A-13

다이그래프를 이용한 자동 결함수 시스템 개발

이근원, 문 일*

*한국산업안전공단, *연세대학교 화공과*

Development of Fault Trees Analysis System Automated using Digraph

Keun-Won Lee, Il Moon*

*Korea Occupational Safety & Health Agency, *Department of Chemical Engineering, Yonsei University*

INTRODUCTION

Fault Tree Analysis(FTA) is based on constructing a hypothetical tree of base events branching into numerous other sub-events, propagating the fault and eventually leading to the top event. The goal of FTA is to evaluate the probability of the occurrence of the top event and show the events that cause the top event to occur and merits of FTA are; 1) The results of FTA is objective due to its statistical analysis, 2) FTA can achieve both quantitative and qualitative safety analysis result of target processes. But manual FTA depends on experts and requires a lot of manpower, cost and time. In addition to this, the result of manual FTA is often unreliable. To resolve these problems, the FTA needs to be automated. The automated FTA can be used as many times as users want and it can analyze a process effectively and conveniently. Lots of researchers therefore, are interested in the automatic FTA. Examples are Fussell's transfer function[1], Salem's Decision table[2], Lapp and Powers's Digraph[3], Camarda's Reliability graph[4], Kelly and Lee's Mini fault tree[5] and Abbasi's PROPAT II[6]. But most of the studies about the FTA automation are concentrated on not the whole procedure of FTA including automatic construction of FT, but only a part of analyzing FT. The aim of this study is to develop an automatic FTA system including the digraph-FT conversion algorithm. The novel FTA system of this study is able to transform a Digraph to a FT and analyzes FTA automatically.

DIGRAPH METHODOLOGY

In order to generate a fault tree automatically, the development of an accurate representation

to generate a fault tree in the system is required at first. This representation must be general so that any type of chemical processes can be analyzed and suited for their computation. Therefore, a digraph is used to meet both of the above needs in this study. The digraph is a set of nodes connected by directed edges. The nodes of digraphs used in fault tree synthesis represent process variables such as temperatures, pressures, and flow rates etc. and certain types of failures including equipment failures and human errors. If a deviation in one variable causes a deviation in a second variable, then a directed edge is drawn from the node representing the first variable to the node representing the second. A number is assigned to the edge as the direction (positive and negative) and the magnitude ("1" and "10"). Loop identification and classification from the system using digraph are very important to build digraph-based fault tree. Loops are classified four types: feedforward loops (FFL-two or more paths from one node to another in a digraph), feedback loops (FBL-a path through the nodes in a digraph that starts and terminates at the same node), positive loops and negative loops.

Further, faults and failures are classified into three types based on the digraph representations and the patterns of their propagation in the system as follows: Type A(*f*) (It is noted that, if both x1 and x2 are on the same PFBL(Positive Feedforward Loop), the values of x2 can be affected not only by f but also by x1 and, in case of NFBL(Negative Feedforward Loop), then x2 is always affected by f alone.), Type B(*f*) (The edge between x1 and x2 can be considered as nonexistent.) and Type C(*f*) (The occurrence of a failure of this type change the direction of the effects of an additional fault propagating from x1 to x2.). Type A(*f*) means that the failure has an effect by not only a normal process variables but the facts composing the process. Type B(*f*) means vanishing of the failure in the facts composing the process. Type C(*f*) means finally that the failure of the facts causing the converse relationship between processes. It increases the efficiency of the automatic FT construction algorithm to make a failure classification simply.

The FT generation rule to transform the information of a digraph to a FT consists of four structures depending on the situation of nodes formation as following: (Structure Ⅰ); when the node is in PFFL,PFBL, or when the node is in NFFL and is not a terminal node, or when the node is not in loop. This is the arrangement of the deviation in input node that has an effect on the target node by connecting to an OR gate. (Structure Ⅱ); when node is a terminal node of NFFL. This is a FT generation rule considering the effect by the start node and also by the non-start nodes(Structure Ⅲ) when the node is in NFBL. This is an FT generation rule considering the ability of Loop to control by itself. Finally (Structure Ⅳ) ; when the node is a terminal node of NFFL and it is in NFBL. In this case, we composed the rule considering the peculiarity of NFBL and NFFL at the same time. Therefore, we made a new FT generation rules through combining Structure Ⅰ and Structure Ⅱ.

