GROUP	H

EXHIBIT

17

NATIONAL TRANSPORTATION SAFETY BOARD
Investigative Hearing
Norfolk Southern Railway general merchandise freight train 32N
derailment with subsequent hazardous material release and fires,
in East Palestine, Ohio, on February 3, 2023

Agency / Organization

Norfolk Southern

Title

Safety and Reliability Analysis in Polyvinyl Chloride Batch Process

Docket ID: **DCA23HR001**

Journal of Hazardous Materials A137 (2006) 1309–1320

Journal of Hazardous Materials

www.elsevier.com/locate/jhazmat

Safety and reliability analysis in a *polyvinyl chloride* batch process using dynamic simulator-case study: Loss of containment incident

Datu Rizal [a,b,*], Shinichi Tani [a], Kimitoshi Nishiyama [a], Kazuhiko Suzuki [a]

[a] *System Analysis Laboratory, Department of Systems Engineering, Okayama University, 3-1-1 Tsushima Naka, Okayama-shi 700-8530, Japan*

[b] *Research Centre for Quality System and Testing Technology, Indonesian Institute of Sciences (LIPI), PUSPIPTEK, Indonesia*

Received 30 December 2004; received in revised form 25 April 2006; accepted 27 April 2006
Available online 6 May 2006

Abstract

In this paper, a novel methodology in batch plant safety and reliability analysis is proposed using a dynamic simulator. A batch process involving several safety objects (e.g. sensors, controller, valves, etc.) is activated during the operational stage. The performance of the safety objects is evaluated by the dynamic simulation and a fault propagation model is generated. By using the fault propagation model, an improved fault tree analysis (FTA) method using switching signal mode (SSM) is developed for estimating the probability of failures. The timely dependent failures can be considered as unavailability of safety objects that can cause the accidents in a plant. Finally, the rank of safety object is formulated as performance index (PI) and can be estimated using the importance measures. PI shows the prioritization of safety objects that should be investigated for safety improvement program 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, the plant simulator, developed by Omega Simulation Corp., Japan). A case study is focused on the loss of containment (LOC) incident at *polyvinyl chloride* (PVC) batch process which is consumed the hazardous material, *vinyl chloride monomer* (VCM).

© 2006 Elsevier B.V. All rights reserved.

Keywords: Dynamic simulator; Safety; Performance index; Fault propagation; Batch process

1. Introduction

Plant safety and reliability are the significant issues in the increasing public acceptability and worldwide market challenges for batch chemical industries (BCI). Particularly, there is a highly demand on the PVC products, since they are relatively inexpensive to manufacture and tended to replace more conventional material such as metal, wood, or leather in a wide variety of products. It has been shown that BCI are more prone to error to safety incidents [1]. As the consequence, BCI should improve safety and reliability aspects at the design stage as well as operational stage. At plant design stage, potential of hazardous situation are clarified and causal relationship between causes and effects are investigated [2]. Based on this issue, the use of dynamic simulator is essential to envisage the future situation and predict the possible hazardous outcomes. Nowadays, the dynamic simulator has been extensively used for operator training, operational design and safety purposes. However, it still needs improvement to achieve the comprehensive safety analysis by integrating the simulator with safety and reliability tools. Simulation practices are widely used to provide quantitative measures to assess fault propagation and abnormal situation [3].

The aim of this article is to assess the hazardous condition (LOC) in the PVC batch plant using improved dynamic simulator, the simulation result is incorporated to the fault propagation analysis. Then, the credible safety assessment can be performed using fault tree analysis and importance measures. The safety assessment is conducted by evaluating critical safety objects. The groups of safety objects are installed in the plant for detecting, preventing and mitigating the hazard. From this point of view, it is important to guarantee all safety objects are working in high performance. This is an essential point, because it is known that during PVC production, the hazardous material (VCM) is consumed and reacted to produce PVC. Therefore, the hazard prevention should be implemented to avoid such consequences.

This paper also proposes a novel approach in implementing batch process safety assessment. A safety object is considered

[*] Corresponding author. Tel.: +81 86 251 8059; fax: +81 86 251 8059.
E-mail address: rizal@syslab.sys.okayama-u.ac.jp (D. Rizal).

0304-3894/$ – see front matter © 2006 Elsevier B.V. All rights reserved.
doi:10.1016/j.jhazmat.2006.04.052

Nomenclature

$\bar{a}_i$	unavailability of repairable basic event
$\bar{A}_j$	unavailability of minimum cut set j
$\bar{A}_\mathrm{T}$	unavailability of top event
BE	basic event
cont:F	controlled by flowrate
cont:T	controlled by temperature
C_v	valve coefficient
d	fraction of valve opening
f	flowrate
F	false
FTA	fault tree analysis
$h(d)$	flow characteristic as function of d
I_FV	Fussell–Vesely index
ISA	Instrument Society of America
LOC	loss of containment
MCS	minimum cut sets
ΔP	pressure drop across valve
$P(\mathrm{BE})$	probability of basic event
$P(F_\mathrm{SO})$	probability of failure for safety object
$P(F_\mathrm{SS})$	probability of failure for subsystem
$P(F_\mathrm{SS}[T_n])$	probability of failure for subsystem at sequence n
$P(\mathrm{TE})$	probability of top event
PFOD	probability of failure on demand
PI	performance index
PV	process variable
sg	specific gravity of material
S	sensor point
SF	sensor-flowrate (flow sensor)
SO_n	safety object n-th
SSM	switching signal mode
ST	sensor-temperature (temperature sensor)
T	true
T_i	test interval for basic event i
TE	top event
V	valve

Greek letters

Ω	valve constant
λ_i	failure rate for basic event i
τ_i	repair time for basic event i

as a critical device which should be inspected by monitoring the process variables. It produces the numerical result of simulation which can be used for further safety investigation. Since the process is in the batch mode, a particular treatment of safety analysis is required by incorporating the process scheduling in a period of time.

The dynamic simulation of batch chemical process is being importantly used for quantitative hazard assessment [4] and is a powerful tool to analyze unsteady state behavior of the chemical process and can be used in all stage of process engineering activities such as process design, operation, control and automation. The dynamic simulation is a very important component of process hazard analysis, since it can quantitatively predict the consequences of critical component failures [5]. Several hazard assessment methods have been established and connected to the dynamic simulation. The dynamic simulation must perform some interpretation and presentation of the output generated by the simulator.

The main focus of this study is the loss of containment (LOC) incident. This incident causes the fires and explosion. Based on the newest data, LOC occurred mostly during normal operations [6]. 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. In this paper, sensors, valves, cooling water pump are considered as safety objects that capable in handling deviations during operational stage.

