A systematic fault tree analysis based on multi-level flow modeling

GOFUKU Akio [1], and OHARA Ai [2]

1. Graduate School of Natural Science and Technology, Okayama University, 3-1-1 Tsushima-Naka, Kita-ku, Okayama 700-8530, Japan (fukuchan@sys.okayama-u.ac.jp)

2. Department of Systems Engineering, Okayama University, 3-1-1 Tsushima-Naka, Kita-ku, Okayama 700-8530, Japan

Abstract: The fault tree analysis (FTA) is widely applied for the safety evaluation of a large-scale and mission-critical system. Because the potential of the FTA, however, strongly depends on human skill of analyzers, problems are pointed out in (1) education and training, (2) unreliable quality, (3) necessity of expertise knowledge, and (4) update of FTA results after the reconstruction of a target system. To get rid of these problems, many techniques to systematize FTA activities by applying computer technologies have been proposed. However, these techniques only use structural information of a target system and do not use functional information that is one of important properties of an artifact. The principle of FTA is to trace comprehensively cause-effect relations from a top undesirable effect to anomaly causes. The tracing is similar to the causality estimation technique that the authors proposed to find plausible counter actions to prevent or to mitigate the undesirable behavior of plants based on the model by a functional modeling technique, Multilevel Flow Modeling (MFM). The authors have extended this systematic technique to construct a fault tree (FT). This paper presents an algorithm of systematic construction of FT based on MFM models and demonstrates the applicability of the extended technique by the FT construction result of a cooling plant of nitric acid.

Keyword: fault tree analysis, functional information, Multilevel Flow Modeling, chemical plant

1 Introduction

The fault tree analysis (FTA) is widely applied to the safety evaluation of systems, especially in the development of large-scale and mission-critical systems such as nuclear power plants, chemical plants, and aircrafts. The FTA is a top-down method to evaluate the risk of a system for the purpose of prevention of happening undesirable events. In the FTA, an undesirable top event of a system is first extracted. Then, plausible anomaly causes to the events are identified hierarchically. The relations among the undesirable events and the anomaly causes identified are expressed in a tree diagram using logical symbols. The diagram is called as a fault tree (FT). Finally, the happening probability of the top event is evaluated based on the happening probability of each identified anomaly cause. In the FTA, the construction of the FT for a target system is an important step.

The potential of the FTA, however, strongly depends on human skill of analyzers, and the following problems are pointed out.

(1) Education and training are required to learn how to analyze systems by the FTA.
(2) The quality is unreliable because human analyzers conduct the FTA.
(3) Expertise is required for a target domain.
(4) It is difficult to update FTA results when a target system is reconstructed, because the initial rationale of the FTA is easy to be lost.

Therefore, a systematic FTA generation technique will solve some of these problems. Up to now, many techniques [1, 2] to systematize FT construction have been proposed by applying computer technologies. On the other hand, these techniques only use structural information of a target system and do not use functional information that is one of important properties of an artifact. Recently, a methodology is developed to use the functional information in a safety evaluation of chemical plants [3].

The principle of FT construction is to trace comprehensively cause-effect relations from a top undesirable event (effect) to anomaly causes. The authors proposed a causality estimation technique [4] based on the functional modeling technique, MFM (Multi-level Flow Modeling) [5, 6] for a target system.

Received date :Feburary 28, 2010

The technique can be said as a technique to trace cause-effect relation although some data are necessary to add for FT construction. From this idea, the authors developed a systematic FT construction technique [7] based on MFM models and applied to the evaluation of MFM models that the authors developed for a diagnostic system of a launcher of middle-size space rockets. However, the applicability of FT construction has not been confirmed by comparing the FT derived by other FT construction techniques.

This study applies the systematic FT construction technique to a simple chemical plant. It also discusses its applicability by comparing the FT construction result with that reported in literature [2].

