AUTOMATION OF QUANTITATIVE SAFETY EVALUATION IN CHEMICAL PROCESSES

Byungwoo Lee

Department of Chemical Engineering, Seoul National University, Seoul 151-742, Korea

Byounggwan Kang

Department of Chemical Engineering, Seoul National University, Seoul 151-742, Korea

Jung Chul Suh

Department of Chemistry, Korea Air Force Academy, Korea

En Sup Yoon

Department of Chemical Engineering, Seoul National University, Seoul 151-742, Korea

ABSTRACT

A method to automate hazard analysis of chemical plants is proposed in this paper. The proposed system is composed of three knowledge bases — unit knowledge base, organizational knowledge base and material knowledge base, and three hazard analysis algorithms — deviation, malfunction and accident analysis algorithm. Hazard analysis inference procedure is developed based on the actual hazard analysis procedures and accident development sequence. The proposed algorithm can perform hazard analysis in two methods and represent all conceivable types of accidents using accident analysis algorithm. In addition, it provides intermediate steps in the accident propagation, and enables the analysis result to give a useful information to hazard assessment. The proposed method is successfully demonstrated by being applied to diammonium phosphate manufacturing process. A system to automate hazard analysis is developed by using the suggested method. The developed system is expected to be useful in finding the propagation path of a fault or the cause of a malfunction as it is capable to approach causes of faults and malfunctions simultaneously.

INTRODUCTION

Hazard analysis is one of the basic tasks to ensure the safety of chemical plants. However, it is an arduous, tedious, and time-consuming work, requires multidisciplinary knowledge, and demands considerable cognitive load from the analysts. To solve these problems, there have been many attempts to automate hazard analysis by using computer technology, especially by using the knowledge-based techniques [1,3,4,6,12,13]. However, many of the past approaches to automated hazard analysis lack some or all of the following desired properties.

① Consideration of safeguards

For the hazard analysis to be useful, it is important to consider the existing safeguards, to verify their effectiveness, and to identify hazards which are not covered by safeguards; these are the very purpose of performing the hazard analysis.

② Diverse accidents

Generally, hazards can be classified into physical hazards and chemical hazards. However, the existing system can only deal with a limited number of them — usually those of physical hazards.

③ Diverse causes and consequences

A malfunction of a single unit may affect the whole plant through stream integration.

④ Pathway or event combination to accidents

An accident may be regarded as a sequence of events. To manage potential accidents in chemical process effectively, the pathway from ultimate malfunction (or initiating event) to the actual accident should be identified.

The previous approaches have drawbacks mentioned above due to the limitations in capturing and utilizing all the available information; the necessary information does not take a specific form. Therefore, it is most important to make an appropriate knowledge representation scheme which meets the demand of the development of expert system.

Recently, Suh[10] proposed a new methodology for automated hazard analysis of chemical plants. In this approach, the information required for hazard analysis is identified through the accident mechanism, and as accidents have their own distinctive features, it is irrational to deal with such information in a single knowledge domain. Therefore, these types of information are represented in four different sub-domains: function, behavior, structure, and material property.

CHEMICAL PROCESS MODELING FOR HAZARD ANALYSIS

The following six types of information are needed for the modeling of an accident mechanism.

① Hierarchical structure between ultimate malfunction and immediate malfunction in a unit.

② Relationship between variable deviation and malfunction.

③ Causal relation among variables of a process unit.

④ Spatial arrangement of units (process topology).

⑤ Relationship among malfunction, deviation and accident.

⑥ Function of safety unit and control system, and their connective relation with process units.

First, second and third types of information (①, ②, ③) is modeled for each basic unit, and information about ④ is obtained from the drawings such as P&ID(Piping & Instrument Diagram) and PFD(process flow diagram). ⑤ is organized by the reasoning algorithm which infers the actual accident from the physical and chemical state of process. ⑥ is presented through the model which represents ④, and by analyzing the function of safety unit and control system in accident mechanism.