2. Methodologies

This part contains the methodologies in plant safety and reliability analysis using simulator. It is started from designing and running the simulator using VM, developing scenario models by using a fault propagation analysis [7–9] and a fault tree analysis method and finding the optimal policy for safety design by estimating the importance of safety measures using Fussell–Vesely method.

2.1. Dynamic simulator

2.1.1. Conceptual design of batch process

A simulator for batch process is effectively designed by using the object-oriented methodology based on the ISA S88 standard on batch control design. This is a worldwide standard which has been applied for a reference in a batch plant design. Naturally, ISA S88 described the model in object-oriented schema. ISA S88 divided a plant structural information with procedural and control model [10]. However, it was only effectively manage the batch process to achieve the high quality product. A batch structural model is divided into process cell, unit, equipment module and control module. Each level represents the specific boundaries of equipment starting from a wide group area (process cell) to a smallest group (control module). A process model can be described in hierarchical level, starting from (i) process stage, (ii) process, (iii) process operation and (iv) process action. Another classification is applied to procedural control model, which consists of (a) procedure, (b) unit procedure, (c) operation and (d) phase. The model of ISA S88 introduced the integrated strategy for performing batch process. This model could manage the complex structure in a simple and a realistic way. The smallest part of the model such as a phase or a process action covers the detail processes, therefore, complete analysis could be done in this level [11].

The general framework of modeling using ISA S88 consists of physical, procedural, process and recipe model. ISA S88 explored the relationship of the models and describes the process objectives in a batch plant. A procedural model combines the physical entities to perform the process. The process objec-

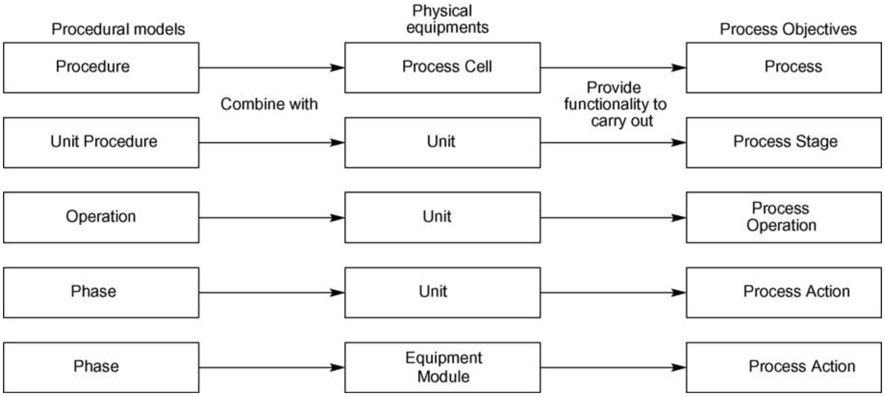

Fig. 1. Procedural model and physical equipment mapping to achieve process objectives [10].

tives can be achieved by implementing the detail procedures to the specific equipments. A safety designer should consider the model framework to construct safety environment and to design the safety aspect parameter. The relationship among the models in ISA S88 can be seen in Fig. 1.

In Fig. 1, it can be seen that the lowest level (phase, equipment module and process action) has an important role in performing safety aspect in the plant operations. The phase level is associated with process-oriented tasks, some examples of phases can be:

- add material;
- heat up;
- agitate.

In the phase level, the instructions should be executed by a equipment module level or a unit level. The equipment module is defined as a functional group of equipment performs a finite number of the specific minor processing activities. An equipment module consists of components performing one or more specific functions and an equipment module may be made up of control modules or other equipment modules. A combination of a phase and an equipment module can execute the process action. The process actions represent minor processing activities that are combined to make up a process operation. Examples of process actions as follows:

- heat material in reactor to 60 °C;
- open valve V-3123 for steaming the reactor;
- hold the reactor temperature about 60 °C until the pressure decrease.

When the process action is executed, a batch process is activated and the state of equipment changes. We introduced the switching signal model (SSM) which can cover the change of batch status. The detail description of SSM in managing batch will be discussed in Section 3.2.

2.1.2. Process dynamic design

The main part of simulator is a knowledge based containing algorithm and data needed to calculate the processes, therefore, mathematical modeling and simulation are valuable tools for quantitative safety investigation [12].

This paper will be focused on the VCM charging line which is the most hazardous line and connected to the polymerization reactor. VCM is identified as colourless gas with empirical formula C_2H_3Cl [13]. VCM is also known as carcinogen and explosive gas. VCM charging line can be drawn in Fig. 2.

VCM gas is loaded from tank truck into the vessel (loading process), after that gas is stored in vessel for a temporary time. Gas in vessel is charged to the reactor through VCM charging line. Several safety objects are implemented to prevent from hazardous condition. For example, when a problem occurs in pump P-110 and causes high output, therefore, flowrate of material will escalate and several safety problems arise.

Therefore, process dynamic design should consider the process variables of the hazardous material such as flow, level, temperature, pressure, etc., these variables are controlled under safety objects (sensors, controllers, valves, pumps, etc.). Here, for the case study, process dynamic design for the valve systems in controlling material flow is presented. The flow through valve can be described as follows [14]:

$$f = C_{\mathrm{v}} h(d) \sqrt{\frac{\Delta P}{\mathrm{sg}}} \tag{1}$$

while ΔP, C_{v} for each valve, sg of VCM are obtained from component specification, however, $h(d)$ for equal percentage valve

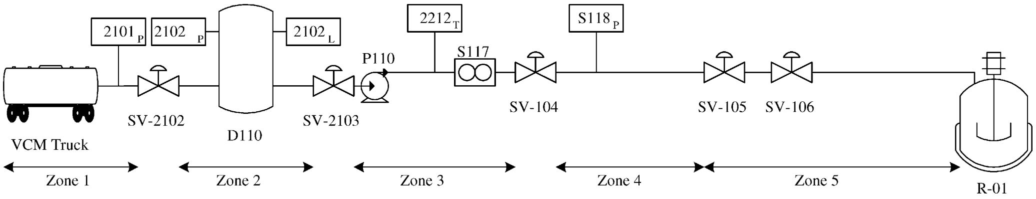

Fig. 2. Overview of VCM charging line.

type can be modeled as follows [14]:

$$h(d) = \Omega^{d-1} \tag{2}$$

For flow-valve position relationship can be expressed as follows [14]:

$$f = C_{\mathrm{v}}\Omega^{d-1}\sqrt{\frac{\Delta P}{\mathrm{sg}}} \tag{3}$$

in logarithmic form, Eq. (3) will be:

$$\log[f] = \log\left[C_{\mathrm{v}}\Omega^{d-1}\sqrt{\frac{\Delta P}{\mathrm{sg}}}\right] \tag{4}$$

assuming $\log\Omega=\Omega_0$, C_{v}, ΔP and sg are constant, d can be obtained as follows:

$$d = \frac{1}{\Omega_0}\log\left[\frac{f}{C_{\mathrm{v}}}\sqrt{\frac{\mathrm{sg}}{\Delta P}}\right]+1 \tag{5}$$

The valve position d will vary between 0 and 1, flow through valve f should represent the ideal/safety value for zone 5. The correlation between d and f can be simulated and shown in Fig. 3. Information from the equation can be used to manipulate an object (a valve) performance index.