2 Fault tree construction based on the model by multi-level flow modeling

2.1 Multi-level flow modeling

The MFM [5, 6] expresses hierarchically the intention of an artifact from the viewpoint that a system is a man-made purposeful system. The MFM represents a system in two dimensions: The relations among system goals, sub-goals, and system functions to achieve goals/sub-goals are represented by a means-end dimension. The MFM also represents a system in a whole-part dimension to express a system by a multiple of descriptions on different levels of aggregation.

The MFM defines a function as a useful behavior. System functions are represented by a set of mass, energy, activity, and information flow substructures on several levels of abstraction. Mass and energy flow substructures represent system functions. On the other hand, activity and information flow substructures represent operator actions and control system functions. The functional aspects of a system are expressed diagrammatically by a set of function primitives such as source, transport, storage, sink, and so on. The MFM enables ones to represent knowledge of a system which they can capture the intentions of designers of a system and its control systems. The authors think that the MFM is essentially suitable for diagnosing a system because this model shows the relations among the behaviors and the intentions of system components through causal relations.

2.2 Knowledge and data for FT construction

An MFM model systematically represents the functional and structural information of a system such as:

(1) goal and sub-goals of the system,
(2) functions of the system,
(3) relations among functions,
(4) relations among goal/sub-goals and functions, and
(5) relations among functions and the components that realize the functions.

In addition to the above information, the following knowledge and data are necessary for systematic FT construction, especially for tracing cause-effect relations implicitly represented in an MFM model:

(a) the *influence propagation rules* and the *reverse influence propagation rules* that trace the cause-effect relations among functions in a flow substructure,
(b) the *goal-function causality knowledge* that expresses the qualitative causality relation specified in each achievement or condition relation of an MFM model,
(c) the *knowledge* of *component behavior* such as plausible anomalies and their functional influences,
(d) the *operation knowledge* that expresses possible operations and the functional influences of them,
(e) the *dangerous situation knowledge* that expresses undesirable system situations and their functional meaning, and
(f) the *anomaly ontology* of devices that grounds the tracing results of cause-effect relation using an MFM model onto the corresponding anomaly instances as well as the information of anomaly causes.

The *influence propagation rules* and the *reverse influence propagation rules* will be explained in detail in the next subsection. An example of the *anomaly ontology* of devices is explained here. Suppose an abstract anomaly in an MFM model, DEGRADATION OF TRANSPORT AT CONTROL VALVE is deduced by tracing cause-effect relations based on an MFM model, and the abstract anomaly corresponds to an anomaly in the MFM description, e.g., CLOSE-TYPE ANOMALY OF CONTROL VALVE. However, there may be a number of possible causes for the anomaly in fact. Therefore, in

order to construct FT, the anomaly must come out of possible causes such as valve stick, control unit malfunction, sensor error, and actuator malfunction.

2.3 Influence propagation by the change of functional achievement

The authors developed an *influence propagation technique* based on an MFM model to derive plausible counter actions in an anomalous situation of a plant [4]. The technique is applied to construct automatically an FT from the MFM model of a target system and the knowledge and data for FT construction.

In the MFM, a system is depicted as diagrams that are composed of goal/sub-goals and function primitives. Each function primitive qualitatively represents a component behavior in terms of mass, energy, information, and activity. A series of function primitives connected by a flow-line provides the information of causal relation among system functions. On the other hand, an achievement or condition relation between a goal/sub-goal and a function expresses the causal relation of the goal/sub-goal and the function. Each function primitive involves a cause-effect relation upon input(s), output(s), and functional achievement(s).

The cause-effect relation is used to calculate the influence propagation upon a series of function primitives, when the functional achievement changes. There are two types of influence propagation. They are called normal influence propagation and reverse influence propagation. The normal influence propagation traces cause-effect relations from bottom to top of an MFM model and from upstream to down stream of a flow substructure. The cause-effect relations for function primitives are derived beforehand as *influence propagation rules*. On the other hand, the reverse influence propagation traces cause-effect relations from top to bottom and from downstream to upstream. For the reverse influence propagation, *reverse influence propagation rules* are derived. Some of the rules are shown in Table 1. For example, if the output flow of a transport function increases, the effect of the cause appears as an increase of its input flow and an increase of its function achievement. The *reverse influence propagation rules* play important roles in the algorithm of automatic FT construction although the *influence propagation rules* are also used to estimate the influence of the top undesirable event for reference.

