAZOP studies are defined by the combination of guide words and process parameters. For example,

Guide Word (No) + Parameter (Flow) = Deviation (No Flow)

Some modification is required to implement the process knowledge into the expert system. In general,

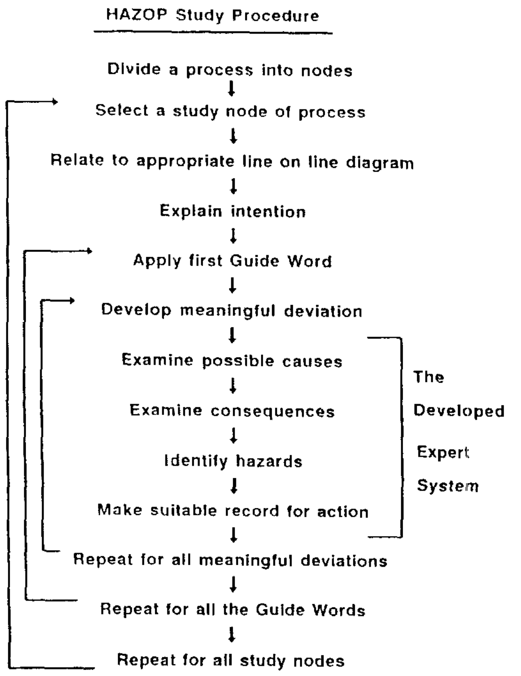

Fig. 1. A typical HAZOP procedure and the covered portion by the developed system.

there is no specific rule to determine a study node, but we divided a process into vessels and transport lines. While we define an equipment such as a storage tank, distillation column, or reactor as *vessel,* and pipe, tube as *transport line*. Other equipments such as a pump, a valve, a control instrument, a heat exchanger are put into either group as adjunct equipments.

The guide words or parameters are not treated separately for the developed system because they are not used for the application by themselves. We have considered only the specific deviations, and these deviations are given as the input data for the expert system. The causes of equipment failures are classified into the equipment knowledge base by these deviation.

An advantageous point of HAZOP is that it provides a more complete identification of the potential hazards, including information on how hazards can develop as a result of operating procedures and operational upsets in the process. HAZOP is completed by a repetitious work and requires considerable manpower and time. But these disadvantages can be overcome by the expert system approach which can represent heuristics efficiently. Moreover, utilizing past experiences is an important principle of hazard identification. This is one of the motivation for developing the expert system. To build a knowledge of the developed system, we referred some standards and codes. Fig. 1 shows the typical HAZOP procedure and the portion covered by the developed system.

PROCESS KNOWLEDGE CLASSIFICATION

The classification of knowledge determines the structure of knowledge base of an expert system. Some criteria are required to classify the process knowledge and the process knowledge for HAZOP study is classified according to deviations, causes and consequences in the developed system. Deviations are predefined with guide words and process parameters. Causes and consequences are the main part of HAZOP. The causes are represented in the form of frame structure and the consequences are in the form of rule networks.

An accident is defined as a specific unplanned sequence of events that has an undesirable consequence. This first event of the sequence is the initiating event. Generally, the initiating event is not the only event for the consequence; usually there are one or more events between the initiating event and the consequence. These intermediate events are the responses of the system and their operators to the initiating event. Different responses to same initiating events will often lead to different accident consequences. Even when the consequences are of the same type, they will usually differ in magnitude. As well as initiating events, intermediate events (system and operator responses) and consequences are the components of accidents.

An event unit is defined with a cause and its consequence. The series of event units represent an accident that proceeds from initiating event to final consequence of the accident.

Event unit 1 : cause 1→consequence 1
Event unit 2 : cause 2→consequence 2
An accident : cause 1→consequence 1 (=cause 2)
→consequence 2

Initiating events are represented as the causes of accidents, and accidents are as the final consequences of a scenarios. But intermediate events are represented as causes or consequences and are linked to initial and final consequences of a accidents through rule networks.

1. Causes

Typical causes of the process failure are equipment failure, improper design, misoperation, and external events. Most of typical causes belong to equipment failure and misoperation those are human errors. Improper design is critical, and hazard identification methods provide design engineers with the chances to find out their faults. The external events such as flood, airplane clash and earthquakes also can be causes of the failure but are excluded because they are considered only in the place where those accidents are frequent. The part of causes that are implemented in the developed system is as follow:

1-1. Heat Exchanger

Cold/hot side blocking, Cooling/heating medium loss, Fouling, Insulation loss, Relief valve opening, etc.