The mathematical equations are implemented for each component, for example, the above equations describe the valve characteristic in controlling material flow. The parameters and constants are adjusted to the operational stages constrain.

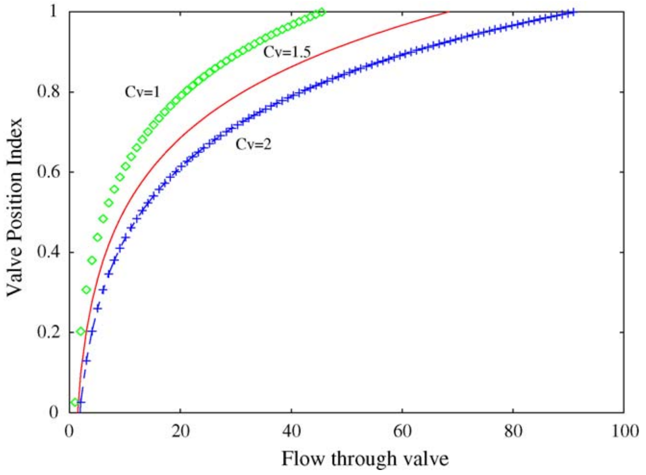

Fig. 3. Simulation of valve position index in controlling material flow.

2.1.3. Development of batch dynamic simulator

The dynamic simulations are often used for operator training, process design, safety system analysis or design and control system design. The charging part of PVC batch process and polymerization reactor can be modeled using dynamic simulator user interface can be seen in Figs. 4 and 5.

In batch process, scheduling has an important role in controlling the process actions based on procedure and time sequence. After one task is completed in a slot of time, another task will be processed. For each task, process variables are detected and controlled by the safety objects. In order to implement the safety and reliability analysis, it is essential to record process variable data, which can be used for scenario model development using fault tree analysis method.

The dynamic simulator provides the real time graphics for simulation results. During simulation, all the data from sensor

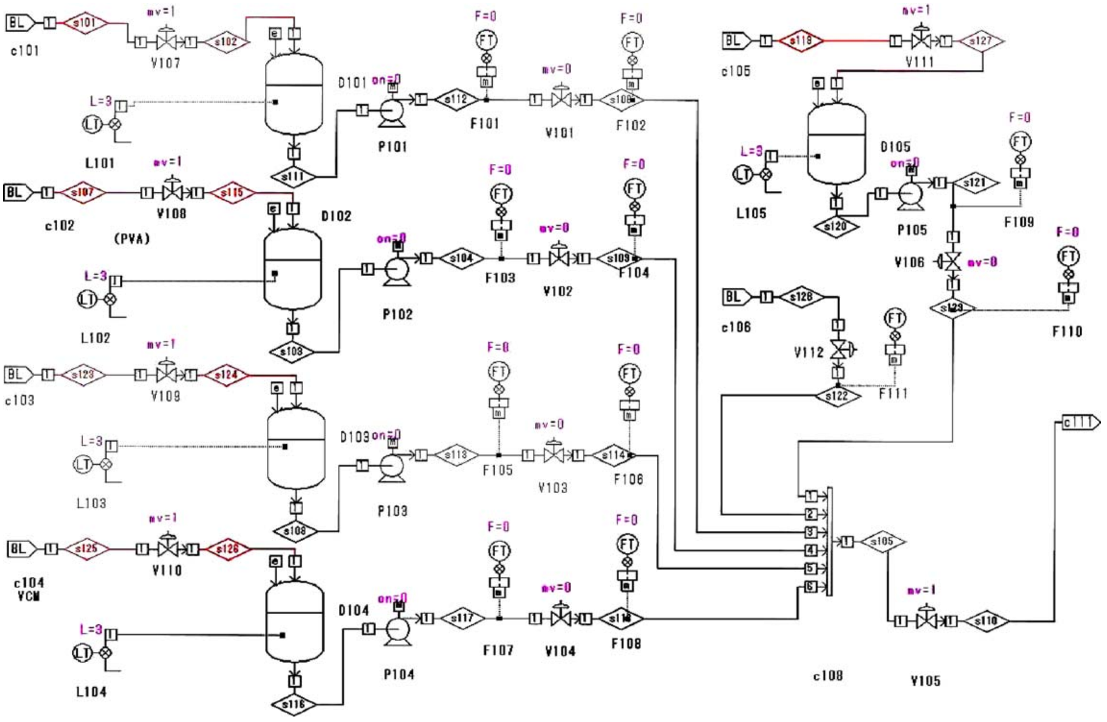

Fig. 4. Charging line part of PVC plant diagram using VM.