Table 1 Examples of reverse influence propagation rules

Function	Cause	Effect
Source	Output +	Function +
	Output -	Function -
Transport	Output +	Input + & Function +
	Output -	Input - & Function -
Sink	Function +	Input +
	Function -	Input -
Balance	One of output +	One of input +
		One of other output +
	One of output -	One of input -
		One of other output -

Figure 1 shows the outline of reverse influence propagation to trace cause-effect relations from a top undesirable event to anomaly causes.

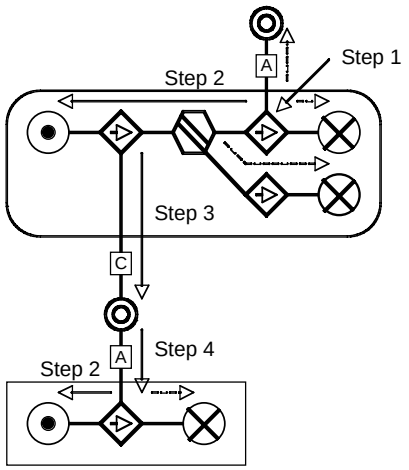

Fig. 1 Reverse influence propagation.

The reverse influence propagation algorithm is composed of the following four steps:

(Step1) A dangerous situation of the target system is mapped to the corresponding function in the MFM model by considering the component to realize a function. Then, go to Step 2.

(Step2) For all the flow substructures that contain influenced functions, this step is adapted. By applying the *reverse influence propagation rules*, the changes of functional achievement at the upstream functions in the flow substructure in Step 1 or functions influenced in Step 4 are estimated. If there is a function in the flow substructure that is conditioned by a sub-goal, continue to Step 3. Otherwise, the reverse influence propagation is terminated.

(Step3) For all the functions conditioned by sub-goals, this step is adapted. The reverse influence at the

sub-goal that is connected to the function by a condition relation is estimated by the *goal-function causality knowledge* between the function and the sub-goal.

(Step 4) For all the sub-goals influenced in Step 3 and achieved by functions, this step is adapted. The reverse influence is propagated to the function in the lower flow structure that achieves the sub-goal by the *goal-function causality knowledge*. Then, return to Step 2.

In this way, the reverse influence of an undesirable behavior on plant is estimated as a whole.

2.4 FT construction algorithm

The construction algorithm of FTs based on an MFM model of a system is explained here.

(Step 1) The top event of FT is determined by the *dangerous situation knowledge*. The functional effect of the top event is given by the representation of the corresponding goal/sub-goal or function node of the MFM model.

(Step 2) The reverse influence propagation is conducted in the MFM model as explained in subsection 2.3.

(Step 3) All the paths in reverse influence propagation are in order traced from the MFM node corresponding to the top event to leaf nodes. In this trace, (1) a sub-goal is captured as an intermediate event in the FT and (2) a component behavior is regarded as a parent node of end events in the FT if a possible change of the component behavior is found by using the *component behavior knowledge* and *operation knowledge*. The end events are derived from the *anomaly ontology* related to the component of the parent FT node.