Unit knowledge base is devised to model a process unit. This model represents physical hazards corresponding to the information ①,②, and ③. It consists of unit behavior model and unit function model. Function model contains the knowledge of ① and ②, and behavior model represents the knowledge of ③. In unit knowledge base, a process unit is modeled in different terms of variables and functions. Variables describing unit are divided into inlet, internal, and outlet variables explicitly. By interconnecting the behavior model and the function model through these variables, the complicated details can be obtained in this approach, which has been difficult to obtain in the other models.

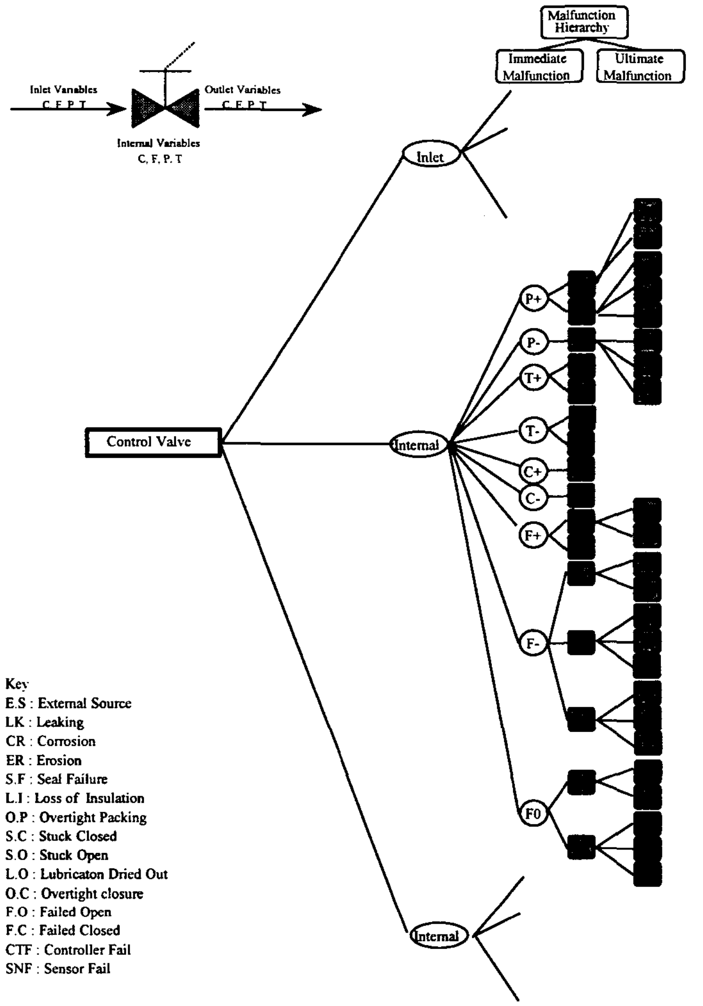

Fig. 1. Unit Function Model of a Control Valve

In unit function model, malfunction hierarchy from ultimate malfunction to immediate malfunction is constructed and it can represent malfunction in various ways. Fig. 1 shows an example of unit function model of a control valve.

A chemical process is composed of basic units, and, through the connection of these basic units, the variable deviation of one unit influences the variables of the adjacent unit. Because of these interactions, the spatial arrangement of units, which is connective relation, must be known in order to reason about cause and effect of malfunction or deviation throughout the whole system. Organizational knowledge base has the knowledge about this. In order to represent the connective relations among the units efficiently, process streams in a plant are decomposed according to their functions, and then process structure is restructured. The purpose of this stream decomposition is to organize the process structure into an efficient form for hazard analysis.

Hazard analysis reasoning operates on this modified process structure. In addition, safeguards are classified according to their functions and are included in organizational knowledge base.