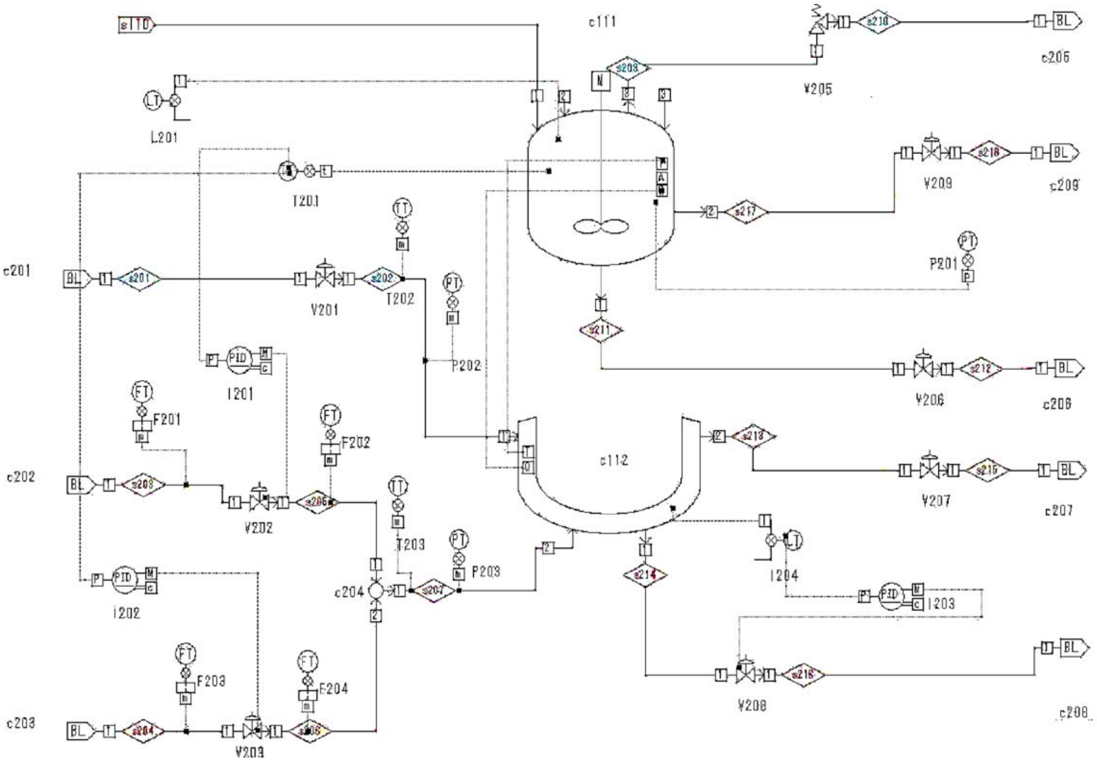

Fig. 5. Reactor part of PVC plant diagram using VM.

is sent in numerical results to the spreadsheet software. Based on the batch plant behavior, the results are sent by following the sequence of task, from the first to the final task. The results are recorded and can be used for further investigation. The example of results of the simulation for temperature inside the reactor can be seen in Fig. 6

Fig. 6 shows that the temperature inside the reactor which is divided into three zones: (i) charging task, it reflects the beginning part of process when materials are charged to the reactor, (ii) heat up, it is indicated with increasing of temperature by steaming the reactor, finally, (iii) reaction task, during this step, temperature is maintained in between 50 and 60 °C by charging the cooling water, it is shown by sinusoidal wave in zone III which represents the up-down of temperature by heating and cooling transition.

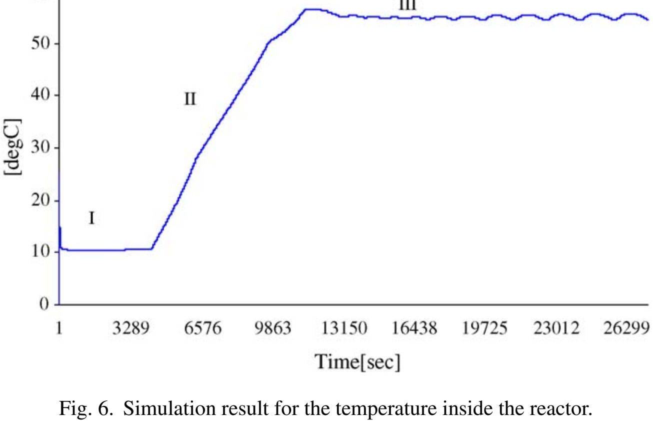

Fig. 6. Simulation result for the temperature inside the reactor.

3. Scenario model based on fault tree analysis

3.1. Developing the scenario model

Dynamic simulation provides a large amount of process variable data. The VM transfers the simulation result to a spreadsheet program. By using a spreadsheet, it is simple to simulate the data for the next purposes. The data should be analyzed to support the safety management level in developing the scenario. The concept of scenario is a description of an expected situation, and the there is a reasonable probability that it would occur [15]. 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 it can be used to investigate the causes that eventually create 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 process safety design, for example to minimize the probability of accidents, industries should follow the related recommendation in maintenance, replacement and rearrangement of safety objects. In order to develop the credible

FTA by using dynamic simulator, there are several steps which will be described as follows:

- *Step 1*: *define the system and context*, this is an essential step since an understanding of the system and context of the failures, causes and the relationships with consequences, including the understanding of:
  - safety objects and the specification;
  - batch topology and structure;
  - batch procedure (recipe) and operational model;
  - logical link among failures, causes, consequences and fault propagation.
- *Step 2*: *construct the fault propagation table based on the simulation results*, this step describes the mapping from numerical results into qualitative analysis using IF-THEN rules:

  $$\text{IF}\,\{\text{PV} \neq \text{PV}_{\text{recipe}}\}\ \text{AND}\,\{\text{time} > t_{\text{critical}}\}\ \text{THEN}\,\{\text{Condition}\} \tag{6}$$

  For example:

  $$\text{IF}\,\{\text{temp} > \text{temp}_{\text{THRESHOLD}}\}\ \text{AND}\,\{\text{time} > 1\ \text{minute}\}\ \text{THEN}\,\{\text{temp is high}\}$$

  The above rule is an example that can be implemented to convert the numerical results (temperature measurement) into qualitative variables (*high temperature*). This example describes how the *high temperature* occurred due to sensor system detected temperature in one point, higher than the threshold and the duration time at this level is longer than 1 min. This rule is effective and efficient in mapping and simulating the numerical result into qualitative measurement for fault propagation analysis. IF-THEN rules create the intelligent decision for the states in batch plant using variable status. The list of variable status of safety objects can be seen in Table 1.
- *Step 3: identify the hazard, hazard identification can be reasoned using fault propagation table*, this step is also simulated by IF-THEN rules:

  $$\text{IF}\,\{\text{Condition at SO}_1\}\ \text{AND}\,\{\text{Condition at SO}_2\}\ldots\text{AND}\ \{\text{Condition at SO}_n\}\ \text{THEN}\,\{\text{Hazard}\} \tag{7}$$

  while, $\text{SO}_1\cdots\text{SO}_n$ (safety objects) are the safety objects in the phase level, for example:

  IF {flow at SF-117 is high} AND {temp at V-104 is open} ... AND {flow at S-110 is high} THEN {LOC}

  The above rule describes the example of hazard identification by reasoning the condition of safety objects using fault propagation. The example shows that LOC may occur after specific conditions are treated at the safety objects.
- *Step 4*: *develop the FTA based on the fault propagation table*, then expand FTA up to the basic events and incorporate the house of event. The house of event becomes a valuable tool for reducing the complexity of FTA, the house of event is expressed in SSM and will be explained more detail in Section 3.2. By using the FTA method, it is possible to simulate a condition that is assumed to be exist as a boundary condition using house of event [16], and an event simulated can be switched on and off to develop appropriate scenario branch. 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 [17]. In this study, the simulated SSM performs the time dependent failure of occurrence of BE. P(TE) can be estimated as a function of successful (T) of SSM in minimum cut set part.