3 FT construction of a simple chemical plant

3.1 Target chemical plant

This study applies the FT construction algorithm introduced in Subsection 2.4 to a simple chemical plant shown in Fig. 2. The purpose of the plant is to cool high-temperature nitric acid. The high-temperature nitric acid flows into a heat exchanger and transfers the heat to cooling water introduced by a pump. A control valve that is driven by air pressure controls the flow rate of cooling water to regulate the outlet temperature

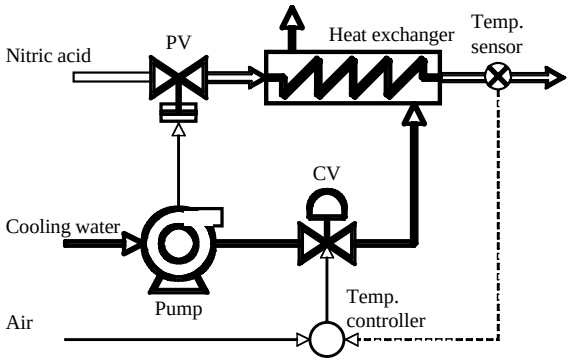

Fig. 2 Structure of a cooling plant of nitric acid.

of nitric acid. The loss of cooling water in the heat exchanger results in an increase of outlet temperature of nitric acid. An excessive temperature increase may lead a fire or explosion of the plant. In order to prevent this situation, a piston valve immediately closes to stop the flow of nitric acid when the cooling water pump stops.

3.2 MFM model for a cooling plant of nitric acid

The nitric acid cooling plant is modeled by the MFM as shown in Fig. 3. This study does not model the control systems of the plant. They play important roles for plant safety operation and need to be studied in the future.

The top goal of the plant is to cool the nitric acid (Go-0) flowing in the heat exchanger. To accomplish the top goal, the energy flow substructure EFS-0 is constructed. The top goal Go-0 is connected to the function Tr-1 (energy flow accompanied by the flow of nitric acid from the heat exchanger) by an achievement relation. This means that the achievement of Go-0 is mainly related with Tr-1 in EFS-0. To maintain the flow of nitric acid, the goal Go-1 (Flowing nitric acid) is identified and is connected to the function Tr-0 (energy flow accompanied by the flow of nitric acid through the piston valve) in EFS-0 by a condition relation. This means that the flow of nitric acid is necessary to transport the heat of nitric acid. The goal Go-1 is achieved by the mass flow substructure MFS-0 that represents the flow of nitric acid. On the other hand, to maintain the heat transfer from nitric acid to cooling water, the goal Go-4 (Keeping the flow of cooling water) is identified and connected to the function Tr-2 (heat transfer in the heat exchanger) in EFS-0 by a condition relation. The goal Go-4 is achieved by the mass flow substructure MFS-1 that represents the flow of cooling water through the pump, the control valve,