1-2. Control Valve

Mechanical failure, Power failure, Sensor failure, etc.

1-3. Valve

Actuator failure, Leakage, Mechanical failure, Power failure, Seal failure, etc.

1-4. Pump

Discharge valve closing, High viscosity of liquid, Large impeller than the capacity, Leakage, Lubrication loss, NPSH (net positive suction head) loss, Overspeed, Power failure, Seal failure, Shaft break, Stop failure, Suction line plugging, Suction valve closing, Underspeed, etc.

1-5. Pipe

Corrosion, Downstream rupture, High pressure difference, High pressure at down stream, Leakage, Plugging, Rupture, No supply from upstream

1-6. Tank

Agitator failure, Circulation failure, Improper rupture disk, Cooling/Heating system failure, Inerting system failure, Overfilling, Relief valve failure, Seal failure, etc.

1-7. Column

Cooling/heating loss, Discharge valve wide open, Dicharge valve blocking, No feed from upstream, Packing loss, Reflux loss, Relief valve failure, Tray blocking, etc.

2. Consequences

The major hazards with which the chemical industry is concerned are fire, explosion and toxic release. Of these three, fire is the most common and the fatalities are dependent on the fire type - gas, liquid, and solid fire. Gas fire has a fatal effect. Explosions are particularly significant in terms of fatalities and loss and classified into unconfined vapor cloud explosion (UVCE), confined vapor explosion, dust explosion, and boiling liquid expanding vapor explosion (BLEVE). Toxic release has perhaps the greatest potential to kill a large number of people, but large-scale toxic gas fatalities hardly occur.

Common consequences to be examined are personal injury, property damage, and environmental impacts. Toxic material, hot temperature or pressure are typical consequences to be examined. Equipment damages cause serious damage to property and productivity. The classification of consequences for implementations are as follow :

2-1. Heat Exchanger

Stream contamination, Side reaction, Pressure buildup, Cold/Hot side failure

2-2. Control Valve

Pipe blocking, Valve wide open, Controller malfunction, Pressure buildup

2-3. Pump

Equipment damage, Equipment trip, Overheat, High pressure, Material release, Backpressure, Excessive flow, Vacuum, Evaporation, Cavitation, Motor damage

2-4. Pipe

No transfer, Excessive flow, Pipe rupture, Pipe blocking, Material loss

2-5. Tank

High pressure, Leakage

2-6. Column

No transfer, Cold side failure, Discharge valve wide open, Discharge valve blocking, Leakage, Pressure buildup

3. Recommendations

A HAZOP study often results in the generation of two basic types of recommendations; Information needs and action items. Action items are the results of the hazard identification to be reflected in redesign and/or modification of operation procedures. Action items are used when a need for improvement should be considered, for example :

- Consider additional safeguards (safety system, alarms, emergency control)
- Provide missing safeguards
- Consider need for addtional/alternative controls, alarms, instrumentation, etc.
- Modify design, equipment, or procedures
- Improve reliability of equipment or utilities
- Increase capacity of services/utilities

Information needs are used when an additional information is needed to determine if a potential hazard exists, for example :

- Verify design intent
- Confirm actual installation of equipment
- Obtain missing information

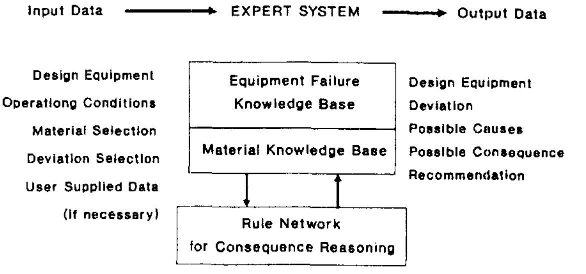

Fig. 2. The input and output data of the expert system.

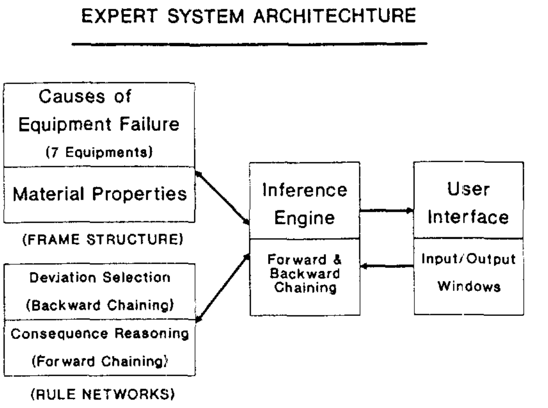

Fig. 3. System architecture.

