Korean J. Chem. Eng., **26**(6), 1429-1440 (2009)
DOI: 10.1007/s11814-009-0253-0

Development of a new automatic system for fault tree analysis for chemical process industries

Jiyong Kim*,[‡], Jinkyung Kim, Younghee Lee*, and Il Moon*,[†]**

*Department of Chemical Engineering, Yonsei University,
134 Shinchon-dong, Seodaemun-gu, Seoul 120-749, Korea
**School of Chemical & Biomolecular Engineering, Georgia Institute of Technology,
311 Ferst Drive, N.W. Atlanta, GA 30332-0100, USA

(*Received 28 January 2009 • accepted 5 April 2009*)

Abstract−The main purpose of this study was to develop a computer automated tool for fault tree analysis (FTA) in order to minimize the flaws of manual FTA. The automated FTA system developed in this study consists of two steps: 1) automatic fault tree conversion from a digraph, and 2) calculation of the probability of the occurrence of the top event and finding a minimal cut set of the top event. For the first step, we propose a new algorithm for automatic conversion of a digraph to a fault tree. The new digraph-FT conversion algorithm has eight FT generation rules to transform node information that is based on the node characteristics. Failures and faults are classified into three types to easily synthesize fault trees and analyze fault trees precisely. The automatic FTA system was then applied the analysis of real chemical processes to illustrate the effectiveness of the system.

Key words: Fault Tree Analysis, Automatic FTA, Digraph, Hazard Assessment, Minimal Cut Set

INTRODUCTION

Risk is defined as a measure of the potential likelihood and magnitude of human injury, environmental damage, or economic loss [1]. An essential goal of risk analysis is the estimation and assessment of risk by gathering and integrating information regarding accident scenarios, frequencies and consequences.

As a powerful tool for a risk assessment, fault tree analysis (FTA) has long been applied for quantitative risk analysis of chemical processes, and much can be gained from the application of FTA in the chemical process industry [1]. FTA is based on constructing a hypothetical tree of base events that branch into numerous sub-events, which propagate the fault and eventually lead to the undesirable top event [2]. FTA has the following merits: i) the results of FTA are reliable due to its inherent statistical analysis; ii) FTA can quantitatively and qualitatively evaluate the safety concerns of a given process; iii) FTA identifies the causal aspects of a system that are relevant to significant failures.

The conventionally applied manual construction of fault trees is dependent on the expertise of the constructor and requires enormous manpower, cost, and time. Additionally, the results achieved from manual construction of fault trees are often unreliable. To mitigate these problems, many researchers have been studying computer-aided FT synthesis for some time. Fussell developed a typical fault tree synthesis methodology using transfer functions and system schematic diagrams [3], while Lapp and Powers proposed their well-known algorithm based on digraphs; a digraph represents an accurate representation of the qualitative relationships between process variables, human errors, and equipment failures [4]. The following are proposed methods for making computer-aided FT synthesis more efficient and concise: the reliability graphs approach of Camarda and Trentadue [5], the decomposition approach of Shafaghi et al. [6], the mini-fault tree model of Kelly and Lees [7], and the knowledge-based approach of Elliott [8]. Based on these approaches, computerized FT synthesis software and automated FTA software have been developed, e.g., the software package PROFAT-II of Khan and Abbasi [2], CARA-Fault Tree of Sysdvest Software [9], and Fault Tree+ of Isograph Software Ltd. [10].

Some of the above studies regarding computer-aided fault tree synthesis only concentrate on individual aspects of analyzing fault trees but not on the entire FTA procedure, including automatic construction of fault trees. Furthermore, some of these products are not suitable for evaluating complex systems, such as real chemical processes. Therefore, in this study, an automatic FTA system is developed from a new digraph-FT conversion algorithm. The new FTA system is able to automatically transform digraph process data to fault trees and evaluate the probability of occurrence of the top event.

AUTOMATIC DIGRAPH-FT CONVERSION ALGORITHM

1. Features of the Digraph-FT Conversion Algorithm

Lapp and Powers proposed a new fault tree synthesis algorithm based on digraphs [4]. Their automatic digraph-FT conversion algorithm is used in this study. By modifying and improving Lapp & Powers' algorithm, it is easier to apply and faster in computation. The new algorithm also gives more reliable results than the original algorithm. The features of the new algorithm in this study are as follows:

[†]To whom correspondence should be addressed.
E-mail: ilmoon@yonsei.ac.kr
[‡]Present address: Department of Chemical & Engineering, University of Wisconsin-Madison, 1415 Engineering Drive, Madison, WI 53705, USA

1-1. Classification with Eight FT Generation Rules

Lapp & Powers' algorithm consists of four FT-generation rules that do not consider node situations, such as deviations (+ or −) and terms of magnitude (0, 1, 10) [4]. In this study, these four FT-generation rules are subdivided into eight types (structure I, II, III-A, III-B, III-C, IV-A, IV-B and IV-C) as node situations. This classification eliminates unnecessary calculations and iterations and combines several steps into one. Furthermore, it is suitable to apply to large and complex systems, and it minimizes computation time.

1-2. Removal of Inconsistent and Repeated Events

The new automatic digraph-FT conversion algorithm in this study checks the appearance of nodes and their relationship with the previous and following events to avoid logical errors such as a recurrence of the top event into the fault tree and infinite loop during the construction of fault trees. For example, consistency requires that X0 (+1) not be traced to X0 (−1) nor to X0 (0). Any inconsistent events that are generated in the course of the synthesis must be deleted, and generated events must be checked for the consistency.

1-3. Classification of Failures

In Lapp & Powers' algorithm, the system variables (temperature, pressure, flow rate, concentration) and failure are regarded as the same node. If the system is small or simple, it is justifiable to identify failures with the variables. This is because a deviation in one variable or occurrence of a failure causes a deviation in a second variable, although it is irrelevant whether this is caused by a variable or occurrence of a failure. For large and complex systems, it is necessary that failure and faults are considered independently of the system variables in order to synthesize fault trees easily and to analyze fault trees precisely. Further, faults and failures are classified into three types based on the digraph representations and the patterns of their propagation in the system. This classification of the failure increases the efficiency of the automatic FT construction algorithm to make failure classification simple.

- Failure type A

Type A(f) refers to failures that can be affected by normal operating variables and external influences. If both x1 and x2 are on the same positive feedback loop (PFBL), the values of x2 can be affected not only by f but also by x1. In the case of negative feedback loop (NFBL), x2 is always affected only by f. In Fig. 1(a), the operating variable C is affected by variable B and failure f simultaneously.

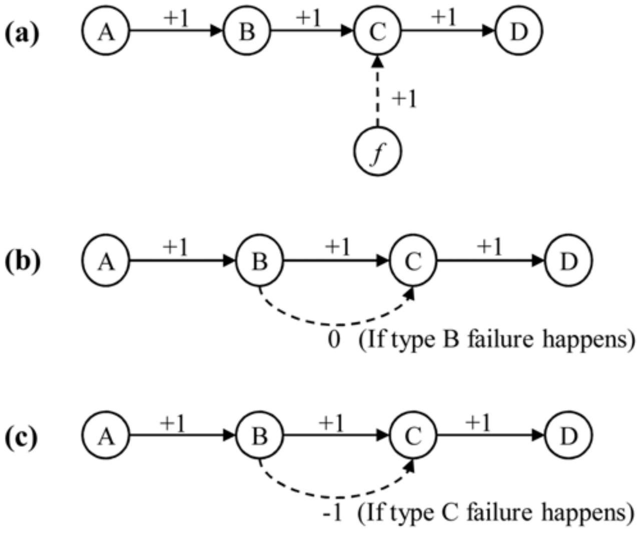

Fig. 1. Configurations of failure (a) Failure type A. (b) Failure type B. (c) Failure type C.

- Failure type B

Type B(f) refers to failures that cause the relationship between variables to change to zero. In type b failures, the edge between x1 and x2 can be considered nonexistent. For example, if a pressure sensor is stuck, its input/output variables become zero (See Fig. 1(b)).

- Failure type C

Type C(f) refers to a failure that causes an inverse relationship between variables. For example, if an A/O valve is equipped in the A/C valve location, the process works inversely to its correct configuration (See Fig. 1(c)).