Safeguards are those equipped to ensure the safety of process, which include indicator, alarm, interlock system, rupture disk, etc. They work only under special circumstances, and are ignored in other fields (e.g., fault diagnosis, dynamic simulation, control, etc.). However, in view of safety, safeguards can function in accident mechanism; these safeguards must be taken into account for the reliable safety analysis. However, the most recent approaches do not deal with safeguards. The structure of their models could not accommodate safeguard, and their main objective was to identify hazard by analyzing process units only. In this model, safeguards are included in modeling and are treated in organizational knowledge base.

One of the main reasons why the safety of chemical processes should be given much attention is that chemical plants deal with hazardous materials. In order to take these into consideration in the course of analysis, the knowledge base has to contain underlying information about those properties. Such properties have already been defined by several standards or codes such as Dow fire index, NFPA code, each of which covers various kinds of chemical substances[5,8,9,11]. The proper use of these standards or codes could save a lot of effort in finding out chemical hazards. In this paper, NFPA(National Fire Protection Association) code is adopted. Material knowledge base consists of hazard indices and reaction matrix. Hazard indices represent flammability hazard rating(Nf), health hazard rating(Nh), and reactivity hazard rating(Nr) according to NFPA code. Each index has five ratings from 0 to 4. The higher degree represents more dangerous situation. The detailed meaning of ratings is described in NFPA code[8]. In addition, there is a possibility that unexpected reaction could occur in chemical plants, and therefore considerable knowledge of chemistry and of reaction kinetics is required to recognize these reactions. Reaction matrix is introduced to simplify this work. Reaction matrix presented here is a variant of basic reaction matrix[11]. It augments the basic reaction matrix by including fault situations which may occur in reactor. This matrix has rows and columns labeled with the various types of materials which are present in plants and each element of the matrix represents the potential reaction phenomenon for each material pair. Especially with regard to reactants in reactor, the matrix element represents the cases that each reactant exists excessively in the reactor. Through material knowledge base, the approach proposed in this study can treat various chemical hazards including unwanted reactions which other systems cannot deal with.

HAZARD ANALYSIS REASONING

The developed system has the following three hazard analysis algorithms;

① Deviation analysis algorithm

② Malfunction analysis algorithm

③ Accident analysis algorithm

A user selects either deviation analysis algorithm or malfunction analysis algorithm. If the user selects deviation analysis algorithm, reasoning begins with variable deviation of the unit given by the user; in case of malfunction analysis algorithm, reasoning begins with malfunction inputted by user. If these two reasoning algorithms are applied to the same process, and, as the two results complement each other, the quality of hazard analysis can be enhanced. As a result of deviation analysis or malfunction analysis, all the states of inlet, internal and outlet variables and malfunctions in every process unit are identified. These verified states are stored in the corresponding slots of organizational knowledge base, and then accident analysis algorithm is called. Accident analysis algorithm discovers all the actual accidents from the physical state of units and material knowledge base. Accident analysis algorithm can represent every conceivable type of accident. Three typical accident types are as follow;

① The situation associated with malfunction and material property

② The situation associated with variable deviation and material property

③ The situation associated with variable deviation and characteristic of the unit

Accident analysis algorithm can infer various types of accidents by incorporating malfunction, deviation, unit characteristics, and material property of process. For example, if a case of deviation: Level High in Tank is determined by deviation analysis algorithm, accident analysis algorithm will lead to the following two different inferences by identifying unit characteristics;

Inference 1: Level (High deviation) + Open Tank (process unit characteristic) → Overflow

Inference 2: Level High (deviation) + Closed Tank (process unit characteristic) → High Pressure Buildup

In case of Inference 1, the process material property is retrieved from material knowledge base, and the inference can be continued further, leading to the following result.

Inference 3: Level High (deviation) + Open Tank (process unit characteristic) → Overflow + Toxic material ($Nh > 2$) → Toxic material release

In addition, human factors are considered and, finally, the following accident is predicted.

Inference 4: Level High (deviation) + Open Tank (process unit characteristic) → Overflow + Toxic material ($Nh > 2$) → Toxic material release + Human → Personnel injury due to toxic material

This kind of knowledge is represented in the form of rule in accident analysis algorithm(Fig. 2).