Table 1
List of variable status of safety objects

Safety objects	Possible status
Flow sensor	Normal
	Very high
	High
	Low
	Very low
	No
	Not detect
Control valve	Open
	Close
	Control:T
	Control:F
Safety decision	Yes
	No
Temperature sensor	Normal
	Very high
	High
	Low
	Very low
	Not detect
Level sensor	Normal
	High
	Low
	Empty
	Not detect
Pressure sensor	Normal
	High
	Very high
	Low
	Very low
	Not detect

- *Step 5*: *find the minimum cut set (MCS)*, a quantification method for FTA using minimum cut set (MCS) method can be described as follows [16]:

$$P(\text{TE}) = \sum_{i=1}^{n} P(\text{MCS}_i) - \sum_{i<j} P(\text{MCS}_i \cap \text{MCS}_j) + \sum_{i<j<k} P(\text{MCS}_i \cap \text{MCS}_j \cap \text{MCS}_k) - \cdots + (-1)^{n-1}\prod_{i=1}^{n} P(\text{MCS}_i) \tag{8}$$

MCS is a set of primary events, that is of basic or undeveloped faults, which can contribute to the top event (TE) [16]:

$$P(\mathrm{MCS}_i) = \prod_{j=1}^{m} P(\mathrm{BE}_j) \tag{9}$$

- *Step 6*: *estimate the probability of occurrence of MCS*, MCS is the combination of BE, therefore, probability of occurrence each MCS is important for estimating the occurrence of TE. At first, the unavailability of repairable basic event can be estimated as follows [16]:

$$\bar{a}_i = \frac{\lambda_i \tau_i}{1+\lambda_i \tau_i}[1 - \mathrm{e}^{(-\lambda_i + 1/\tau_i)t}] \tag{10}$$

where λ_i represents the failure rate of basic event, τ_i is the repair time, and for non-repairable basic event, the probability of failure on demand (PFOD) can be estimated as follows [16]:

$$\mathrm{PFOD} = \frac{1}{T_i}\int_0^{T_i} \bar{a}_i(t)\,\mathrm{d}t \tag{11}$$

where T_i represents test interval for BE_i, after that, the unavailability of MCS can be calculated as follows [16]:

$$\bar{A}_j = \prod_{i=1}^{n_j} \bar{a}_i \tag{12}$$

and the PFOD of MCS can be shown by [16]:

$$\mathrm{PFOD}_j = \frac{1}{T}\int_0^{T} \bar{A}_j(t)\,\mathrm{d}t \tag{13}$$

- *Step 7: estimate the unavailability of TE*, this is given by [16]:

$$\bar{A}_T = \sum_{j=1}^{n_j} \bar{A}_j \tag{14}$$

These steps describe the numerical simulation of FTA and the results for plant safety and reliability improvement can be obtained.

3.2. Dynamic analysis using simulator

A dynamic simulator simulates time dependent of hazardous situation. For the batch process, each task is activated based on the time sequence. Time sequence is modeled by switching the on (1) and off (0). The dynamic simulator generates the switching signal mode (SSM) to activate or deactivate the process. Therefore, SSM contributes to the system configuration changes. It reduced the complexity in analyzing the hazardous situation when SSM set to off (0 or false) condition, because the safety objects at time *t* are non-activated. The other advantage is PI rank can be managed timely dependent, since MCS depends on BE and SSM. The result gives the optimal policy for improvement and maintenance activities of safety objects.

Generally, the batch process is conducted by activating the tasks. These tasks are implemented using SSM which naturally describes the process task execution based on time sequence. The SSM model for one batch is shown in Fig. 7.

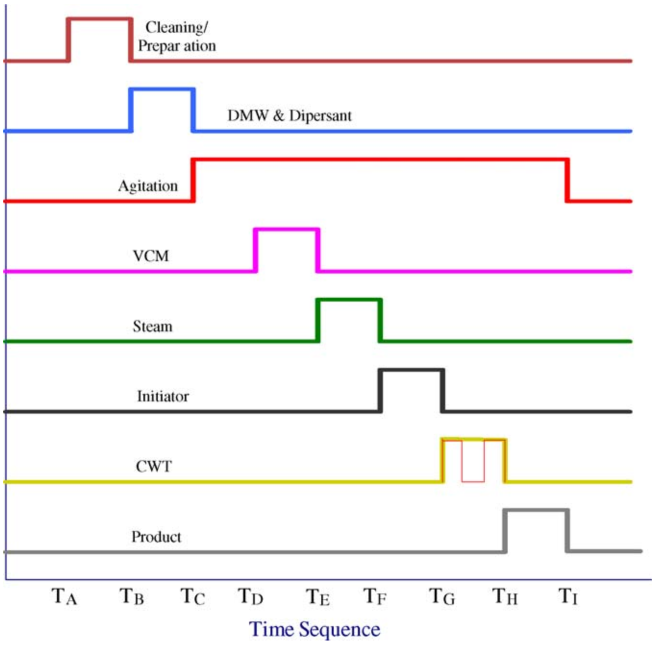

Fig. 7. Switching signaling mode for PVC batch process.

From Fig. 7, we generate the characteristic of the processes which can be described by process matrix (PM). PM for a batch product may differ from other products. Thus, PM can be adaptively modeled and designed as a tool for safety and reliability analysis in a batch process. The example of PM can be seen as follows:

$$\mathrm{SSM}_1 = \begin{bmatrix} P_{\mathrm{Aa}} & P_{\mathrm{Ab}} & P_{\mathrm{Ac}} & P_{\mathrm{Ad}} & P_{\mathrm{Ae}} & P_{\mathrm{Af}} & P_{\mathrm{Ag}} & P_{\mathrm{Ah}} & P_{\mathrm{Ai}} \\ P_{\mathrm{Ba}} & P_{\mathrm{Bb}} & P_{\mathrm{Bc}} & P_{\mathrm{Bd}} & P_{\mathrm{Be}} & P_{\mathrm{Bf}} & P_{\mathrm{Bg}} & P_{\mathrm{Bh}} & P_{\mathrm{Bi}} \\ P_{\mathrm{Ca}} & P_{\mathrm{Cb}} & P_{\mathrm{Cc}} & P_{\mathrm{Cd}} & P_{\mathrm{Ce}} & P_{\mathrm{Cf}} & P_{\mathrm{Cg}} & P_{\mathrm{Ch}} & P_{\mathrm{Ci}} \\ P_{\mathrm{Da}} & P_{\mathrm{Db}} & P_{\mathrm{Dc}} & P_{\mathrm{Dd}} & P_{\mathrm{De}} & P_{\mathrm{Df}} & P_{\mathrm{Dg}} & P_{\mathrm{Dh}} & P_{\mathrm{Di}} \\ P_{\mathrm{Ea}} & P_{\mathrm{Eb}} & P_{\mathrm{Ec}} & P_{\mathrm{Ed}} & P_{\mathrm{Ee}} & P_{\mathrm{Ef}} & P_{\mathrm{Eg}} & P_{\mathrm{Eh}} & P_{\mathrm{Ei}} \\ P_{\mathrm{Fa}} & P_{\mathrm{Fb}} & P_{\mathrm{Fc}} & P_{\mathrm{Fd}} & P_{\mathrm{Fe}} & P_{\mathrm{Ff}} & P_{\mathrm{Fg}} & P_{\mathrm{Fh}} & P_{\mathrm{Fi}} \\ P_{\mathrm{Ga}} & P_{\mathrm{Gb}} & P_{\mathrm{Gc}} & P_{\mathrm{Gd}} & P_{\mathrm{Ge}} & P_{\mathrm{Gf}} & P_{\mathrm{Gg}} & P_{\mathrm{Gh}} & P_{\mathrm{Gi}} \\ P_{\mathrm{Ha}} & P_{\mathrm{Hb}} & P_{\mathrm{Hc}} & P_{\mathrm{Hd}} & P_{\mathrm{He}} & P_{\mathrm{Hf}} & P_{\mathrm{Hg}} & P_{\mathrm{Hh}} & P_{\mathrm{Hi}} \end{bmatrix} \tag{15}$$