- Evaluate need for equipment, procedural step, instrumentation, etc.

PROCESS KNOWLEDGE REPRESENTATION

The process knowledge domain for HAZOP studies is wide and most of the knowledge exist in the form of checklists for equipment. To implement the knowledge with modularity, we adopted a frame-based structure as well as rule networks. The frames represent the knowledge to be referred to by the rules. Hierarchical relationships between classes and objects can give rule networks greater flexibility. The input required and the output produced are described in Fig. 2 and the internal architecture of the system is shown in Fig. 3.

The system has two kinds of frames. One is the frame representing knowledge about the process equipment and the other, process materials. The seven types of equipments which are currently available on the expert system are heat exchanger, control valve, pipe, pump, valve, tank, and column. The equipment frame has the knowledge about the causes of

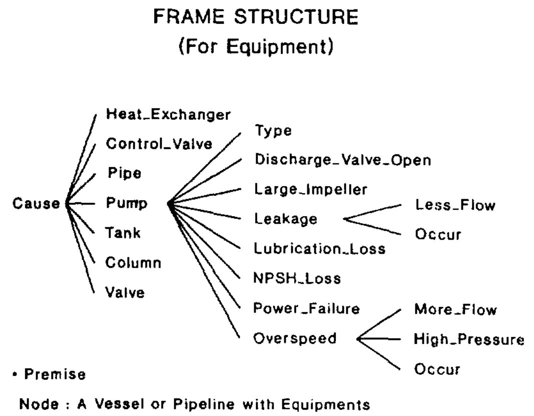

Fig. 4. Frame structure for process equipments.

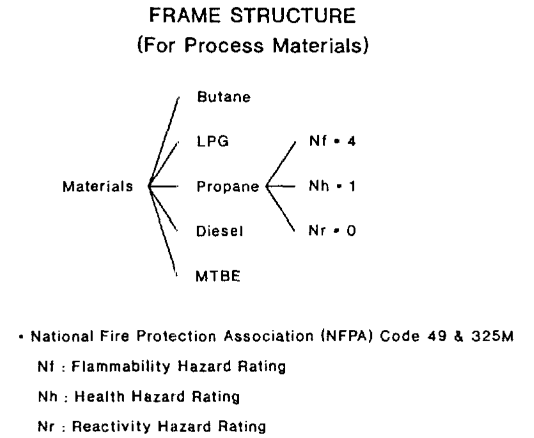

Fig. 5. Frame structure for process materials.

equipment failures. The frame is composed of classes, objects, and slots. Each equipment is represented as a class. The causes of an equipment failure are represented as objects which belong to classes and the objects have deviations as slots which belong to the objects. The frame structure for process equipment is as follows :

```
                ┌─Cause 1           ┌─Deviation 1
                │ (Object 1)        │ (Slot 2)
Equipments ─────┼─Cause 2  ─────────┼─Deviation 2
(Class)         │ (Object 2)        │ (Slot 3)
                └─Specific Type     └─Occurrence
                  (Slot 1)            (Slot 4)
```

As shown in the frame structure above, every piece of equipment has its own slot which represents the type of equipment or its own attributes. For example, the pump class has the slot which describes the pump type-cetrifugal or reciprocating. And each object has the slot representing the occurrence of the event, which means that the rules relevant to the causes are to be triggered. The partial form of the implemented structure for process equipment is represented in Fig. 4.

The frame for process materials has the indices of the material properties which represent health (Nh), flammability (Nf) and reactivity (Nr) hazard rating according to National Fire Protection Association (NFPA) 325 M code. Each index has five degrees ranging from 0 to 4. The higher degree represents more dangerous situation. These material data are used in rules to reason the expected effect from the causes. Every material class has slots for the indices. The frame structure for process materials is shown in Fig. 5.

The rules describe heuristics for inferences while the frames have equipment knowledge. The rules are used for reasoning consequences with causes of failures and user-supplied data for this system. The rules consist of the knowledge structure which is referred to by backward or forward chaining along the reasoning mechanism. The format of a rule is as follows :

IF All Conditions are met (AND Gate among Conditions)

THEN HYPOTHESIS becomes true (OR Gate among HYPOTHESES)

DO Actions are executed.