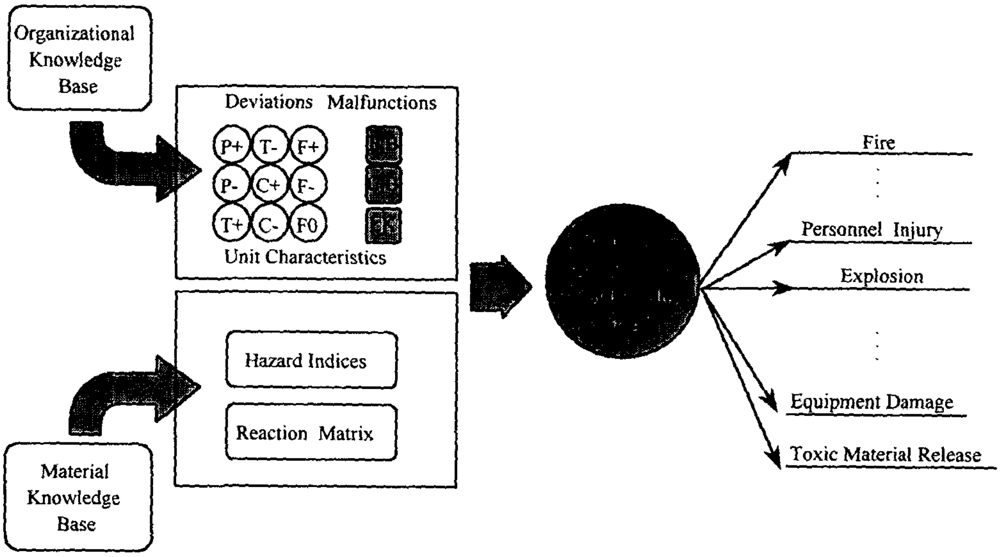

Fig. 2. Accident Analysis Algorithm

Next, to find out whether there exist safeguards for identified accidents, the information about the arrangement of the safety units is gained from the organizational knowledge base. There are two kinds of safeguards for malfunction, deviation and accident: preventive safeguard and mitigative safeguard.

The overall procedure of deviation analysis algorithm is outlined in Figure 3. Deviation analysis results are composed of root malfunction, given deviation, cause deviation, cause malfunction, effect deviation, accidents and safeguards. Meanwhile, malfunction analysis results are composed of given malfunction, effect deviation, accidents, and safeguards. Fig. 4 is the inference procedure of the malfunction analysis algorithm.