2. Digraph-FT Conversion Algorithm Procedure

The new algorithm for automatic digraph-FT conversion used in this study is shown in Fig. 2. The digraph-FT conversion algorithm was developed by using a recursive method with FT-generation rules. For a given digraph, the algorithm investigates the top event chosen at the beginning stage. According to this process, the algorithm also applies each FT-generation rule to compose a fault tree. The recursive technique that was used to create fault trees depends on the given situations and node type. The algorithm then recognizes the digraph's next node that is related to the top event as the new target node and applies the FT-generation rules again. If the node is considered a basic event, the FT composition is completed. The main steps of this algorithm are summarized as follows:

(1) Is X0 a non-basic event?

It is first determined if the given node is a basic event that has no event or gate. If the node is a basic event that has no influence on any other event or gate, it is not necessary to consider further and the algorithm is stopped.

(2) Is X0 on NFBL?

In step 6, it is determined if the given node is a component of an NFBL. If there is an external influence that is in control, nodes on NFBLs are not affected because an NFBL has a regulatory action itself. However, if an external influence is out of control, nodes on NFBLs can be affected. Thus, the FT-generation rule considering features of NFBLs needs to be developed.

(3) Is X0 a terminal node on a negative feed forward loop (NFFL)?

Step 7 determines if the given node is a terminal node of an NFFL. In an NFFL, a start node is different from a terminal node, contrary to NFBLs. The start node on the NFFL is only affected by external influences; however, the terminal node is affected not only by external influences but also by other nodes on the NFFL. Therefore, nodes other than the terminal node on NFFLs follow the FT-generation rule like nodes that are not on a loop. The terminal node on an NFFL follows the FT-generation rule by considering effects of external influences and other nodes on the NFFL.

(4) Is X0 both a node on an NFBL and the terminal node of an NFFL?

This step checks the combined questions of step 6 and step 7 to determine if the given node is both a node of an NFBL and the terminal node of an NFFL. In this case, because a node is changed by features of NFBLs and NFFLs, an FT-generation rule that considers the two features simultaneously needs to be developed.

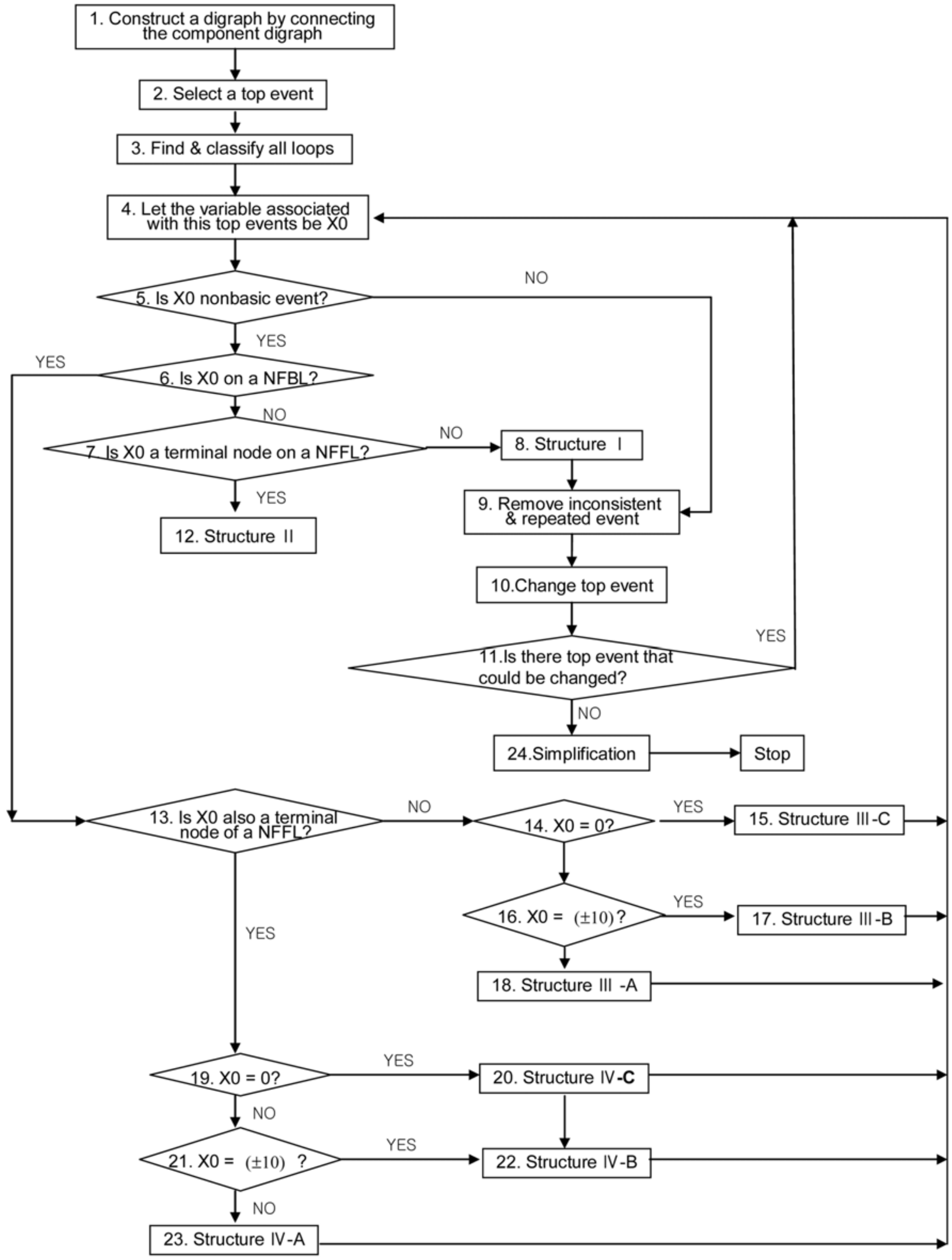

Fig. 2. The new digraph-FT conversion flow chart.

(5) Remove the inconsistent and repeated event

This step plays an important role in the digraph-FT conversion algorithm to prevent a recurrence of the top event into the fault tree. In addition, if an event is repeated on the same level, the event will be eliminated to prevent the algorithm from becoming stuck in an infinite loop.

3. FT Generation Rules

To correctly transform digraph information into a fault tree requires some uniform rules. In this study, the FT-generation rules are classified into four structures depending on the situation of nodes discussed above. These four rules are embedded with the modified transfer function presented by Fussell [3]. The fault-tree-generation

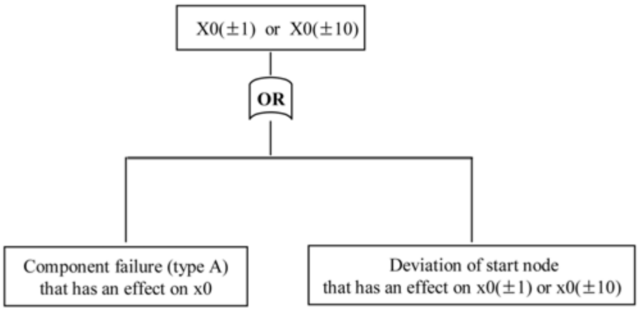
X0(±1) or X0(±10)
OR
Component failure (type A) that has an effect on x0
Deviation of start node that has an effect on x0(±1) or x0(±10)

Fig. 3. FT generation rules: structure I.

rules in this study are as follows:

(a) Structure I

When the situation of nodes belongs to the following three cases, those nodes form a fault tree like Fig. 3 when one of the following holds:

(i) The node is in a PFFL and in a PFBL.

(ii) The node is in an NFFL and it is not a terminal node.

(iii) The node is not in a loop.

Structure I is the arrangement of the deviation in an input node that has an effect on the target node by connecting to an OR gate.

(b) Structure II

When the node is a terminal node of an NFFL, this node forms structure II. Structure II is a FT-generation rule that considers the effect of the start node and also of the non-start nodes. This is shown in Fig. 4.

(c) Structure III

When the node is in an NFBL, a fault tree is constructed by structure III. Structure III is a FT-generation rule that considers the control ability of loop by itself and consists of three types of structures: III-A, III-B and III-C (See Fig. 5).