The rules implemented in the system are classified into two types. One of them is to activate the inference engine from the given deviation by backward chaining. The other is to verify the related consequences using the data from equipment and material frames by forward chaining. By forward chaining mechanism, the rules can trigger the activation or the evaluation of other rules.

The hierarchical rule structure for consequence reasoning is as follows :

```
      Rule 1
      Condition 1┐
AND   Condition 2┼HPT 1┐    Rule 3
      Action 1   ┘     │
      Rule 2       OR  ├─HPT 3          ┐
      Condition 3┐     │  Condition 4 ──┼─HPT 4
      Action 2   ┼HPT 2┘  Action 4      ┘
AND   Action 3   ┘
```

*HPT : Hypothesis

With the hierarchical rule structure, this system can

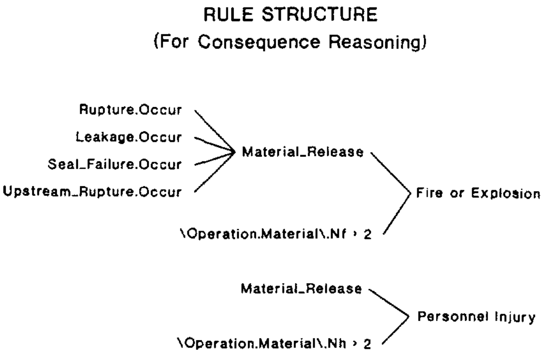

Fig. 6. Rule structure.

provide partial scenarios for hazardous events propagation, which are required at the stage of risk assessment. The partial form of the rule structure is shown in Fig. 6.

The inference starts with the user's deviation selection. And then this system proceeds with questions about basic information for design intention such as design equipment and some operation conditions. Then rules are used for consequence reasoning of the cause of the design equipment. These rules become an important part of this system with frame-based structure. The frame and rule networks make this system expanded to more practical one with flexibility and modularity. This system has been developed on SUN4 SPARCstation with an expert system development shell, NEXPERT OBJECT. The developed system is operated in interactive mode.

EXAMPLES

For a case study, we applied the expert system to the LPG storage and fractionation process. The diagram for the process is shown in Fig. 7. We divided the process into three study nodes-the storage tank, the column, and the transport lines between them. A transport line from LPG storage to fractionation column was studied as an example. This transport line was selected as a study node for the example. This study node has some components - the valve, the pump, the control valve, and the heat exchanger. For the complete study of this node with this expert system, it is necessary to repeatedly apply all the deviations to these components. That example shows the case

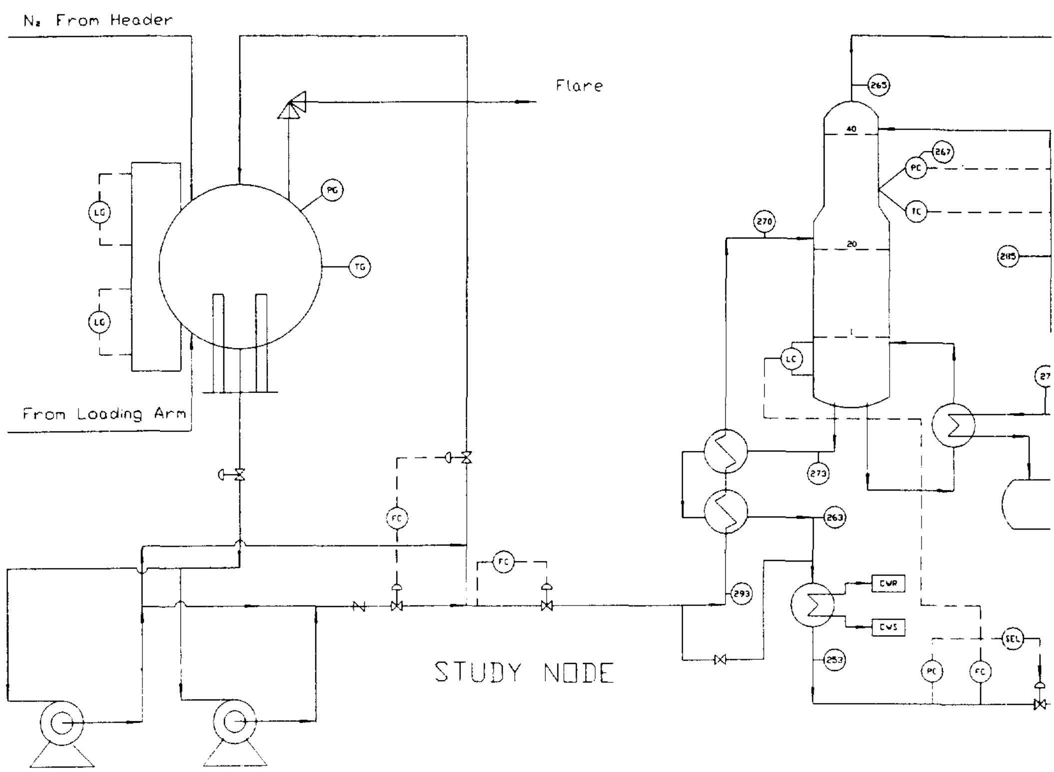

Fig. 7. Process diagram for the example.