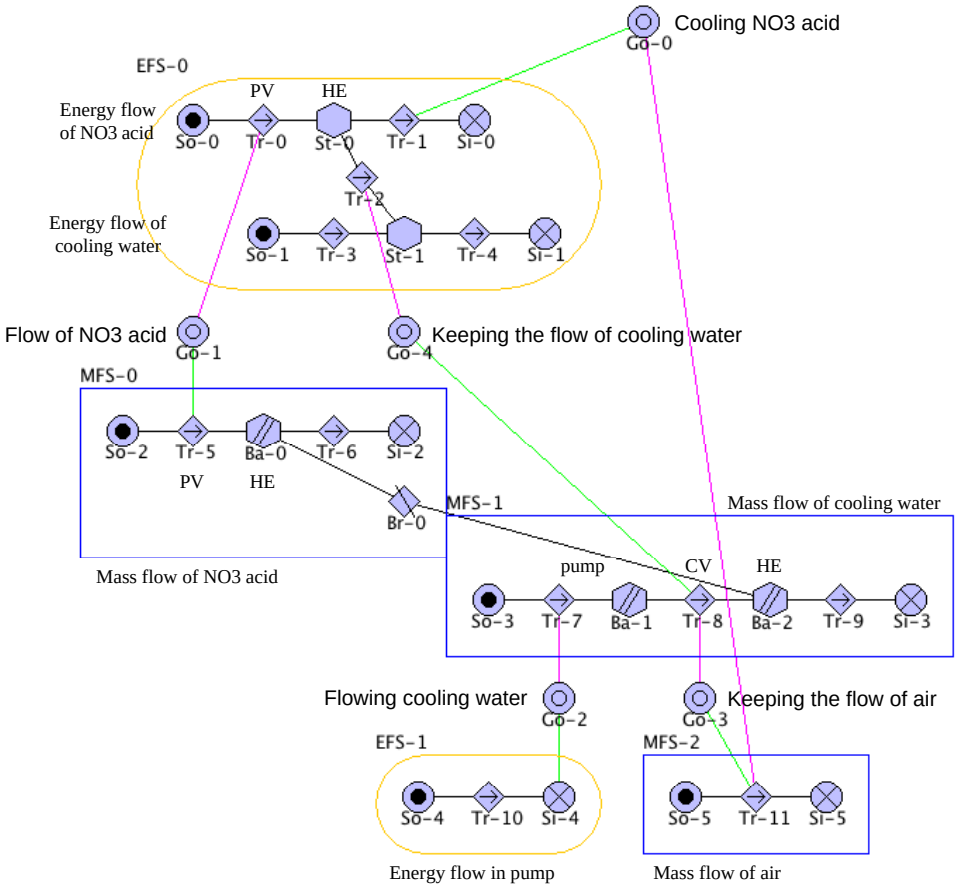

Fig. 3 MFM model for a cooling plant of nitric acid.

and the heat exchanger. The flow path from Ba-0 in MFS-0 to Ba-2 in MFS-1 through Br-0 in MFS-0 represents the leak flow of nitric acid to the cooling water in the heat exchanger. The function of pipe wall in the heat exchanger not to leak nitric acid is represented by the barrier function Br-0 in MFS-0. The function of the pump to flow the cooling water is represented by the energy flow structure EFS-1.

3.3 FT construction results

FT results are obtained based on the MFM model for the cases of increase and decrease of the outlet temperature of nitric acid. The FT obtained for the temperature increase case is shown in Fig. 4. In the figure, the estimated influences to goal/sub-goals or functional nodes are also shown for the understanding of the FT. The "+" or "-" in the bracket shows the qualitative value of reversely propagated influence to a goal/sub-goal or function node.

3.4 Discussions

In order to evaluate the applicability of the FT construction technique based on an MFM model, the FT obtained by this technique is compared with that given by Wang, et al. [2]. The FT by Wang, et al. is shown in Fig. 5. The elements of FT corresponding to the control systems are omitted for comparison.

Almost the same FT is obtained by the technique based on the MFM model. However, there are several differences between two FTs. The comparison of these two models is summarized in Table 2. The differences seem to be mainly caused by the differences of the specifications of anomalies for each component of the plant. The FT given by Wang, et al. does not give the anomaly in pump performance. The anomaly nodes of leak and choke in pipes are obtained only by the authors' technique. These anomaly nodes may be included in the anomaly node of "CW F (-10)" in the FT by Wang, et al. On the other hand, the FT by the authors' technique does not give the anomaly of pressure of cooling water that can be considered as an external anomaly of the target plant.