(d) Structure IV

Structure IV is applied when the given node is the terminal node of an NFFL and is also a node in an NFBL. In this case, the FT-generation rule considers the peculiarities of being in an NFBL and an NFFL at the same time. Therefore, the FT-generation rule is a combination of structure I and II as shown in Fig. 6.

NEW AUTOMATIC FTA SYSTEM

The new automatic FTA system in this study includes both construction and analysis of fault trees. Before the fault trees are analyzed, the fault tree produced from the above conversion algorithm must be simplified. Because fault trees drawn directly from a computer algorithm usually have superfluities, some simplification can help to make them more clear and concise. This new automatic FTA system uses the method proposed by Wang et al. [11] for simplification of fault trees. Two kinds of simplification are performed: algebraic simplification and tree simplification. Algebraic simplification basically deals with certain or negligible events. When a certain event (with the probability of 1) is under an OR gate, algebraic simplification is performed to remove the parent gates until an AND

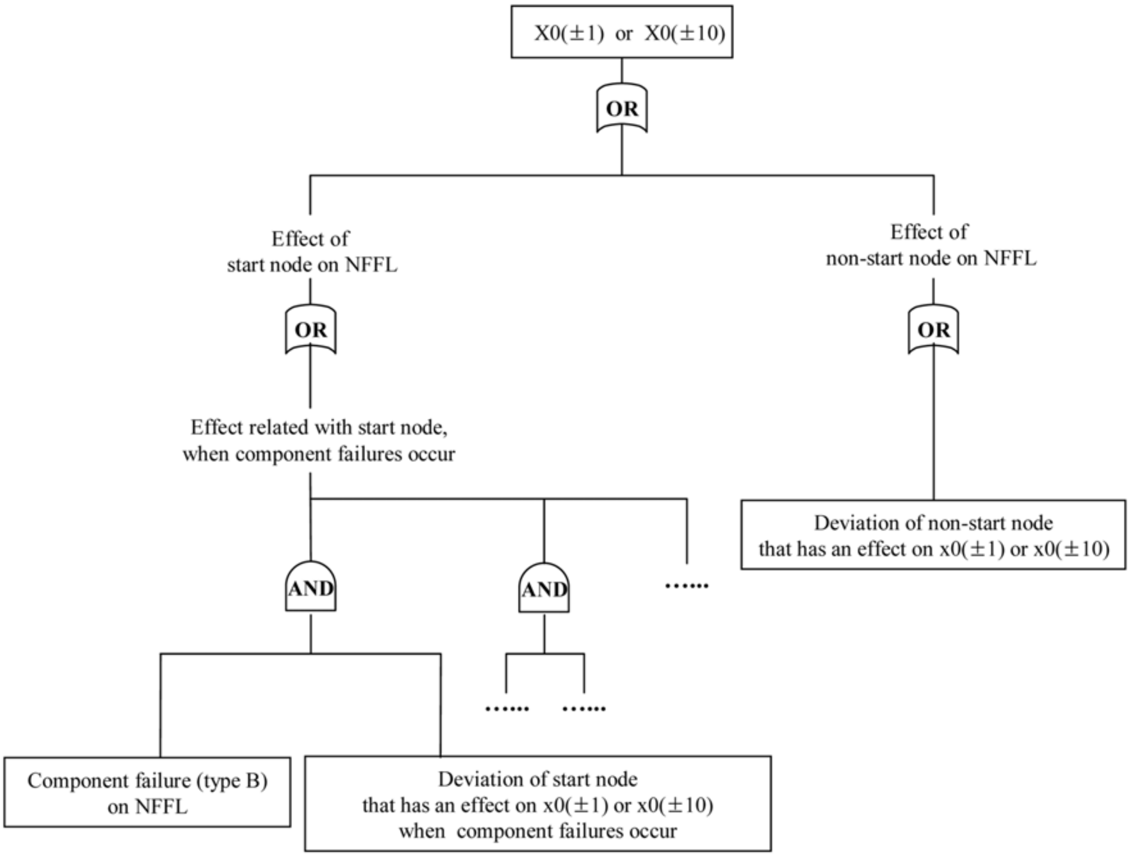
X0(±1) or X0(±10)
OR
Effect of start node on NFFL
OR
Effect related with start node, when component failures occur
AND
AND
......
......
......
Component failure (type B) on NFFL
Deviation of start node that has an effect on x0(±1) or x0(±10) when component failures occur
Effect of non-start node on NFFL
OR
Deviation of non-start node that has an effect on x0(±1) or x0(±10)

Fig. 4. FT generation rules: structure II.

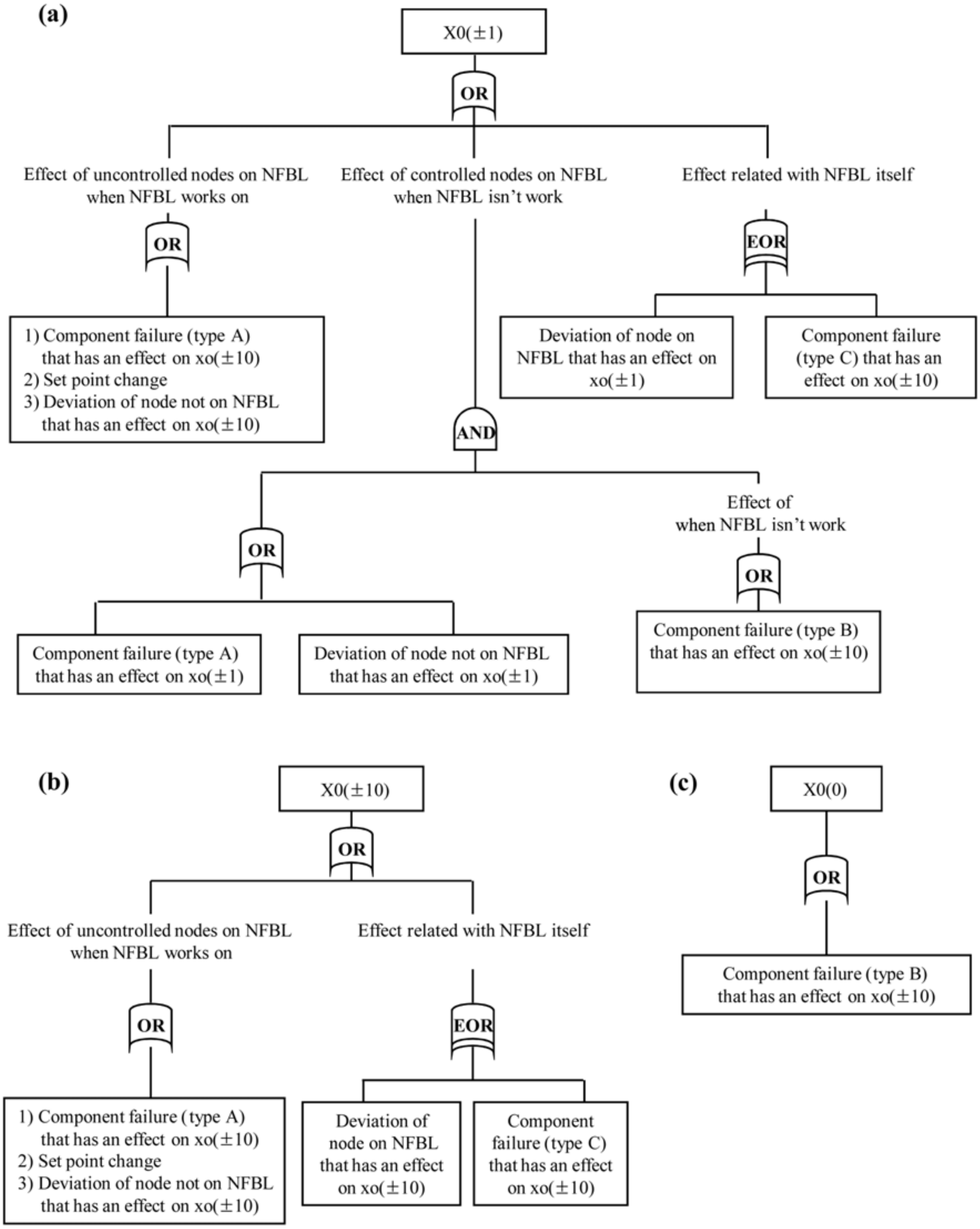
(a)
X0(±1)
OR
Effect of uncontrolled nodes on NFBL when NFBL works on
Effect of controlled nodes on NFBL when NFBL isn't work
Effect related with NFBL itself
OR
EOR
1) Component failure (type A) that has an effect on xo(±10)
2) Set point change
3) Deviation of node not on NFBL that has an effect on xo(±10)
Deviation of node on NFBL that has an effect on xo(±1)
Component failure (type C) that has an effect on xo(±10)
AND
OR
Effect of when NFBL isn't work
OR
Component failure (type A) that has an effect on xo(±1)
Deviation of node not on NFBL that has an effect on xo(±1)
Component failure (type B) that has an effect on xo(±10)
(b)
X0(±10)
OR
Effect of uncontrolled nodes on NFBL when NFBL works on
Effect related with NFBL itself
OR
EOR
1) Component failure (type A) that has an effect on xo(±10)
2) Set point change
3) Deviation of node not on NFBL that has an effect on xo(±10)
Deviation of node on NFBL that has an effect on xo(±10)
Component failure (type C) that has an effect on xo(±10)
(c)
X0(0)
OR
Component failure (type B) that has an effect on xo(±10)