AUTOMATIC FTA SYSTEM

The digraph-FT conversion algorithm is developed with the recursive method using the FT

generation rules. On digraph, the algorithm investigates the top event that is chosen at the beginning. According to that process, algorithm can also apply each FT generation rule to compose a FT. We use repeating techniques to compose a FT, which depends on the situation of the node. After these are done, the algorithm recognizes the digraph's next node related to the top event as a new target node on the algorithm, and it applies the FT generation rule following the situation of nodes. If the node considered is a basic event, the composition of the FT is over.

The next step of the FT automation requires the quantitative analysis. This study uses Fussell algorithm that searches minimal cut sets. For the qualitative analysis this study computes the probability of occurrence of the top event with the unavailability for each basic event. The probability data is q(Unavailability), which is presented as the combination of λ (The Failure Rate) and τ (The mean time to repair).

With the FT generated, users can search the minimal cut sets, the ranking of basic event frequency and the gate list. Especially minimal cut sets from FT analysis is the most accurate way to find a basic event that has the most powerful effect on failure of the top event.

The automatic FT conversion algorithm includes the following procedures; 1) user input node data representing process variables and failure data to build the system digraph according to P&ID, 2) names of these node data and failure data are defined by a user, 3) top event is selected, 4) loops in the system digraph are identified and classified, 5) fault and failure types are classified, 6) probability data are calculated, 7) the system digraph is conversed to a fault tree automatically, and 8) the minimal cut sets or the ranking of basic event frequency is represented as user's demand. This procedure is explained schematically in Figure 1.

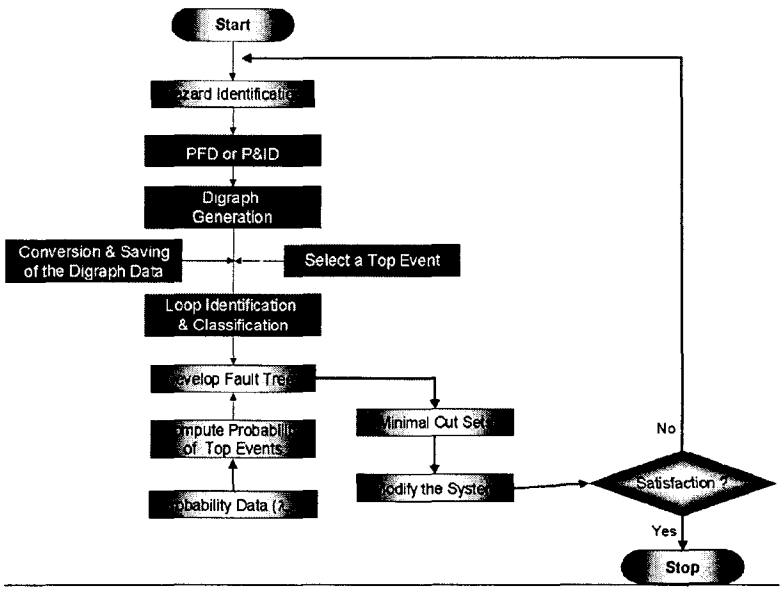

Figure 1. The procedure of the automatic FTA system.

CASE STUDY

A reactor shown in Figure 2 is monitored by two temperature elements (TE) and two pressure transmitters (PT). High system pressure or temperature indicates a possible exothermic reaction in progress. The processor provides a shutdown signal if it receives a high signal from either the TEs or PTs. The reaction pressure and temperature are continuously monitored. The processor is tested once every shift (8hr). If the processor (combination of output card and CPU) is found failed, the reactor is shut down while the processor is repaired.

Figure 3 represents the digraph for the reactor process. To construct the FT for this digraph, the required data are node data (variable on the process diagram), failure data (equipment failure and Human error), probability data (λ , τ) and description data.