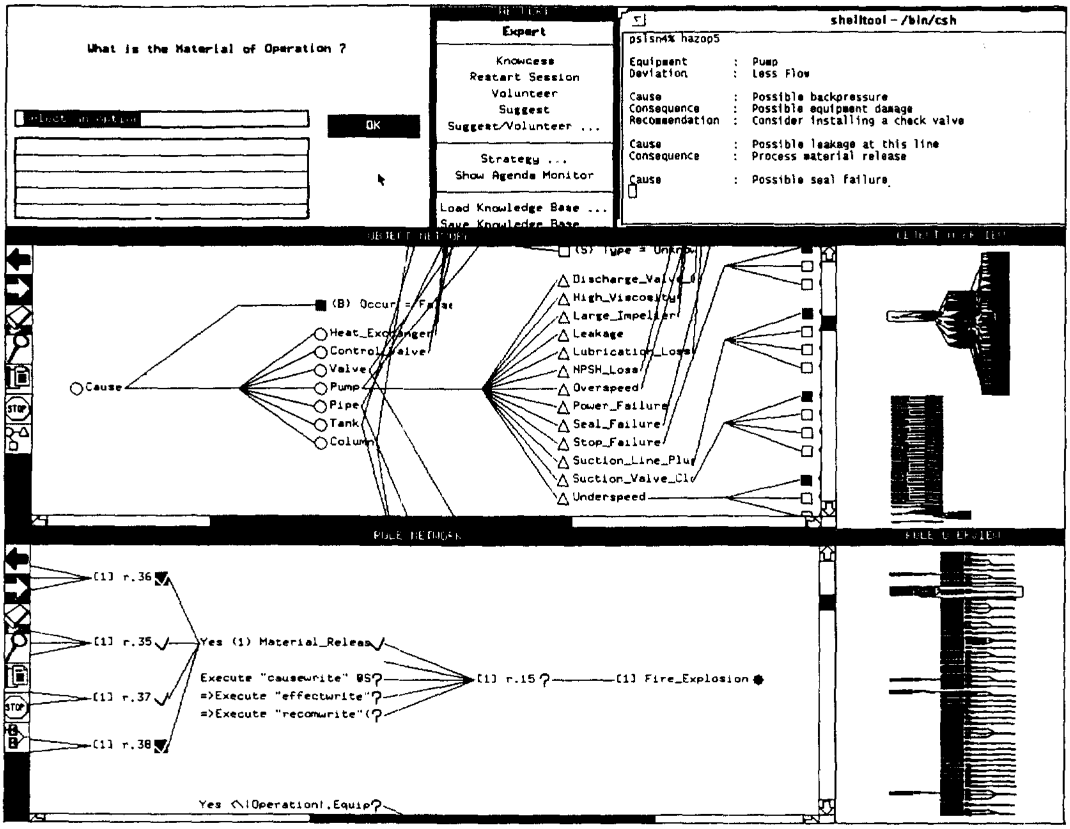

Fig. 8. System development environment.

in which we have applied this expert system to the pump with a deviation of "Less Flow" for that study node.

One step of the system operation for the example is illustrated in Fig. 8. The input and output windows are shown in the topside of the screen, the frame-based structure in the middle and the rule networks in the bottom. For run-time mode, only an input (left above) and an output (right above) window are needed. The result for this example is summarized in Fig. 9. Fig. 8 is the third step of the example as described in Fig. 9. In Fig. 9, the "→" mark is used to represent the question in the input window and other messages are the results shown in the output window.

The recommendations made in this system including this example can be classified into hardware and software solution. The hardware solution is to install some equipment or to modify the design. The software solution is, for example, to ensure training operator, or to modify the maintenance program.