and the PM for Fig. 7 is

$$\mathrm{SSM}_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

SSM_1 is a representation of a batch switching mode through sequence of time. The horizontal part represents a number of time sequences for a batch process which determines the activation period of the systems. The vertical part contains a number of batch tasks (phases) for one batch cycle. For example,

$\{P_{\mathrm{Aa}}, P_{\mathrm{Ab}}, \ldots, P_{\mathrm{Ai}}\}$ are the parameters of activation for preparation/cleaning task in time sequences $\{T_a, T_b, \ldots, T_i\}$. SSM_1 describes the behavior of the certain process as a function of time sequence.

The simulator performs the process based on SSM, therefore, the complexity of the process and the hazards are managed by the matrix configuration. Since, the batch is a discontinuous process, SSM is important in order to obtain credible analysis of the batch process. In the other way, for a continuous process, SSM is not required due to all steps are steady state and relatively simple.

3.3. Integrating the scenario model and dynamic behavior

This section describes the integration between the scenario model and dynamic behavior in order to perform batch process safety analysis. The new approach is developed to evaluate the condition which covers the plant behavior. The method is designed by integrating the probabilistic safety assessment (PSA) and dynamic simulation. PSA method using FTA for developing scenario has been explained in Section 3.1. In this section, we intend to synchronize that scenario with the PM which is discussed in Section 3.2.

A complex batch process is divided to several phases/tasks, each task is recognized as a subsystem (SS) of the batch process system (S). The hazard in a batch system is identified in two categories—*single failure model*: this model represents that an initiating event generates the failures in a subsystem, the single failure model as a function of safety objects is expressed as

$$P(F_{\mathrm{SS}_n}) = P(F_{\mathrm{SO}_1}) \cap P(F_{\mathrm{SO}_2}) \cdots \cap P(F_{\mathrm{SO}_n}) \qquad (16)$$

to synchronize the failure in batch process, Eq. (16) should be integrated with PM:

$$P(F_{\mathrm{SS}_n}[T_n]) = P(F_{\mathrm{SS}_n}) \cap P(\mathrm{SSM}_n) \qquad (17)$$

while probability of failure for the batch system is

$$P(F_{\mathrm{S}}[T_n]) = P(F_{\mathrm{SS}}[T_n]) \qquad (18)$$

Eq. (18) represents a consequence or a top event that may occur if the fault propagates through the process. By considering this model, the failure of batch system can be evaluated, and failure configuration can be known. The failure configuration is significant for further investigation of the system—*multiple failure model*: this model is caused by a combination of initiating events. These events contribute to the failure of subsystems and systems. The multiple failure model is expressed in a task matrix (TM) that should be analyzed concurrently with the process matrix (PM):