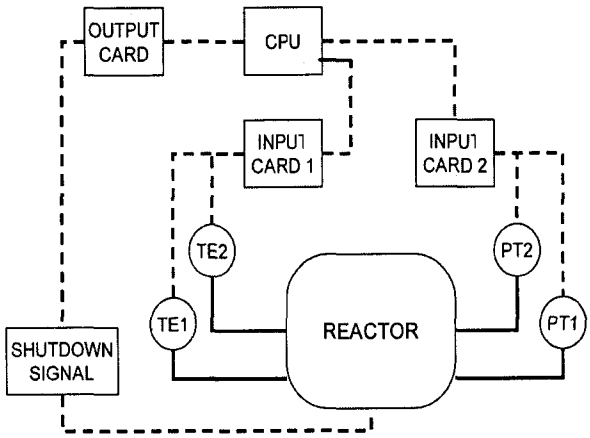

Figure 2. System diagram for the example process.

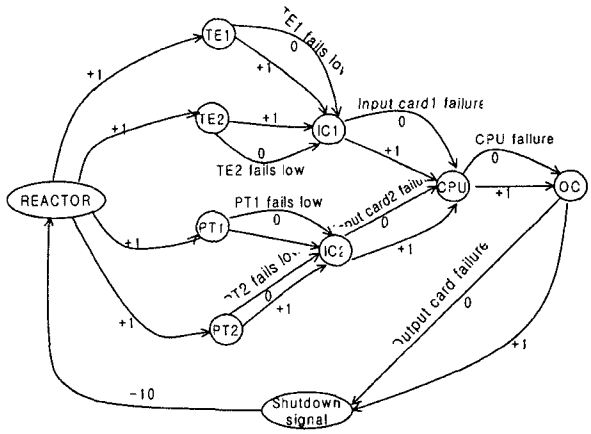

Figure 3. The digraph for example problem.

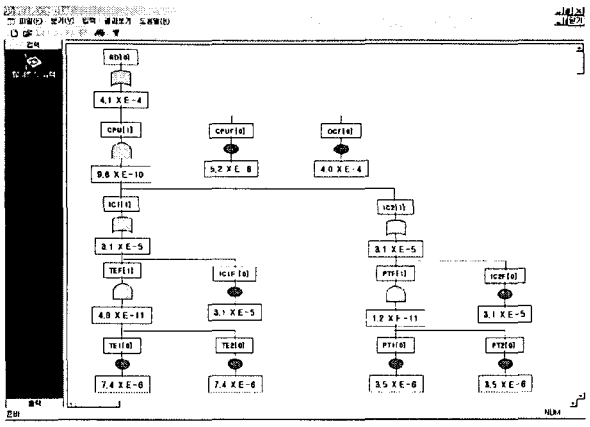

Figure 4. The FT for example problem.

A huge explosion is possible if the shut down signal is not sent to the reactor because of high pressure and temperature. If the top event is selected as the shut down signal, the FT generated from the FTA system is shown in Figure 4.

CONCLUSION

This study developed a novel FTA System automated using the FT automatic construction algorithm and the automatic FT analysis algorithm. The FTA system improves the defeat of manual FTA and can get a minimal cut sets and the probability of the occurrence of the top event with less time and cost. This system could overcome the technical problems even with a little information like PFD or P&ID and accomplish FTA simply. This system could also get over objectivity problems of FTA results possibly happened due to user's logical problem or subjective experience because it composes and analyzes FT with regular rules. Through various case studies, we proved that the weakness of the manual FTA (much time, manpower and cost consuming) can be overcame. Many chemical processes can be used more safe by the FTA system.

REFERENCES

1. J. B. Fussell and G. J. Powers, "Fault Trees- A State of the Art Discussion," IEEE Trans. Rel., Vol. 23, No. 1, (1972).
2. S. L. Salem, G. E. Apostolakis, and D. Okrent, Comp. & Chem. Eng., Vol. 4, (1977).
3. G. J. Powrer and F. C. Tompkins, "Fault Tree Synthesis for Chemical Processes," AIChE, Vol. 20, No. 2, pp. 376-387 (1974).

4. P. Camarda and F. Corsi, A. Trentadue, IEEE Trans. Rel., Vol. 27 (1978).
5. B. E. Kelly and F. P. Lees, Reg. Eng., Vol. 16 (1986).
6. Faisal I. Khan and S. A. Abbasi Analytical simulation and PROPAT II, "A New Methodology and a Computer Automated Tool for Fault Tree Analysis in Chemical Process Industries," Journal of hazardous Materials, **A75, pp. 1-27** (2000).