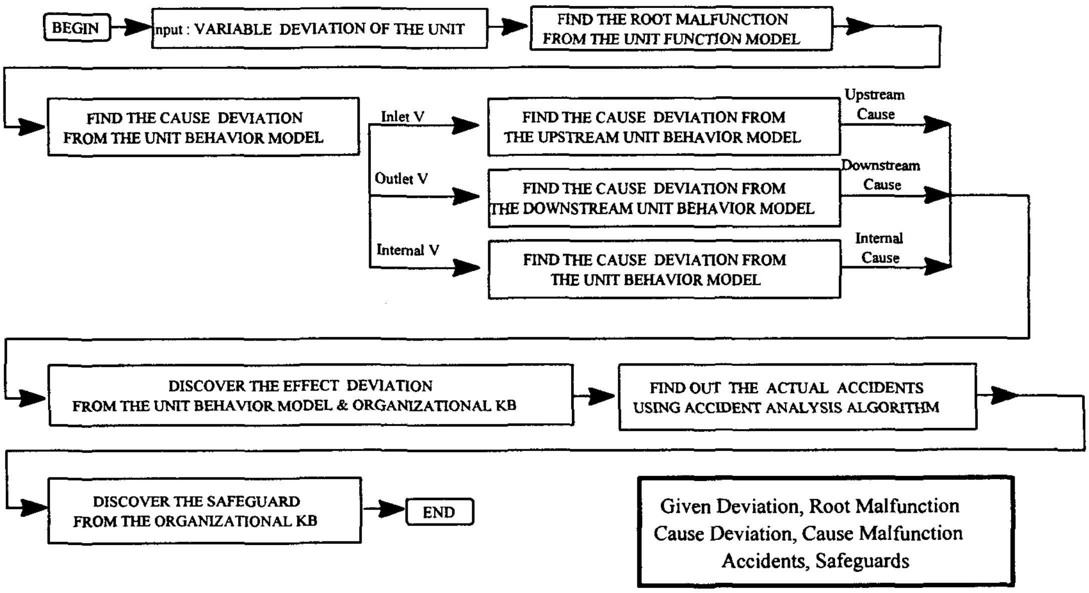
BEGIN
nput : VARIABLE DEVIATION OF THE UNIT
FIND THE ROOT MALFUNCTION FROM THE UNIT FUNCTION MODEL
FIND THE CAUSE DEVIATION FROM THE UNIT BEHAVIOR MODEL
Inlet V
Outlet V
Internal V
FIND THE CAUSE DEVIATION FROM THE UPSTREAM UNIT BEHAVIOR MODEL
FIND THE CAUSE DEVIATION FROM THE DOWNSTREAM UNIT BEHAVIOR MODEL
FIND THE CAUSE DEVIATION FROM THE UNIT BEHAVIOR MODEL
Upstream Cause
Downstream Cause
Internal Cause
DISCOVER THE EFFECT DEVIATION FROM THE UNIT BEHAVIOR MODEL & ORGANIZATIONAL KB
FIND OUT THE ACTUAL ACCIDENTS USING ACCIDENT ANALYSIS ALGORITHM
DISCOVER THE SAFEGUARD FROM THE ORGANIZATIONAL KB
END
Given Deviation, Root Malfunction
Cause Deviation, Cause Malfunction
Accidents, Safeguards

Fig. 3. Inference Procedure of Deviation Analysis

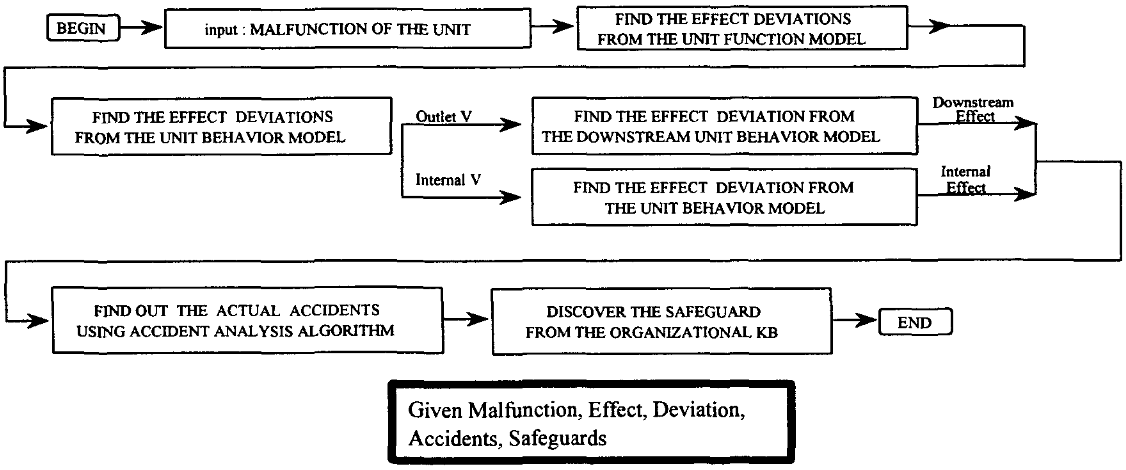
BEGIN
input : MALFUNCTION OF THE UNIT
FIND THE EFFECT DEVIATIONS FROM THE UNIT FUNCTION MODEL
FIND THE EFFECT DEVIATIONS FROM THE UNIT BEHAVIOR MODEL
Outlet V
Internal V
FIND THE EFFECT DEVIATION FROM THE DOWNSTREAM UNIT BEHAVIOR MODEL
FIND THE EFFECT DEVIATION FROM THE UNIT BEHAVIOR MODEL
Downstream Effect
Internal Effect
FIND OUT THE ACTUAL ACCIDENTS USING ACCIDENT ANALYSIS ALGORITHM
DISCOVER THE SAFEGUARD FROM THE ORGANIZATIONAL KB
END
Given Malfunction, Effect, Deviation,
Accidents, Safeguards

