European Symposium on Computer Aided Process Engineering – 15
L. Puigjaner and A. Espuña (Editors)

Dynamic Simulator for Evaluation of Safety Objects in Batch Process

D. Rizal*, S. Tani, K. Nishiyama and K. Suzuki
System Analysis Laboratory, Department of Systems Engineering, Okayama University
700-8530, 3-1-1 Tsushima Naka, Okayama, Japan

Abstract

In this paper, a novel methodology for batch plant safety analysis is proposed using process dynamic modelling. Batch processes are divided into several safety objects that are linked to operation level. Safety objects are evaluated by dynamic simulation and fault propagation models are generated. By using this model, an improved fault tree analysis (FTA) method using house event-time (HET) is proposed and can be developed for calculating the probability of failures. The timely dependent failures can be considered as unavailability of safety objects that can lead to accidents in plants. Finally, the rank of safety object performance index (PI) can be estimated using importance measures. PI shows the prioritization of safety objects that should be investigated for safety improvement in the plants. The output of this method can be used for optimal policy in safety object improvement and maintenance. The dynamic simulator was constructed using Visual Modeler™ (VM™, *Omega Simulation, Japan*) and the loss of containment (LOC) at *polyvinyl chloride* (PVC) batch process is used for case study.

Keywords: dynamic simulator, safety, performance index, fault propagation

1. Introduction

Dynamic simulation of batch chemical process is being importantly used for quantitative hazard assessment (Srinivasan & Venkatasubramanian, 1998) and is a powerful tool to analyze unsteady state behaviour of the chemical process and can be used in all stage of process engineering activities such as process design, operation, control and automation. Dynamic simulation is a very important component of process hazard analysis, since it can quantitatively predict the consequences of critical component failures (Shacham, Brauner & Cutlip, 2000). Several hazard assessment methods have been established and connected to the dynamic simulation. The dynamic simulation should perform some interpretations and presentations of the output generated by the simulator. The purpose of this paper is to assess batch process safety by evaluating critical safety objects. An assessment is conducted by using a dynamic simulation that provides engineering data and a pseudo of real process. The simulation results show the process variable in time series data. The main focus of this study is the loss of containment (LOC) incident. This incident leads to fires and explosion. Based on

* Correspondent author: rizal@syslab.sys.okayama-u.ac.jp

the newest data, LOC occurred mostly during normal operations (Collins & Keeley, 2003). An integrated evaluation should be developed to support safety management in batch chemical industries by evaluating safety objects (devices). Safety objects prevent and mitigate the hazards, e.g. sensors, valves, cooling water pump are considered as safety objects that capable in handling deviations during normal operations.

2. Methodologies

This part contains the methodologies in evaluating the safety objects, start from designing and running the simulator using VM, developing scenario models by a fault tree analysis method and find the optimal policy for safety design by estimating the importance of safety measures using probabilistic method.

2.1 Dynamic simulator

The dynamic simulations are often used for operator training, process design, safety system analysis or design and control system design. The dynamic simulator user interface can be seen in Fig. 1