Fig. 5. FT generation rules: (a) Structure III-C. (b) Structure III-B. (c) Structure III-C.

gate is encountered. When a certain event is under an AND gate, the event is directly deleted. If an event with negligible probability is under an AND gate, the removal of the entire parent gate will continue until an OR gate is met. If a negligible event is under an OR gate, the event will be directly deleted.

For qualitative analysis, the automatic FTA system in this study computes the probability of the occurrence of the top event with unavailability, which is the probability that a component is not available (i.e., failed, out for testing, etc.) at time t. Unavailability is calculated from the failure rate and the mean time to repair. Because it can be difficult to obtain this reliability data for chemical processes, users can directly input the value of the unavailability instead of the failure rate and the mean time to repair. The procedures for computing the top event probability are as follows: 1) Input probability data (the failure rate and the mean time to repair) of each basic event. 2) Compute the unavailability for each basic event. 3) Compute the probability of occurrence for each cut set. 4) Compute the probability of the top event.

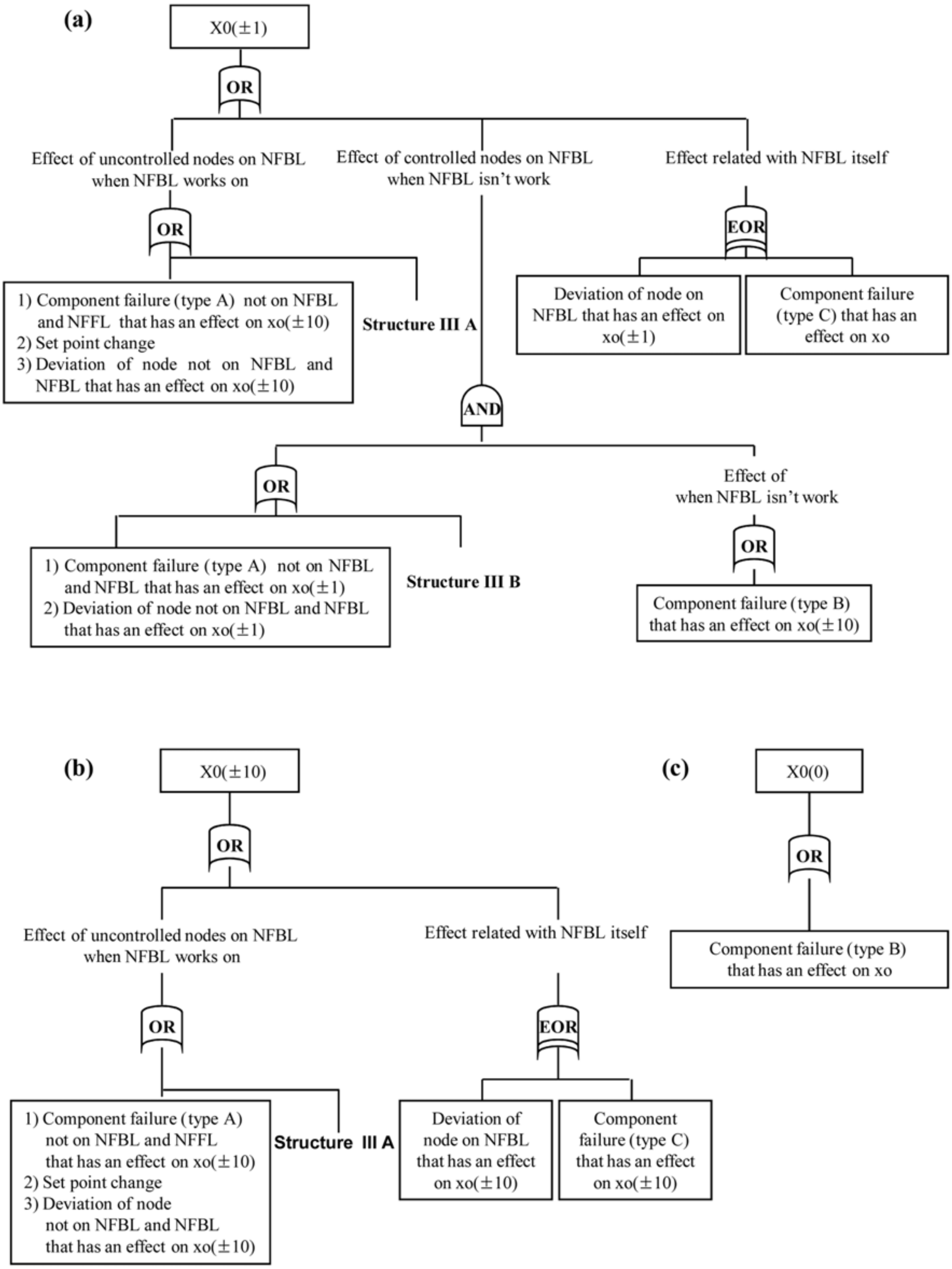
(a)
X0(±1)
OR
Effect of uncontrolled nodes on NFBL when NFBL works on
Effect of controlled nodes on NFBL when NFBL isn't work
Effect related with NFBL itself
OR
EOR
1) Component failure (type A) not on NFBL and NFFL that has an effect on xo(±10)
2) Set point change
3) Deviation of node not on NFBL and NFBL that has an effect on xo(±10)
Structure III A
Deviation of node on NFBL that has an effect on xo(±1)
Component failure (type C) that has an effect on xo
AND
OR
Effect of when NFBL isn't work
1) Component failure (type A) not on NFBL and NFBL that has an effect on xo(±1)
2) Deviation of node not on NFBL and NFBL that has an effect on xo(±1)
Structure III B
OR
Component failure (type B) that has an effect on xo(±10)
(b)
X0(±10)
OR
Effect of uncontrolled nodes on NFBL when NFBL works on
Effect related with NFBL itself
OR
EOR
1) Component failure (type A) not on NFBL and NFFL that has an effect on xo(±10)
2) Set point change
3) Deviation of node not on NFBL and NFBL that has an effect on xo(±10)
Structure III A
Deviation of node on NFBL that has an effect on xo(±10)
Component failure (type C) that has an effect on xo(±10)
(c)
X0(0)
OR
Component failure (type B) that has an effect on xo

Fig. 6. FT generation rules: (a) Structure IV-C. (b) Structure IV-B. (c) Structure IV-C.