Fig. 4. Inference Procedure of Malfunction Analysis

Fig. 3 and Fig. 4 show the distinctive difference between two algorithms. Deviation analysis algorithm determines physical state of units by performing backward reasoning to find causes by starting from intermediate event of accident developing sequence and forward reasoning to identify effects. Malfunction analysis infers from malfunction of a unit, that is the initial event of accident. By forward reasoning only, it infers the propagation effect and defines the state of affected units.

FAULT TREE SYNTHESIS ALGORITHM

The following is the algorithm to synthesize fault tree automatically based on the proposed knowledge representation scheme.

The top event of a fault tree is an accident. If the user supplies the possible accident for a given process, the inference starts by the suggested algorithm. Once the top event is determined, primal causes which may cause the given accident are found by backward search. These causes are variable deviations or equipment malfunctions, and are found by using accident knowledge base. If a variable deviation is the cause, then the malfunction or other variable deviation which causes this variable deviation is searched. Firstly, a root malfunction which causes the given variable deviation is found in the unit function model of the corresponding equipment; this root malfunction may not exist or may be more than one. Then other variable deviation which may cause the studied variable deviation is found in the unit behavior model. Once the cause deviation is found, then the cause malfunction which causes the detected cause deviation is searched for. This cause malfunction may be a 1st level or the lower level malfunction in the unit behavior model; if it is not an ultimate malfunction, then the ultimate malfunctions are searched for in the unit behavior model. This procedure is shown in Fig. 5.

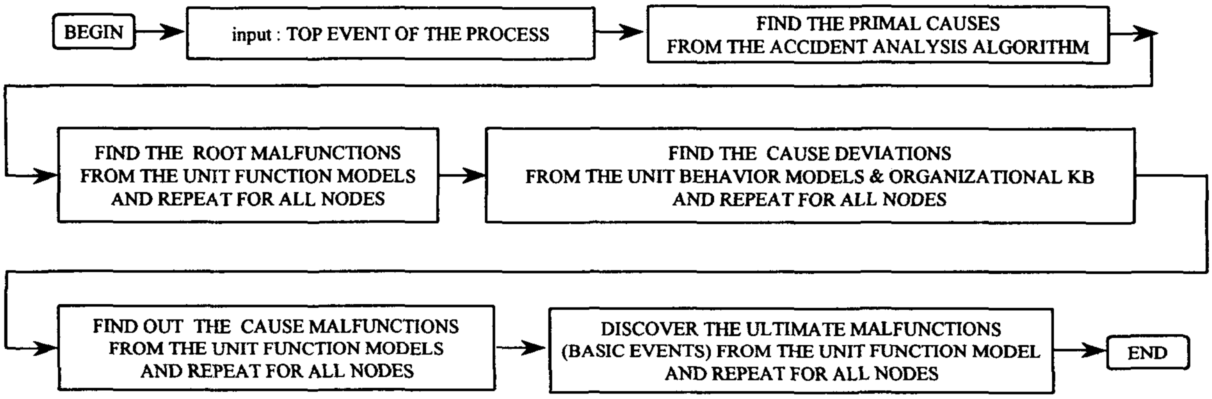
BEGIN
input : TOP EVENT OF THE PROCESS
FIND THE PRIMAL CAUSES FROM THE ACCIDENT ANALYSIS ALGORITHM
FIND THE ROOT MALFUNCTIONS FROM THE UNIT FUNCTION MODELS AND REPEAT FOR ALL NODES
FIND THE CAUSE DEVIATIONS FROM THE UNIT BEHAVIOR MODELS & ORGANIZATIONAL KB AND REPEAT FOR ALL NODES
FIND OUT THE CAUSE MALFUNCTIONS FROM THE UNIT FUNCTION MODELS AND REPEAT FOR ALL NODES
DISCOVER THE ULTIMATE MALFUNCTIONS (BASIC EVENTS) FROM THE UNIT FUNCTION MODEL AND REPEAT FOR ALL NODES
END