No recommendation is shown at the second and third results in Fig. 9, because the reasoning has not finished for that consequence. While reasoning the rule relevant to leakage or seal failure, this system requires the answer for which process material would be treated. Then it asks the operation pressure and the type of pump for further reasoning. The rule checks the flammability index (Nf) after the third question. The consequences are the results obtained by reasoning the rule networks with knowledge base and user-supplied information.

This case study was performed by only one process engineer using the developed system and took only half an hour to cover one study node. Although the result is not a completed one, it will take about 10 or more man-hour without aid of the computer-aided system. The saved manpower is expected to be very useful for more thorough analysis and increasing the safety of the process.

CONCLUSIONS AND FURTHER STUDIES

The developed system shows that the approach of a knowledge-based expert system is quite efficient and

```
-> Select Deviation     : Less Flow
-> Select Equipment     : Pump

C  : Possible excessive backpressure
E  : Possible equipment damage
R  : Consider installing a check valve

C  : Possible seal failure
E  : Process material release

C  : Possible leakage
E  : Process material release

-> What is the Material of Operation ? : LPG

C  : Flammable material release
E  : Possible fire with ignition source
R  : Consider installing a release detector

-> What is the Pressure of Operation?: 10atm

C  : Material leakage with high pressure
E  : Possible personnel injury
R  : Check the pressure relief equipment

-> What is the Type of Pump? : Centrifugal

   C : Underspeed of this equipment
   E : Less transfer of this equipment
   R : Check safeguard at this equipment

   C : Lubrication loss
   E : Possible equipment damage
   R : Check safeguard at this equipment

   C : Possible suction line plugging
   E : Possible caviation
   R : Check the suction pressure

   C : Loss of net positive suction head
   E : Possible cavitation
   R : Consider installing a vertical type

 * C:Cause     E:Consequence     R:Recommendation
```

Fig. 9. The Result for the case study.

time-saving for HAZOP studies for chemical processes. The system can be used not only for industrial purposes but also for educational ones.

The system represents the knowledge by frames and rules. The frame-based structure was adopted for process equipment/process material and the rule networks for reasoning consequence. The rule uses forward chaining for consequence reasoning and backward chaining for inference start of inferencing. The frame and rule networks have the hierarchical structure.

The expert system substantiates the efficiency and reliability for HAZOP study. To be more specific, the system is flexible and modular enough to expand its knowledge base by including checklists and design experience. More than 50% of the requested manpower for HAZOP studies could be reduced with the developed system. And the results of the system provide safety engineers with scenarios for hazardous events to perform risk assessment. Further studies are needed to include capability to accept the topologies of complex chemical plants and to include layout and startup/shutdown procedure.

REFERENCES

1. American Institute of Chemical Engineers-Center for Chemical Process Safety : "Guidelines for Hazard Evaluation Procedure", AIChE (1985).
2. Chemical Industries Association : "A Guide to Hazard and Operability Studies", London (1990).
3. American Institute of Chemical Engineers : "Dow's Fire and Explosion Index Hazard Classification Guide", 6th ed. AIChE (1987).
4. Crowl, D. A. and Louvar, J. F.: "Chemical Process Safety : Fundamentals with Application", Prentice-Hall (1990).
5. Lee, F. P.: "Loss Prevention in the Process Industries", Butterwords (1980).
6. Weatherill, T. and Camron, I. T.: *Computers and Chemical Engineering*, **13**, 1229 (1989).
7. Benuzzi, A. and Zaldivar, J. M.: "Safety of Chemical Batch Reactors and Storage Tanks", Kluwer Academic Publishers (1991).
8. Himmelblau, D. M.: "Fault Detection and Diagnosis in Chemical and Petrochemical Processes", Elsevier Science Publishing Company (1978).
9. Hushon, J. M.: "Expert Systems for Environmental Applications", American Chemical Society (1990).
10. Kletz, T. A.: *Chemical Engineering*, **Apr.**, 48 (1985).
11. Lieberman, N. P.: "Troubleshooting Refinery Process", PennWell Books (1981).
12. Martine, J. and Oxman, S.: "Building Expert Systems : A Tutorial", Prentice-Hall (1988).
13. National Fire Protection Association : "NFPA Code 325M : Fire Hazard Properties of Flammable Liquids, Gases, and Volatile Solids", National Fire

Protection Association (1991).
14. National Fire Protection Association : "NFPA Code 49 : Hazardous Chemical Data", National Fire Protection Association (1991).
15. Rolston, D. W.: "Principles of Artificial Intelligence and Expert Systems Development", McGraw-Hill (1988).