As the next step of the automatic FTA system, quantitative analysis is used to determine the minimal cut sets. After a large fault tree has been constructed, it may be difficult to "see" how combinations of events can cause the top event. In this case, it is most instructive to rearrange the fault tree into its minimum cut-set form. Determining the minimum cut-set form of a fault tree is the most accurate way to find a basic event that causes a failure of the top event. Minimal cut sets are sets in which no smaller cut sets are included. For small fault trees, it is often possible to enumerate the minimal cut sets by inspection. However, for larger fault trees, inspection alone may not be feasible. For efficient determination of minimal cut sets, the automatic FTA system in this study uses Fussell's algorithm

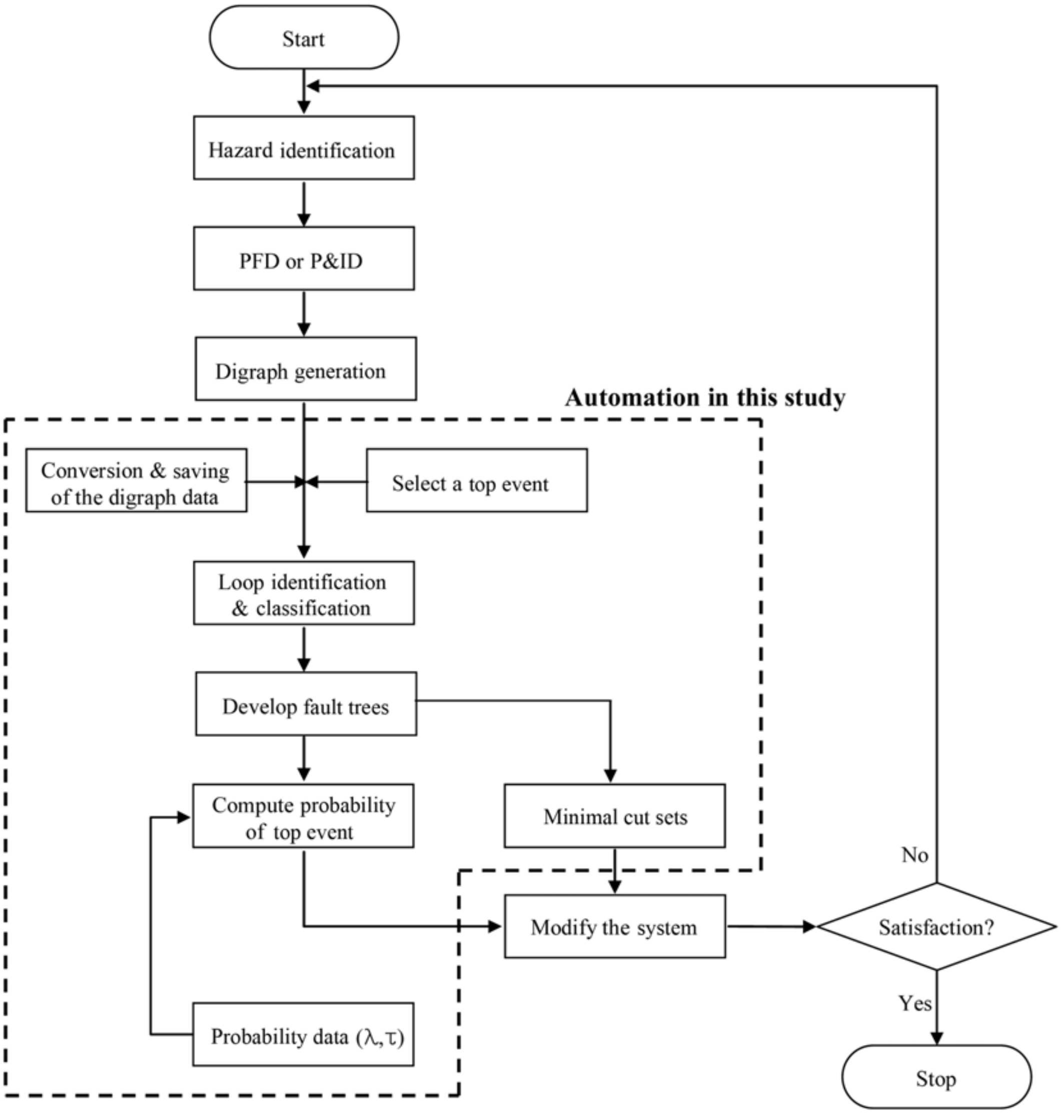

Fig. 7. Hazard identification and automation of FTA.

[3]. With the generated fault trees, users can search not only the minimal cut sets but also the ranking of basic event frequency and the gate list.

The automatic FT conversion algorithm includes the following procedures: 1) user-input node data representing process variables and failure data for building the system digraph according to P&ID, 2) user-input names of these node and failure data, 3) selection of the top event, 4) identification and classification of loops in the system digraph, 5) classification of fault and failure types, 6) calculation of probability data, 7) automatic conversion of the system digraph into a fault tree, and 8) the minimal user-determined representation of cut sets or the ranking of basic event frequency. These procedures are described schematically in Fig. 7.

CASE STUDY

1. FTA of a Chlorination Reactor

To verify the results of the new automatic FTA system, we studied a chlorination reactor, which was adapted from Lapp and Powers [4]. Unsaturated hydrocarbons are chlorinated via the process shown in Fig. 8. Gaseous chlorine enters the process and is mixed with an excess of gaseous hydrocarbons before entering an adiabatic tubular thermal reactor. The hydrocarbon vapor then enters the process through a compressor and passes through a steam-heated heat exchanger before entering the mixer. The flow of the steam to the heater is controlled by the temperature of the reactor effluent. If the compressor is shut down, a signal is sent to close the chlorine flow control valve and to open the inerts injection valve. A list of basic events and failure events is given in Table 1.

In this study, the digraph drawn by Lapp and Powers (1989) [5] is used. By analyzing the digraph, it is observed that there are 2 PFFLs, 2 NFFLs and an NFBL.

(1) NFFL 1
P7→P8→M10→Cl_2(11)→Cl_2(13)
P7→P5→P6→M3→M11→Cl_2(13)
(2) NFFL 2
M20→M12→M13→T14
M20→T12→T13→T14

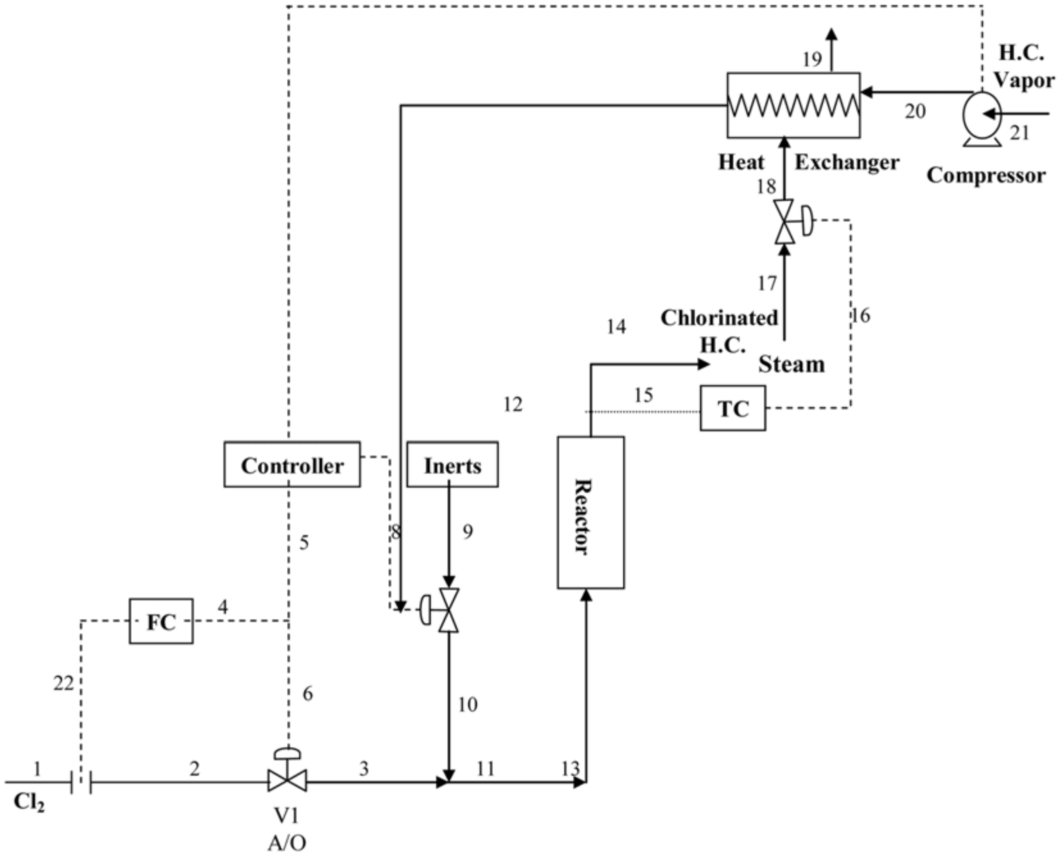

Fig. 8. PFD of the chlorination reactor [4].