Fig. 5. Fault Tree Construction Algorithm

CONCLUSIONS

This article has presented a new methodology for automated hazard analysis of chemical plants. The developed system composed of three knowledge bases -- unit knowledge base, organizational knowledge base and material knowledge base and three hazard analysis algorithms -- deviation, malfunction and accident analysis algorithm. A method to utilize the analysis result for fault tree analysis is also suggested. The usefulness of the suggested method is validated by being applied to DAP process. The developed system can perform hazard analysis in view of malfunction and deviation as well. These results can be mutually complemented, and therefore, it can detect the potential accident more exhaustively than other hazard analysis systems that perform identification from only one viewpoint. As a result, the quality of hazard analysis can also be enhanced. Accident analysis algorithm incorporates the physical state of process with material knowledge base, by which all conceivable types of accidents can be represented.

ACKNOWLEDGEMENTS

This work was supported by Science and Technology Policy Institute of Ministry of Science and Technology, Yukong Co., Ltd., and Korea Science and Engineering Foundation(KOSEF) through the Automation Research Center at POSTECH.

REFERENCES

1. Catino, C. A. and Ungar, L. H., Model-Based Approach to Automated Hazard Identification of Chemical Plants, AIChE Journal, **41**(1), 97-109, 1995.
2. Center for Chemical Process Safety(CCPS), Guidelines for Hazard Evaluation Procedures, 2nd Edn, AIChE, New York. 1992.
3. Chae, H., Yoon, Y. H., and Yoon, E. S., Safety Analysis Using an Expert System in Chemical Processes, Korean J. of Chem. Eng., **11**(3), 153-161, 1994.
4. Goring, M.H. and Schecker, H.G., HAZEXPERT - an Integrated Expert System to Support Hazard Analysis in Process Plant Design, ESCAPE-2, S429-S434, 1992.
5. Greenberg, H. R., and Cramer, J. J.(Eds), Risk Assessment and Risk Management for the Chemical Process Industry, Van Nostrand Reinhold, New York, 1991.
6. Heino, P., Heikkil, J., and Koivisto, R., Knowledge Based Safety Management, Computer-Oriented Process Engineering, 259, Elsevier, Amsterdam, 1995.
7. Kang, B., Suh, J. C., and Yoon, E.S., A Multimodel Approach for Automated Hazard Analysis of Chemical Processes, Proc. 2nd Asian Control Conference, Ⅱ-883 - Ⅱ-886, 1997.
8. NFPA, NFPA Code 325M Fire Hazard Properties of Flammable Liquids, Gases, and Volatile Solids, National Fire Protection Association, 1991a.
9. NFPA, NFPA Code 49 Hazardous Chemical Data, National Fire Protection Association. 1991b.
10. Suh, J. C., Lee, S., and Yoon, E. S., New Strategy for Automated Hazard Analysis of Chemical Plants, J. of Loss Prevention, **10**(2), 1997.
11. Suh, J. C., Lee, B., Kang, I. K., and Yoon, E. S., An Expert System for Automated Hazard Analysis based on Multimodel Approach, Computers chem. Engng., **21**(Supple), S917-S922, 1997.
12. Taylor, J. R., Risk Analysis for Process Plant, Pipelines and Transport, E&F N SPON, London, 1994.
13. Vaidhyanathan, R. and Venkatasubramanian, V., Digraph-based models for automated HAZOP Analysis, Reliability Eng. and System Safety, **50**, 33-49, 1995.