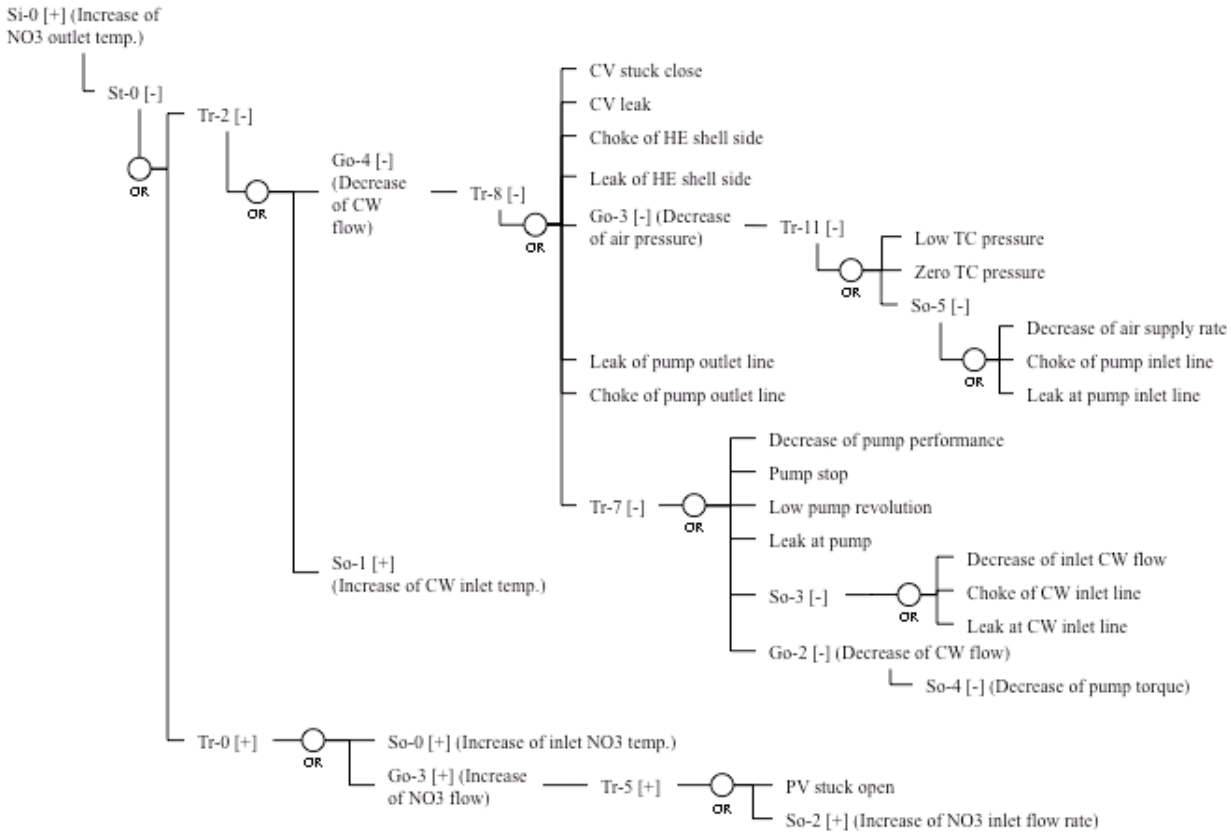

Fig. 4 Fault tree generated based on MFM model.