$$P(F_{\mathrm{SS}}) = \mathrm{TM} \cap \mathrm{PM} \qquad (19)$$

$$P(F_{\mathrm{SS}}) = \begin{bmatrix} P_{\mathrm{SS_{Aa}}} & P_{\mathrm{SS_{Ba}}} & P_{\mathrm{SS_{Ca}}} & P_{\mathrm{SS_{Da}}} & P_{\mathrm{SS_{Ea}}} & P_{\mathrm{SS_{Fa}}} & P_{\mathrm{SS_{Ga}}} & P_{\mathrm{SS_{Ha}}} \\ P_{\mathrm{SS_{Ab}}} & P_{\mathrm{SS_{Bb}}} & P_{\mathrm{SS_{Cb}}} & P_{\mathrm{SS_{Db}}} & P_{\mathrm{SS_{Eb}}} & P_{\mathrm{SS_{Fb}}} & P_{\mathrm{SS_{Gb}}} & P_{\mathrm{SS_{Hb}}} \\ P_{\mathrm{SS_{Ac}}} & P_{\mathrm{SS_{Bc}}} & P_{\mathrm{SS_{Cc}}} & P_{\mathrm{SS_{Dc}}} & P_{\mathrm{SS_{Ec}}} & P_{\mathrm{SS_{Fc}}} & P_{\mathrm{SS_{Gc}}} & P_{\mathrm{SS_{Hc}}} \\ P_{\mathrm{SS_{Ad}}} & P_{\mathrm{SS_{Bd}}} & P_{\mathrm{SS_{Cd}}} & P_{\mathrm{SS_{Dd}}} & P_{\mathrm{SS_{Ed}}} & P_{\mathrm{SS_{Fd}}} & P_{\mathrm{SS_{Gd}}} & P_{\mathrm{SS_{Hd}}} \\ P_{\mathrm{SS_{Ae}}} & P_{\mathrm{SS_{Be}}} & P_{\mathrm{SS_{Ce}}} & P_{\mathrm{SS_{De}}} & P_{\mathrm{SS_{Ee}}} & P_{\mathrm{SS_{Fe}}} & P_{\mathrm{SS_{Ge}}} & P_{\mathrm{SS_{He}}} \\ P_{\mathrm{SS_{Af}}} & P_{\mathrm{SS_{Bf}}} & P_{\mathrm{SS_{Cf}}} & P_{\mathrm{SS_{Df}}} & P_{\mathrm{SS_{Ef}}} & P_{\mathrm{SS_{Ff}}} & P_{\mathrm{SS_{Gf}}} & P_{\mathrm{SS_{Hf}}} \\ P_{\mathrm{SS_{Ag}}} & P_{\mathrm{SS_{Bg}}} & P_{\mathrm{SS_{Cg}}} & P_{\mathrm{SS_{Dg}}} & P_{\mathrm{SS_{Eg}}} & P_{\mathrm{SS_{Fg}}} & P_{\mathrm{SS_{Gg}}} & P_{\mathrm{SS_{Hg}}} \\ P_{\mathrm{SS_{Ah}}} & P_{\mathrm{SS_{Bh}}} & P_{\mathrm{SS_{Ch}}} & P_{\mathrm{SS_{Dh}}} & P_{\mathrm{SS_{Eh}}} & P_{\mathrm{SS_{Fh}}} & P_{\mathrm{SS_{Gh}}} & P_{\mathrm{SS_{Hh}}} \\ P_{\mathrm{SS_{Ai}}} & P_{\mathrm{SS_{Bi}}} & P_{\mathrm{SS_{Ci}}} & P_{\mathrm{SS_{Di}}} & P_{\mathrm{SS_{Ei}}} & P_{\mathrm{SS_{Fi}}} & P_{\mathrm{SS_{Gi}}} & P_{\mathrm{SS_{Hi}}} \end{bmatrix} \cap \begin{bmatrix} P_{\mathrm{Aa}} & P_{\mathrm{Ab}} & P_{\mathrm{Ac}} & P_{\mathrm{Ad}} & P_{\mathrm{Ae}} & P_{\mathrm{Af}} & P_{\mathrm{Ag}} & P_{\mathrm{Ah}} & P_{\mathrm{Ai}} \\ P_{\mathrm{Ba}} & P_{\mathrm{Bb}} & P_{\mathrm{Bc}} & P_{\mathrm{Bd}} & P_{\mathrm{Be}} & P_{\mathrm{Bf}} & P_{\mathrm{Bg}} & P_{\mathrm{Bh}} & P_{\mathrm{Bi}} \\ P_{\mathrm{Ca}} & P_{\mathrm{Cb}} & P_{\mathrm{Cc}} & P_{\mathrm{Cd}} & P_{\mathrm{Ce}} & P_{\mathrm{Cf}} & P_{\mathrm{Cg}} & P_{\mathrm{Ch}} & P_{\mathrm{Ci}} \\ P_{\mathrm{Da}} & P_{\mathrm{Db}} & P_{\mathrm{Dc}} & P_{\mathrm{Dd}} & P_{\mathrm{De}} & P_{\mathrm{Df}} & P_{\mathrm{Dg}} & P_{\mathrm{Dh}} & P_{\mathrm{Di}} \\ P_{\mathrm{Ea}} & P_{\mathrm{Eb}} & P_{\mathrm{Ec}} & P_{\mathrm{Ed}} & P_{\mathrm{Ee}} & P_{\mathrm{Ef}} & P_{\mathrm{Eg}} & P_{\mathrm{Eh}} & P_{\mathrm{Ei}} \\ P_{\mathrm{Fa}} & P_{\mathrm{Fb}} & P_{\mathrm{Fc}} & P_{\mathrm{Fd}} & P_{\mathrm{Fe}} & P_{\mathrm{Ff}} & P_{\mathrm{Fg}} & P_{\mathrm{Fh}} & P_{\mathrm{Fi}} \\ P_{\mathrm{Ga}} & P_{\mathrm{Gb}} & P_{\mathrm{Gc}} & P_{\mathrm{Gd}} & P_{\mathrm{Ge}} & P_{\mathrm{Gf}} & P_{\mathrm{Gg}} & P_{\mathrm{Gh}} & P_{\mathrm{Gi}} \\ P_{\mathrm{Ha}} & P_{\mathrm{Hb}} & P_{\mathrm{Hc}} & P_{\mathrm{Hd}} & P_{\mathrm{He}} & P_{\mathrm{Hf}} & P_{\mathrm{Hg}} & P_{\mathrm{Hh}} & P_{\mathrm{Hi}} \end{bmatrix} \qquad (20)$$

The failure of the system can be estimated as follows:

$$P(F_{\mathrm{S}}[T_{\mathrm{S}}]) = \bigcup_{n=1}^{m} P(F_{\mathrm{SS}_n}[T_n]) \qquad (21)$$

The multiple failures model is constructed for at least two initiating events. A horizontal part of TM represents the probability of all subsystems in a period of time and a vertical part represents the probability of each subsystem for whole the processes. Multiple failures model shows how the initiating events can generate the multiple failures in the subsystem, and a combination of failures in a subsystem propagates and generates the failure of systems. It is known that T_n is the time sequence of a subsystem, and failure of systems are treated in a total time of related subsystems T_{S}.

The model can be used for estimating the performance of a system based on the simulation of switching on and off of the subsystems. It contributes to reducing the complexity of batch process without neglecting the nature of batch process in discontinuous type. This method offers a technique to manage the safety analysis in batch process which can give more advantages in estimating the performance index.

4. Performance index (PI) simulation

An advantage of using fault tree analysis is the importance for each components or each MCS [18]. 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. The result of the analysis will be used in design stage to modifying and improving the system. This measure was introduced by Vesely and followed by Fussell, the basic idea is a component can contribute to system failure by its presence in one or more cut sets [19]. The established method to estimate PI is Fussell–Vesely (I_{FV}). I_{FV} shows the same result with the risk reduction worth (RRW) method. The I_{FV} can be explained as follows:

$$I_{\mathrm{FV}} = \frac{P(\mathrm{TE}) - P(\mathrm{TE})_{P(\mathrm{BE}_j)=0}}{P(\mathrm{TE})} \qquad (22)$$

I_{FV} 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 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. These measures estimate the probability that event *i* is contributing to system failure. The PI is a type of sensitivity analysis and can be used for system design, diagnosis and optimization. For example, based on the PI simulation results, enterprises can estimate the rank of root causes that contribute to the hazards in the batch plant. Safety and reliability improvement can be implemented after considering this simulation result such as inspection, maintenance and failure detection. The other advantage is the implementation of safety and reliability re-design for batch process after considering the results of simulation.

5. Case study—simulation result

5.1. Simulation of LOC and scenario development—Case 1

This method is implemented for LOC at polymerization batch process, the two main causes of LOC are runaway temperature and overflow [6]. Reported by an industry that temperature at reactor lead to 110 °C, 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 47–55 psig. It is known that a runaway reaction leads to LOC. The simulation result for runaway can be seen in Fig. 8.

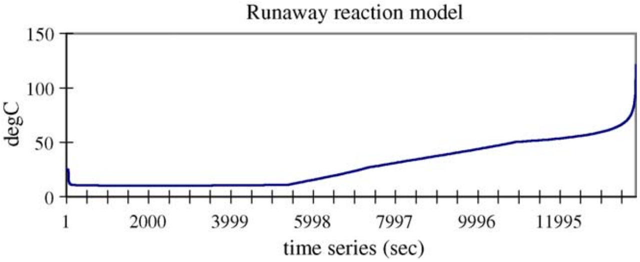

Fig. 8. Simulation result for runaway reaction.