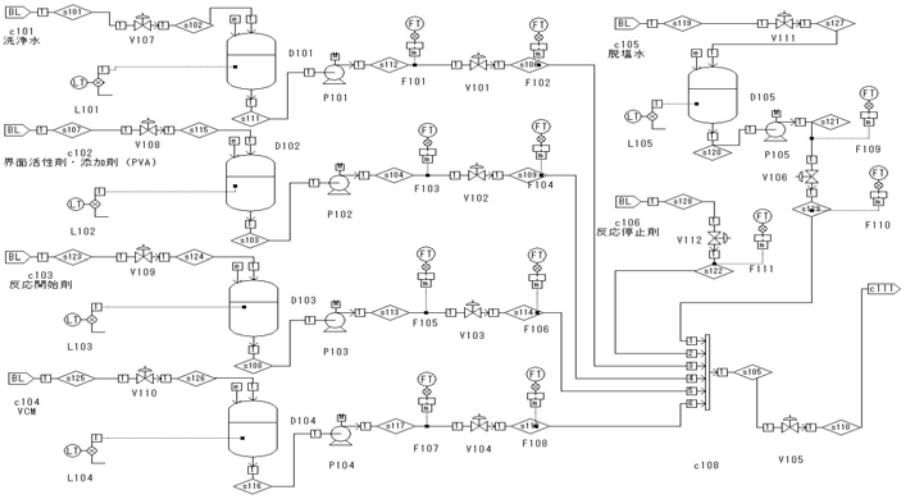

Figure 1. Batch dynamic simulator diagram using VM

Dynamic simulator was developed using the process dynamic. Model and simulation was verified using recipe phase from a PVC industry in Japan. The results of simulation have been checked and validated with the real plant.

The examples for safety object model are presented, the flow rate through control valve and sensor instrument reading can be modelled:

$$F_{CV} = C_V f(x) \sqrt{\frac{\Delta P}{sg}} \tag{1}$$

$$\frac{dT}{dt} = (T_{real} - T_{reading}).const \tag{2}$$

2.2 Scenario model based on fault tree analysis

Dynamic simulation provides a large amount of process variable data. The data should be analyzed to support the safety management level. The concept of scenario is a description of an expected situation, and the there is a reasonable probability that it would occur (Khan and Abbasi, 2002). Fault tree analysis (FTA) and event tree analysis (ETA) are widely used for analyzing complex components and systems, especially in identifying system interrelationships. FTA method is chosen for this study, because of FTA can be used to investigate causes that eventually lead to an undesired consequence (top event). FTA describes the scenario model for LOC based on simulated process data. A group of qualitative data can be structured and developed to obtain the building block of FTA. In order to perform the safety analysis for chemical plants, it is necessary to have an estimation of top event probability. The results of safety analysis support the optimal policy for safety design and process, for example to minimize the probability of accidents, industries should follow recommendation in maintenance, replacement and rearrangement of safety objects. A quantification method for FTA using minimum cut set (MCS) method can be described as follows:

$$P(TE) = \sum_{i=1}^{n} P(MCS_i) - \sum_{i<j} P(MCS_i \cap MCS_j) + \sum_{i<j<k} P(MCS_i \cap MCS_j \cap MCS_k) - \ldots + (-1)^{n-1} \prod_{i=1}^{n} P(MCS_i) \quad (3)$$

Minimum cut set (MCS) is a set of primary events, that is of basic or undeveloped faults, which can give rise to the top event (TE):

$$P(MCS_i) = \prod_{j=1}^{m} P(BE_j) \quad (4)$$

In the FTA, it is possible to simulate a condition that is assumed to exist as a boundary condition using house of event (CCPS, 1989), and an event simulated can be switched on and off to develop the appropriate scenario branches. For each of house of event is set to Boolean status T (true) or F (false). The switch signal can be generated as the function of time, yields dynamic analysis for systems. Cepin and Mavko (2002) introduced house event matrix that covers a condition to be timely switch on and off.

2.3 Performance index (PI)

This part can be used to support safety and risk management to evaluate the importance of components and parameters influencing the performance of a system. Result of the analysis will assist design stage to modifying and improving the system. The established method to estimate PI is Fussell-Vesely (I_{PV}). I_{PV} shows the same result with the Risk reduction worth (RRW) method. The I_{PV} can be explained as follow

$$I_{PV\,BE_j} = \frac{P(TE) - P(TE)_{P(BE_j)=0}}{P(TE)} \quad (5)$$

I_{PV} considers the ratio of the probability of the union of all MCS containing the BE_j, divided by the probability of the union of all MCS. In the other word, the numerator is

replaced by probability of TE minus probability of TE when the probability of occurrence of the basic event of interest is set to zero and the denominator is probability of occurrence of the TE.