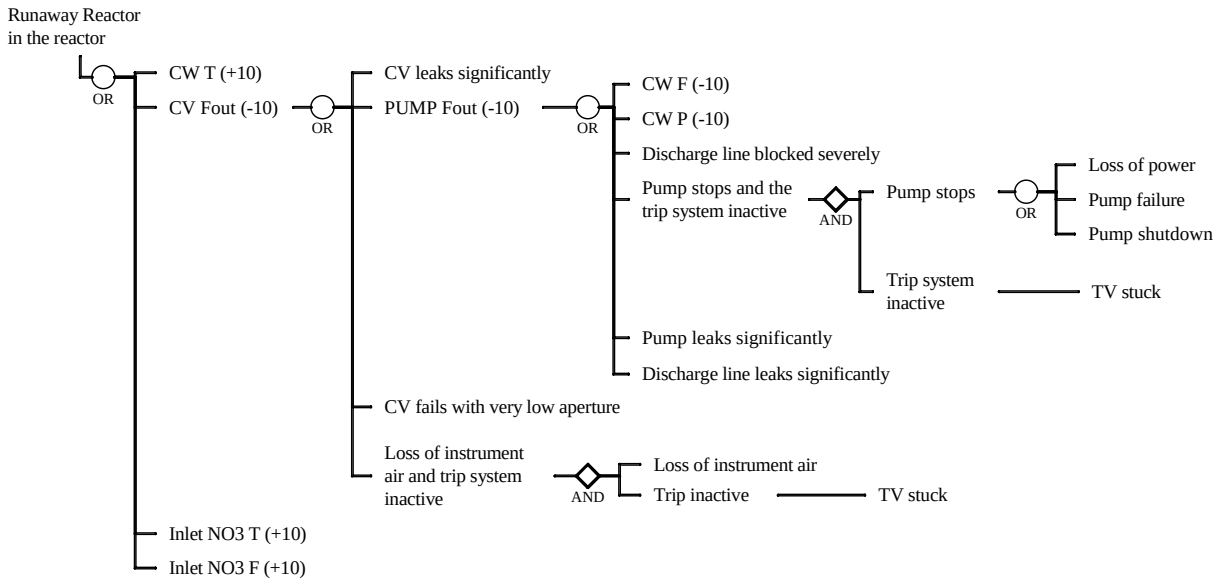

Fig. 5 Fault tree given by Wang, et al. [2].

Table 2 Summary of comparison results of fault trees

	Based on MFM	By Wang, et al.
Equivalent	Increase of NO3 inlet flow rate	Inlet NO3 F (+10)
	Increase of NO3 inlet temp.	Inlet NO3 T (+10)
	Leak of pump outlet line	Discharge line leaks significantly
	Choke of pump outlet line	Discharge line blocked severely
	Increase of inlet CW temp.	CWT (+10)
Similar	CV stuck close	CV fails with very low aperture
	CV leak	CV leaks significantly
	Low TC pressure	Loss of instrument air
	Zero TC pressure	
	Decrease of air supply rate	
	Pump stop	Loss of power
		Pump failure
		Pump shutdown
	Leak at pump	Pump leaks significantly
	Decrease of inlet CW flow	CW F (-10)
Only MFM	Decrease of pump torque	
	Decrease of pump performance	
	Low pump revolution	
	Choke of pump inlet line	
	Leak at pump inlet line	
	Decrease of inlet CW flow	
	Choke of CW inlet line	
	Leak at CW inlet line	
	Choke of HE shell side	
	Leak of HE shell side	
Only Wang, et al.		CW P (-10)

4 Conclusions

This study develops an automatic FT construction technique to solve the problems that the result of FTA depends on human skill of analyzers. This paper extends the causality estimation technique of an anomaly or an operator action on plant behavior to an automatic FT construction technique based on the MFM model of a target system.

The applicability of the technique is evaluated by FT construction of a nitric acid cooling plant. The automatically generated FT based on the MFM model of the system excluding its control systems is confirmed to cover the FT reported in a literature [2].

The future works include that this technique should be extended to treat control systems of a plant that play important roles for safety operation. The manipulation to calculate the reliability of a system from failure probabilities of components based on the generated FT is another future topic.

References

[1] LAPP S. A., POWERS G. J., Computer-aided synthesis of fault trees, *IEEE Transactions on Reliability*, 1977, R-26: 2-12.

[2] WANG Y., TEAGUE T., WEST H., MANNAN S., A new algorithm for computer-aided fault tree synthesis, *J. Loss Prevention in the Process Industries*, 2002, 15, 265-277.

[3] ROSSING N. L., LIND M., JENSEN N., JORGENSEN S. T., A functional HAZOP methodology, *Computers and Chemical Engineering*, 2010, 34, 244-253.

[4] GOFUKU A., TANAKA Y., Application of a derivation technique of plausible counter actions to an oil refinery plant [A], *Proc. IJCAI Fourth Workshop on Engineering Problems for Qualitative Reasoning*, 1999, 77-83.

[5] LIND M., Representing goals and functions of complex systems – an introduction to multilevel flow modelling, report No. 90-D-381, Institute of Automatic Control Systems, Technical University of Denmark, 1990.

[6] LIND M., Modeling goals and functions of complex industrial plants, *Applied Artificial Intelligence*, 1994, 8 (2), 259-283.

[7] GOFUKU A., KOIDE S., SHIMADA N., Fault tree analysis and failure mode effects analysis based on multi-level flow modeling and causality estimation, *Proc. SICE-ICASE International Joint Conference 2006*, 2006, 497-500.