Table 1. Basic events and failure events of the chlorination reactor

	Basic and failure events		Basic and failure events
Px	Pressure in stream x	SDCBA	Shutdown controller backward
Mx	Mass flow rate in stream x	SDCBO	Shutdown controller broken
Tx	Temperature in stream x	CBA	Controller backward
Cl_2 (11)	Conc. of Cl_2 in line 11	CBO	controller broken
Cl_2 (13)	Conc. of Cl_2 in line 13	COM Cl_2	Cl_2 flow controller on manual
FCBOCl2	Cl_2 flow controller broken	TSBO	High temperature set pt.
FCBACl2	Cl_2 flow controller backward	COMSTM	Steam controller on manual
FSBACl2	Cl_2 flow sensor backward	CBOSTM	Steam controller broken
FSBOCl2	flow sensor broken	CBASTM	Steam controller backward
VRCl2	Cl_2 valve reversed	FSTH	High Cl_2 flow set pt.
IVS	Inerts valve stuck	CSD	Compressor shutdown
IVR	Inerts valve reversed	EFAR	External fire around reactor
LIF	Low inerts flowrate	TSTH	High temperature set pt.
VRSTM	Steam valve reversed		

(3) PFFL 1
M2→P22→P4→P6→M3
M2→M3
(4) PFFL 2
M20→M12→Cl(13)→T14
M20→T12→T13→T14
(5) NFBL 1
T14→P15→P16→M18→T12→T13→T14

The top event of interest is the high temperature in the reactor (T14 (+10)). T14 (+10) is a terminal node of an NFFL and is also in an NFBL. If T14 (+10) is the top event, a fault tree is constructed with FT-generation rules of structure IV-B. The fault tree that is automatically generated using the digraph is shown in Fig. 9 without the probabilities of basic events. The fault tree of Fig. 9 consists of 3 AND gates, 40 OR gates, and 2 EOR (exclusive or) gates. On the other hand, the fault tree produced by Lapp and Powers had 7

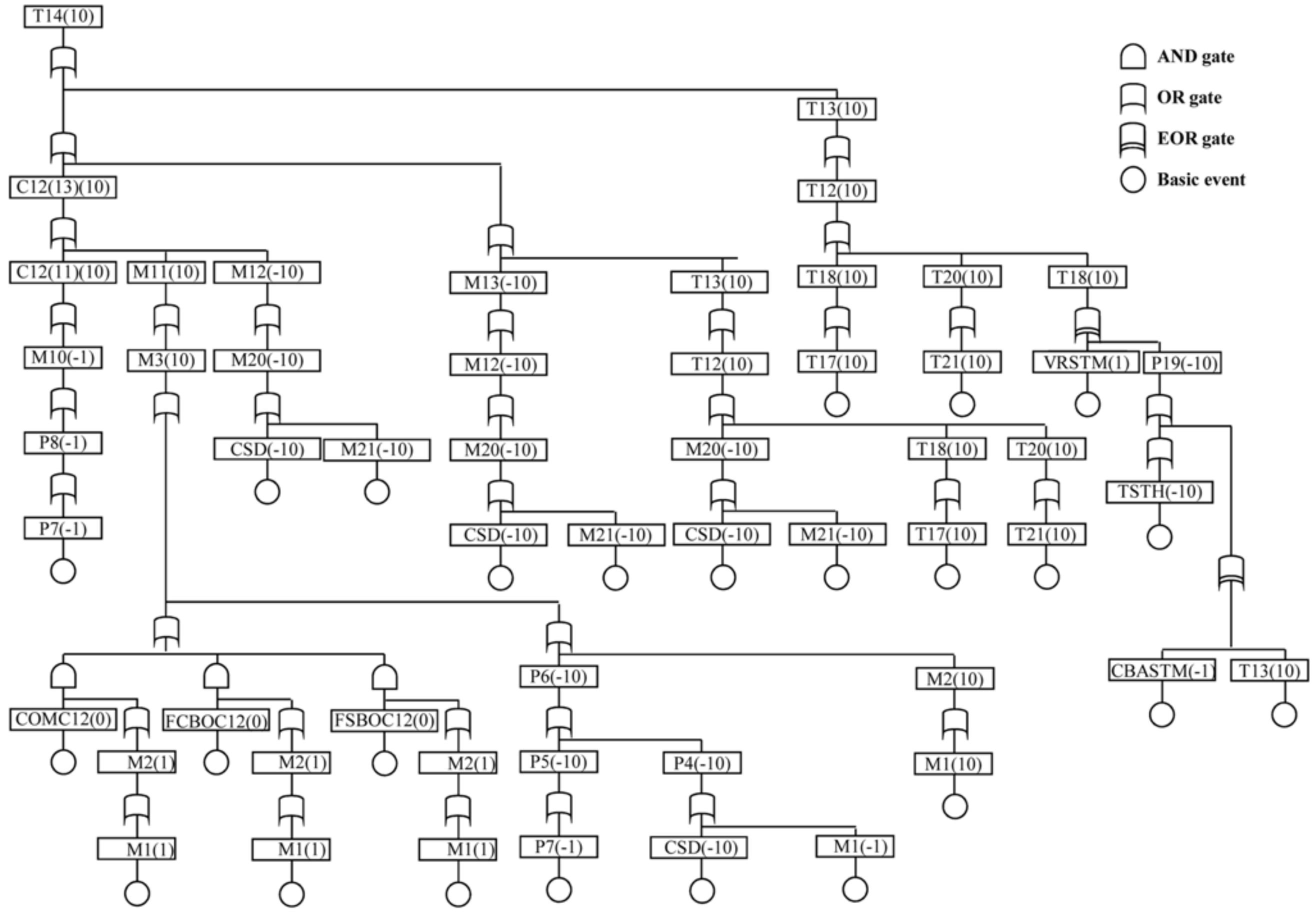

Fig. 9. Fault tree for the top event of the chlorination reactor.

AND gates, 59 OR gates and 11 EOR gates for the same top event, T14 (+10) [4]. Due to the FT-simplification step used in this study, there are fewer intermediate events (AND gates, OR gates, and EOR gates) than shown by Lapp and Powers. Nevertheless, the minimal cut sets that directly cause a failure of the top event are the same as in their results; this is because the FT simplification step in this study only eliminates unnecessary intermediate events and basic events. The minimal cut sets of the above fault tree are as follows:

1. {Cl_2 flow controller on manual (0), Mass flow rate in line 1 (0)}
2. {Cl_2 flow controller broken (0), Mass flow rate in line 1 (0)}
3. {Cl_2 flow sensor broken (0), Mass flow rate in line 1 (0)}
4. {High Cl_2 flow set point (−10)},
5. {Compressor shutdown (−10)}
6. {High temperature set point (−10)}
7. {Steam valve reversed (+1)}
8. {Steam controller backward (−1)}
9. {Pressure in line 7 (−1)}
10. {Pressure in line 15 (−10)}
11. {Mass flow rate in line 1 (−10)}
12. {Mass flow rate in line 21 (−10)}
13. {Temperature in line 17 (+10)}
14. {Temperature in line 21 (+10)}

Based on the results of the minimal cut sets analysis, the top event (T14 (+10)) occurs mainly due to failure of the Cl_2 flow controller, failure of the compressor, the wrong set point, and/or deviations of the flow rate and temperature.

2. FTA of the Nitration Unit

To verify this algorithm again, we have studied here the fault tree for the nitration unit of a hexagon industry. The unit was identified for the detailed FTA after all the units were screened by using indices and the nitration unit was found to be potentially most hazardous [2].