3. Case study

This method is implemented for LOC at polymerization batch process, the two main causes of LOC are runaway temperature and overflow (Collins & Keeley, 2003). Reported by an industry that temperature at reactor lead to 383 K, this temperature was exceeded than normal temperature during process, however cooling process did not help much, and reaction began to runaway and pressure in the reactor rose to 324 – 379 kPa. It is known that a runaway reaction leads to LOC. The simulation result for runaway can be seen in Fig. 2

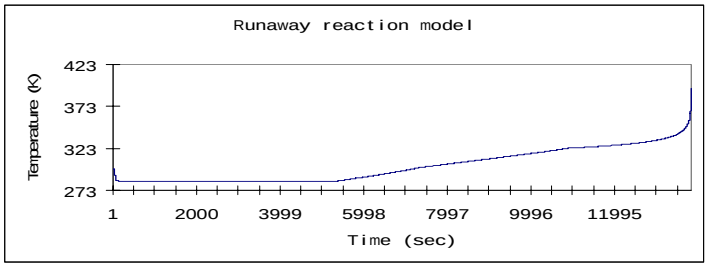

Figure 2. Runaway reaction model

Some results of the simulation show the importance of safety objects in mitigating the chain of events from BE. We consider instrumentation devices (flow, temperature) and control valves (automatic and manual) and cooling water pump as the objects under study. The qualitative analysis result after implementation of rule base mechanism shows the fault propagation model that can be shown in Table 1.

Table 1. Example of fault propagation model using dynamic simulator output with high flow deviation triggered

HET	Trigger	SF-117	V-104	SF-118	V-105	S-110	LOC
T	P-104:H	high	open	high	open	high	**yes**
T	P-104:H	high	(cont:F)	high	open	high	**yes**
T	P-104:H	not detect	open	high	open	high	**yes**
T	P-104:H	not detect	open	high	(cont:F)	high	**yes**
T	P-104:H	not detect	open	not detect	open	high	**yes**
T	P-104:H	not detect	open	not detect	open	high	**yes**
.....	.....	.....	.....	.....	.....	.....	.....

Based on qualitative analysis, we implement FTA, this graph can be shown in Fig. 3

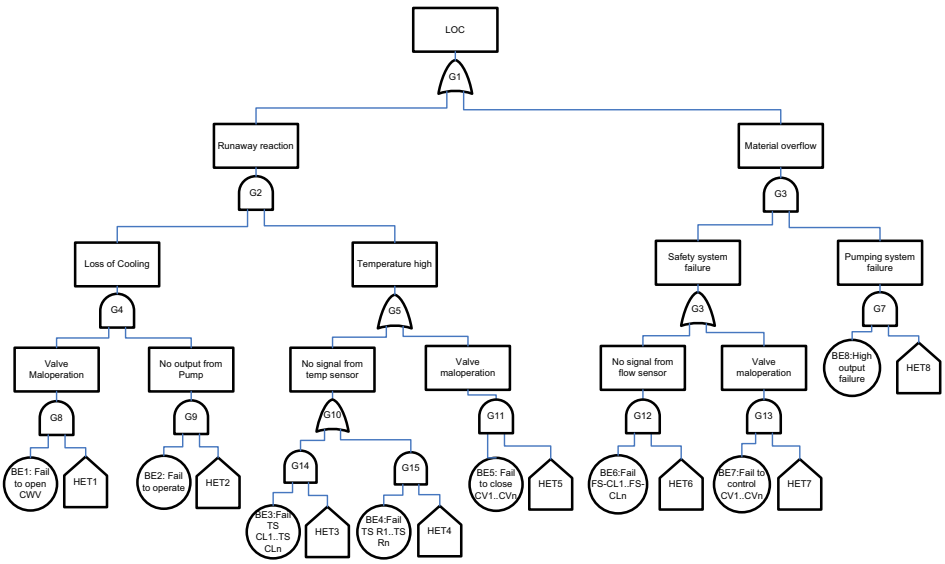

Figure 3. FTA based on qualitative analysis

Considering the FTA in Fig.3, it can be seen on the right hand side (RHS), overflow material (G3) contributes to LOC. P(G3)=P(G6) AND P(G7), or P(G3)=(P(G12) OR P(G13)) AND P(G7). The MCS can be obtained automatically from reliability block diagram of the systems and generates the MCS and their unavailability:

- $MCS_1=[(BE_8,HET_8),(BE_6,HET_6)] = 2.88 \times 10^{-11}$
- $MCS_2= [(BE_8,HET_8),(BE_7,HET_7)] = 1.4 \times 10^{-11}$
- $MCS_3= [(BE_1,HET_1),(BE_5,HET_5)] = 4.05 \times 10^{-10}$
- $MCS_4= [(BE_1,HET_1),(BE_3,HET_3)] = 3.42 \times 10^{-10}$
- $MCS_5 =[(BE_1,HET_1),(BE_4,HET_4)] = 2.1 \times 10^{-9}$
- $MCS_6 =[(BE_2,HET_2),(BE_3,HET_3)] = 2.1 \times 10^{-9}$
- $MCS_7= [(BE_2,HET_2),(BE_4,HET_4)] = 2.1 \times 10^{-9}$
- $MCS_8= [(BE_2,HET_2),(BE_5,HET_5)] = 2.48 \times 10^{-9}$

The redundancy safety objects can be simulated by AND gate for every MCS. After estimating the MCS, we can simulate the unavailability of TE by the combination of MCS, it is obtained about 9.56×10^{-9}.

3.1 Simulator triggering effect

The concept of HET promotes a better understanding of the process. Simulator can be used to investigate the effects of triggering signal to safety condition in plants especially, in evaluating safety objects. Assuming the BE_n in MCS is set to be exist, the minimum triggering signal (MTS) can be determined as MTS=[*(HET_8,HET_6); HET_8,HET_7); (HET_1,HET_5);(HET_1,HET_3);(HE_1,HET_4);(HET_2,HET_3);(HET_2,HET_4);(HET_2,HET_5)*].The configuration of MTS will be important for time dependent failures analysis and partial analysis of the systems by timely switching on/off.

3.2 PI rank

The purpose of PI rank is to give an indication in considering improvement program by selecting critical safety objects that contribute significantly to the TE by its presence.

The rank of BE based on I_{FV} and RRW can be seen in Table 2.

Table 2. Indices of FV –RRW and rank of each safety objects

	FV index	RRW index	Rank
BE_1	0.297	1.423	4
BE_2	0.698	3.311	1
BE_3	0.255	1.342	5
BE_4	0.439	1.782	2
BE_5	0.301	1.431	3
BE_6	0.003	1.003	7
BE_7	0.001	1.001	8
BE_8	0.004	1.004	6

From Table 2., BE_2 (failure of pump) and BE_4 (failure of temperatures sensor) are considered to investigate because these objects have highest rank among others.

3.2.1 Dynamic analysis using simulator

Dynamic simulator simulates time dependent of hazardous situation. The HET can be switched on/off based on availability versus unavailability (probability of event exists at some specified time *t*) function. Therefore HET contributes to the changes of the system configuration. It will reduce the complexity and time in analyzing the hazardous situation and safety objects when HET set to off (0 or false) condition because of the high availability of safety objects at time *t*. The other advantage is PI rank can be managed timely dependent, since MCS will depend on BE and HET. The result gives the optimal policy for improvement and maintenance activities of safety objects.

4. Conclusion

The process dynamic simulation was developed to evaluate the safety objects and to support the optimal policy for improvement the systems availability. Dynamic simulator provides a pseudo process that can be utilized to understand the propagation of fault and generate the credible accident scenarios for processes. The ideas of this paper have been successfully tested in PVC batch plant. Process dynamic analysis results are translated into process safety analysis to get the PI rank and this results can be considered as valuable input to safety design stage for a chemical process system engineering.

References

CCPS, 1989, Guidelines for chemical process quantitative risk assessment, AIChE, New York

Cepin, M. and Mavko, B., 2002,A dynamic fault tree, Rlb.Eng.Sys.Saf., 75

Collins, A and Keeley, D., 2003,Loss of containment incident analysis, HSL, England

Khan, F.I. and Abbasi,S.A., 2002, A criterion for developing credible accident scenarios for risk assessment, Loss Prev.Proc.Ind., 16,1

Shacham, Brauner & Cutlip, 2000,Open architecture modelling and simulation in process hazard assessment,Comp.Chem.Eng,24

Srinivasan,R. and Venkatasubramanian,V., 1998,Multiperspective models for process hazards analysis of large scale chemical processes, Comp.Chem.Eng, 22