2-1. Process Boundary of the Nitration Unit and Precautions

The unit handles nitric acid and hexamine in 8 : 1 molar ratio at an ideal temperature of 108 °C. Any positive deviation in temperature or reactant proportions may cause a runaway reaction. The reactor is cooled while passing a mixture of water and methanol through the cooling coil at a temperature of 58 °C. The coolant flow rate is controlled by a pneumatic valve i to maintain a reaction temperature of around 108 °C. A slow-moving stirrer is used in the reactor to avoid local heating and hot-spot formation. In case of an emergency, the contents of the reactor may be discharged into an emergency tank. The discharge from the reactor is activated by either pulling an electric chain, using an automatic button, or opening a manually operated manhole valve. The simplified process flow diagram of the unit is shown in Fig. 10.

A detailed study of the unit reveals that to control the risk of an explosion in the reactor the following precautions are necessary:

1. The reactant proportions must be controlled; especially, the

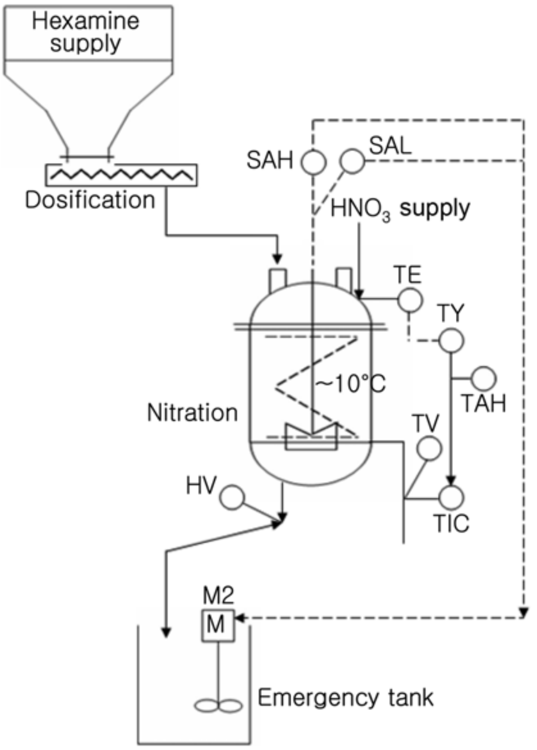

Fig. 10. PFD of the nitration unit [2].

proportion of HNO_3 must not be allowed to fall below eight times that of hexamine.

2. The temperature in the unit must be maintained close to 108 ºC.

3. Local heating must to be avoided.

4. Proper working of the emergency system must be ensured.

2-2. Scenario and Digraph

To represent the process as a digraph, 15 basic nodes were selected, which are typical components of the nitration process, shown in Table 2.

A detailed study of the process and accident scenario measures yielded 23 failure nodes that have a direct and indirect dependency on the top event; namely, explosion of the nitration reactor. These failure nodes include stirrer motor fail, control valve fail, HNO_3 concentration falling below its permissible value, coolant leaks into the reactor, ratio control fails, transmission error, thermostats malfunction, and signal transmission devices fail. A list of failure nodes with their probability of failure is given in Table 3. The probability data has been adapted from Kahn & Abbasi [2].

The digraph for the nitration unit is shown in Fig. 11. A solid line is the normal edge between nodes and a dotted line is a failure edge between nodes. Each gain (0, (±1), (±10)) is estimated based on the detailed study of an accident scenario.

2-3. Fault Tree Synthesis and Analysis

The complete fault tree that is automatically generated from the digraph in Fig. 11 is shown in Fig. 12. The probability of the occurrence of the top event (EXtk) is 1.8E-6 and the minimal cut sets of the above fault tree are as follows:

1. {Coolant ingress into the reactor (+10)}
2. {Cooler control valve stuck (0), Temperature alarm stuck (0), Sensing of higher temp. fails (+10)}
3. {Cooler control valve stuck (0), Temperature alarm stuck (0), Temperature sensor stuck (0)}
4. {Cooler control valve stuck (0), Temperature alarm stuck (0), Automatic discharge valve stuck (0)}
5. {Cooler control valve stuck (0), Automatic discharge valve stuck (0)}, Operator ignores alarm (0)}
6. {Stirrer motor fails (0), Hexamine supply fails (0), Ratio control fails (0)}
7. {Stirrer motor does not start (−1), Not enough HNO_3 (−10), Ratio control fails (0)}
8. {Upper composition alarm stuck (0), HV stuck (0), Automatic discharge valve stuck (0)}
9. {Lower composition alarm stuck (0), HV stuck (0), Automatic discharge valve stuck (0)}
10. {Upper composition alarm stuck (0), Ratio control fails (+10)}
11. {Lower composition alarm stuck (0), Ratio control fails (–10)}

Analysis of these minimal cut sets revealed that the top event

Table 2. Basic events and their probabilities of occurrence

Event name	Basic events	Normal operation condition (gain=+1 or −1)	Probability (failure rate/year)
Ptk	Pressure of reactor	2-3 atm	-
Ntk	Flow rate of reactor	260 kgMol/Hr	-
Ttk	Temperature of reactor	7-10 ºC	-
M1	Flow rate of hexamine	20 kgMol/Hr	-
M2	Flow rate of emergency tank	300 kgMol/Hr	-
M3	Flow rate of HNO_3	240 kgMol/Hr	-
SAH	Upper composition alarm	On	4.6E-5
SAL	Lower composition alarm	On	4.6E-5
TE	Temperature sensor	On	6.7E-4
TY	Signal transmission device	On	9.8E-4
TIC	TV controller	On	1.3E-3
TAH	Temperature alarm	On	5.0E-5
TV	Cooler control valve	On	1.3E-3
HV	Discharge control valve	On	9.2E-5
HHV	Manual discharge valve	On	2.1E-4

Table 3. Failure events and their probabilities of occurrence

Event name	Failure events	Available gain value	Probability (failure rate/year)
A	Temperature alarm fails	0	4.0E-5
B	Operator ignores sounding of alarm	0	1.0E-5
C	Failure of control valve	(±10)	8.0E-6
D	Failure of temperature sensor	0	3.0E-4
E	Sensing of higher temperature fails	0, (+10)	1.0E-5
F	Signal transmission device fails	(±10)	3.2E-4
G	Coolant supply is inadequate	0, (±1)	5.2E-6
H	Failure of SAH	0, (+10)	4.0E-5
I	Failure of SAL	0, (−10)	4.0E-5
J	Alarm fail SAH	0, (+10)	5.0E-6
K	Alarm fail SAL	0, (−10)	5.0E-6
L	Ratio control fails	0, (±10)	4.0E-4
M	Not enough HNO_3 available	(−1), (−10)	2.0E-4
N	Stirrer motor fails	0, (±1)	7.0E-5
O	Coolant ingress into the reactor	0, (±10)	1.5E-6
P	Stirrer motor does not start on demand	0, (±1)	3.0E-4
Q	Hexamine supply fails	0, (±1)	5.5E-5
R	HV gets stuck	0	4.5E-5
S	Operator fails to activate manual discharge	0	2.5E-4
T	Manually discharge valve gets stuck	0	2.1E-4
U	Operator fails to activate automatic discharge	0	1.2E-4
V	Automatic discharge valve gets stuck	0	3.0E-4
W	Operator ignores sounding of alarm SAH or SAL	0, (±10)	1.0E-5

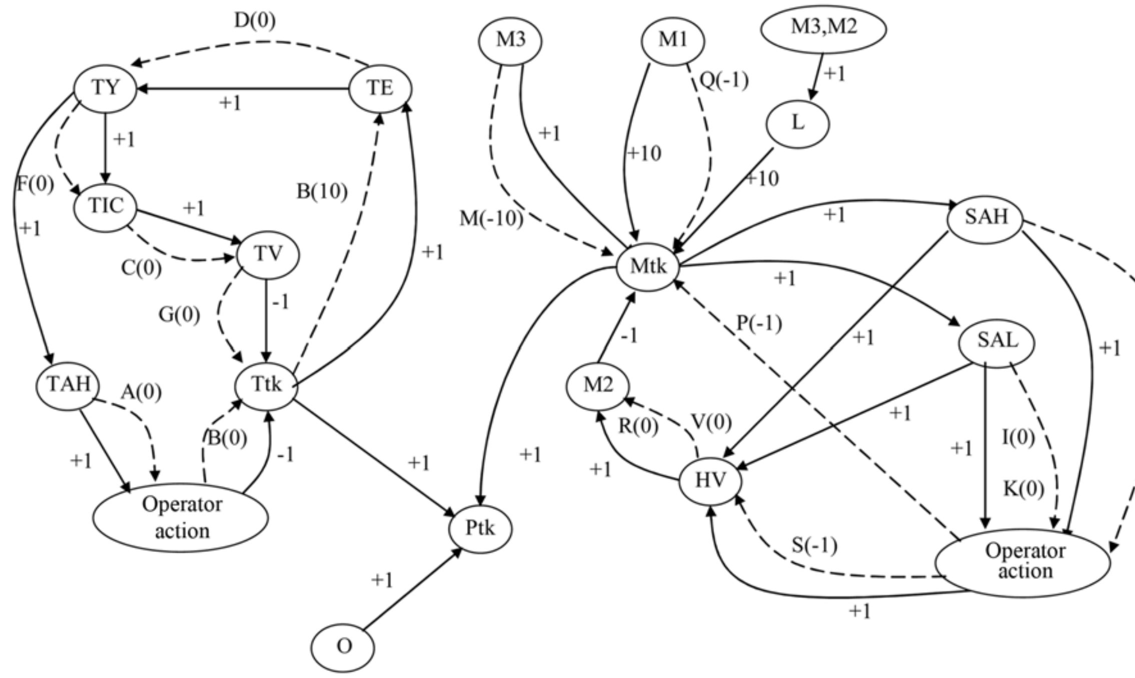

Fig. 11. Digraph for nitration unit (—: normal edge, ---: failure edge).

(EXtk) occurs mainly due to the failure of control valves and composition alarms. Therefore, the probability of the occurrence of a nitration unit explosion is reduced by safety supervision or by installing additional control valves and composition alarms.

CONCLUSION

An automatic FTA system based on a new digraph-FT conversion algorithm is proposed in this paper. For simplicity in program-

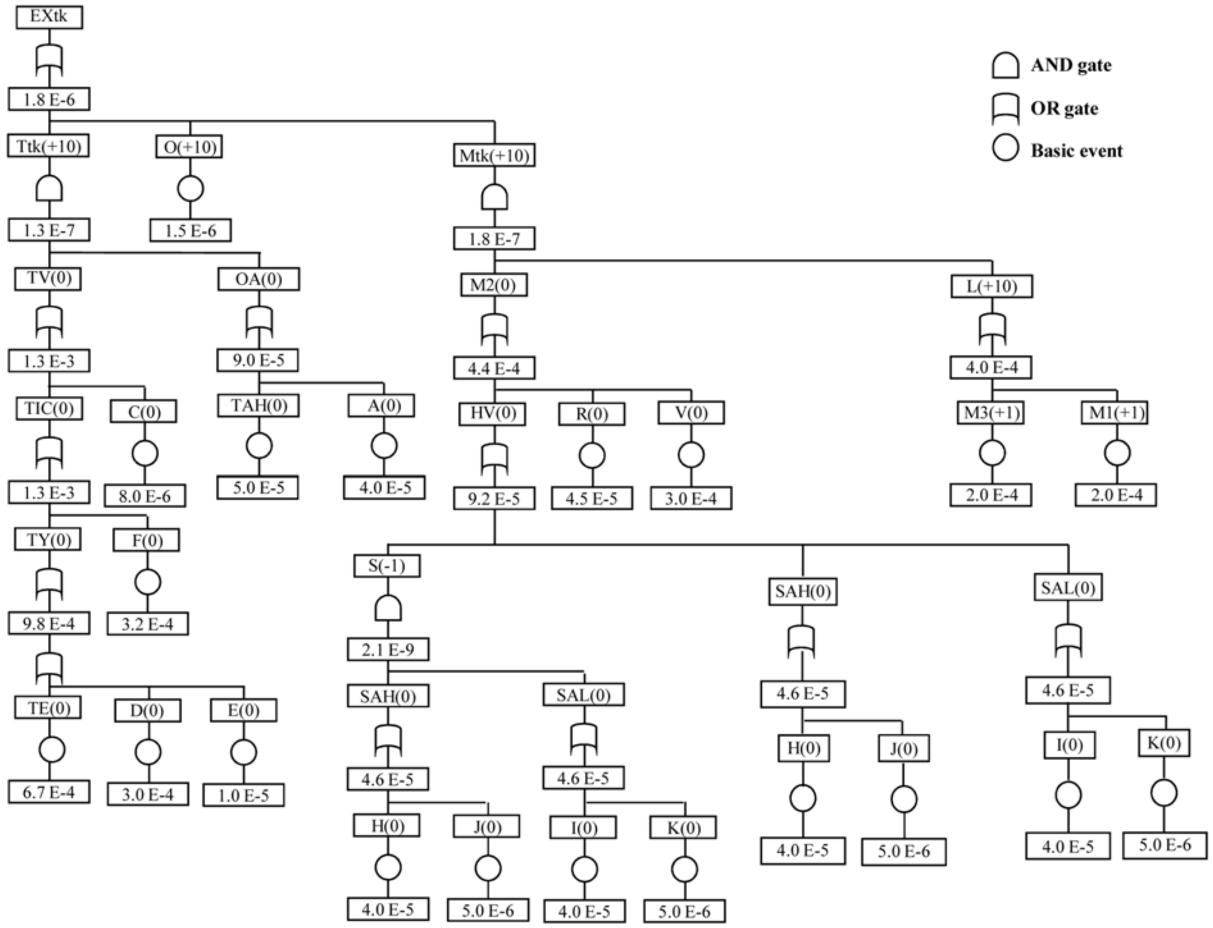

Fig. 12. Fault tree for explosion of the nitration unit.

ming and for application to large and complex systems in a group, this new algorithm includes eight FT-generation rules, which are an improvement of the computer-aided methodology for fault tree synthesis of Lapp and Powers. Additionally, steps are included that remove inconsistent and repeated events. By classifying the failures and the fault tree simplification procedure, the fault trees created by the new automatic FTA system are expected to be correct and concise. This new automatic FTA system mitigates the flaws of manual FTA and determines the minimal cut sets and the probability of occurrence of the top event with less time and cost than manual FA. This system overcomes technical problems with little information, as is the case for PFD or P&ID, and executes FTA in a simple manner. Because it composes and analyzes the fault trees with constant rules, this system also avoids objectivity problems associated with the FTA results, which can result from users' logical problems or subjective experiences. Two case studies, FTA of a chlorination reactor and a nitration unit, proved that this automatic FTA system is suitable for application to large and complex systems and is easy to use.

ACKNOWLEDGMENTS

This work was supported by the Ministry of Education (MOE) of Korea by its BK21 Program.

REFERENCES

1. CCPS, *Guideline for chemical process quantitative risk analysis*, 1st edition Ed. New York: Center for Chemical Process Safety, AIChE (1989).
2. F. I. Khan and S. A. Abbasi, *J. Hazard. Mater.*, **75**, 1 (2000).
3. J. B. Fussell, *Nucl. Sci. Eng.*, **52**, 421 (1973).
4. S. A. Lapp and G. J. Powers, *IEEE T. Reliab*, **R26**, 2 (1977).
5. P. Camarda and A. Trentadue, *IEEE T. Reliab*, **R27**, 215 (1978).
6. A. Shafaghi, F. P. Lees and P. K. Andow, *Reliab. Eng. Sys. Safe.*, **8**, 193 (1984).
7. B. E. Kelly and F. P. Lees, *Reliab. Eng. Sys. Safe.*, **16**, 39 (1986).
8. M. S. Elliott, *IEEE T. Reliab.*, **R43**, 112 (1994).
9. CARA-Fault Tree light edition 4.1 SR1, *Sysdvest software* (1999) (www.sysdvest.com).
10. FaultTree+ Ver. 11.0 Demo, *Isograph Software Ltd.* (2008) (http:// www. isograph-software.com).
11. Y. Wang, T. Teague, H. West and S. Mannan, *J. Loss Prevent. Proc.*, **15**, 265 (2002).