From the results of the simulation show the importance of safety objects in mitigating the chain of events from BE. We consider the instrumentation devices (flow, temperature) and the control valves (automatic and manual) and a 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 Tables 2 and 3.

Based on qualitative analysis, we implement FTA, this graph can be shown in Fig. 9.

Considering the FTA in Fig. 9, it can be seen on the right-hand side (RHS), overflow material (G3) contributes to LOC. $P(\mathrm{G3}) = P(\mathrm{G6})$ AND $P(\mathrm{G7})$, or $P(\mathrm{G3}) = (P(\mathrm{G12})$ OR $P(\mathrm{G13}))$ AND $P(\mathrm{G7})$, and $P(\mathrm{G3})$ based on BE and SSM will be $((P(\mathrm{BE}_{61\ldots6n})$ AND $\mathrm{SSM}_1)$ OR $(P(\mathrm{BE}_{71\ldots7n})$ AND $\mathrm{SSM}_1)$ AND $(P(\mathrm{BE}_8)$ AND $\mathrm{SSM}_1))$. For the left-hand side (LHS), $P(\mathrm{G2}) = P(\mathrm{G4})$ AND $P(\mathrm{G5})$, where (i) $P(\mathrm{G4}) = ((P(\mathrm{BE}_1)$ AND $\mathrm{SSM}_2)$ OR $(P(\mathrm{BE}_2)$ AND $\mathrm{SSM}_2))$; (ii) $P(\mathrm{G5}) = ((P(\mathrm{BE}_{31\ldots3n})$ AND $P(\mathrm{BE}_{41\ldots4n})$ AND SSM_2 AND $\mathrm{SSM}_2)$ OR $(P(\mathrm{BE}_{51\ldots5n})$ AND $\mathrm{SSM}_2))$. The MCS can be obtained automatically from

Table 2
Example of fault propagation model using dynamic simulator output with high flow deviation triggered

SSM	Trigger	SF-117	V-104	SF-118	SF-105	V-105	S-110	LOC
[0 0 0 1 0 0 0 0 0]	P-104:H	High	Open	High	High	Open	High	Yes
[0 0 0 1 0 0 0 0 0]	P-104:H	High	(Cont:F)	High	High	Open	High	Yes
[0 0 0 1 0 0 0 0 0]	P-104:H	High	(Cont:F)	High	High	(Cont:F)	High	Yes
[0 0 0 1 0 0 0 0 0]	P-104:H	High	Open	High	High	(Cont:F)	High	Yes
[0 0 0 1 0 0 0 0 0]	P-104:H	Not detect	Open	High	High	Open	High	Yes
[0 0 0 1 0 0 0 0 0]	P-104:H	Not detect	Open	High	High	(Cont:F)	High	Yes
[0 0 0 1 0 0 0 0 0]	P-104:H	Not detect	Open	Not detect	High	Open	High	Yes
[0 0 0 1 0 0 0 0 0]	P-104:H	Not detect	Open	Not detect	Not detect	Open	High	Yes
[0 0 0 1 0 0 0 0 0]	P-104:H	Not detect	Open	High	Not detect	Open	High	Yes
[0 0 0 1 0 0 0 0 0]	P-104:H	High	Open	Not detect	Not detect	Open	High	Yes
[0 0 0 1 0 0 0 0 0]	P-104:H	High	Open	High	Not detect	Open	High	Yes
[0 0 0 1 0 0 0 0 0]	P-104:H	Norm	Open	Norm	Norm	Open	Norm	No
[0 0 0 1 0 0 0 0 0]	P-104:H	Norm	Open	Norm	Norm	Open	Norm	No
[0 0 0 1 0 0 0 0 0]	P-104:H	High	Close	No	No	Op/cl	No	No
[0 0 0 1 0 0 0 0 0]	P-104:H	High	Open	High	High	Close	No	No
[0 0 0 1 0 0 0 0 0]	P-104:H	High	(Cont:T)	Norm	Norm	Open	Norm	No
[0 0 0 1 0 0 0 0 0]	P-104:H	High	Open	High	High	(Cont:T)	Norm	No
[0 0 0 1 0 0 0 0 0]	P-104:H	Not detect	Open	High	High	Close	No	No
[0 0 0 1 0 0 0 0 0]	P-104:H	Not detect	Open	High	High	(Cont:T)	Norm	No
[0 0 0 1 0 0 0 0 0]	P-104:H	High	Open	Not detect	High	Close	No	No
[0 0 0 1 0 0 0 0 0]	P-104:H	High	Open	Not detect	High	(Cont:F)	Low	No
[0 0 0 1 0 0 0 0 0]	P-104:H	High	Open	Not detect	High	(Cont:T)	Norm	No
Cont.	...	...	...	...	...	...	...	...

Table 3
Example of fault propagation model using dynamic simulator output with high temperature deviation triggered in charging line and followed by loss of cooling

SSM-1	Trigger	S-110	V-104	V-105	SSM-2	Trigger	V-202	SF-205	Temp high	LO cooling	LOC
[0 0 0 1 0 0 0 0 0]	ST-105:H	Not detect	Open	Open	Non-active	N/A	N/A	N/A	Yes	N/A	No
[0 0 0 1 0 0 0 0 0]	ST-105:H	High	Open	Close	Non-active	N/A	N/A	N/A	No	N/A	No
[0 0 0 1 0 0 0 0 0]	ST-105:H	Not detect	Open	Open	Non-active	N/A	N/A	N/A	Yes	N/A	No
[0 0 0 1 0 0 0 0 0]	ST-105:H	Not detect	Close	Open	Non-active	N/A	N/A	N/A	No	N/A	No
[0 0 0 1 0 0 0 0 0]	ST-105:H	High	Open	Open	Non-active	N/A	N/A	N/A	Yes	N/A	No
[0 0 0 1 0 0 0 0 0]	ST-105:H	High	Open	Open	[0 0 0 0 0 0 1 0 0]	P-202:UD	Open	Norm	Yes	No	No
[0 0 0 1 0 0 0 0 0]	ST-105:H	High	Open	Open	[0 0 0 0 0 0 1 0 0]	P-202:UD	Open	Low	Yes	Yes	Yes
[0 0 0 1 0 0 0 0 0]	ST-105:H	High	Open	Open	[0 0 0 0 0 0 1 0 0]	P-202:UD	Close	No	Yes	Yes	Yes
[0 0 0 1 0 0 0 0 0]	ST-105:H	High	Open	Open	[0 0 0 0 0 0 1 0 0]	P-202:UD	Open	No	Yes	Yes	Yes
[0 0 0 1 0 0 0 0 0]	ST-105:H	High	Open	Open	[0 0 0 0 0 0 1 0 0]	P-202:UD	Open	Not detect	Yes	Yes	Yes
Cont.	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .

reliability block diagram of the systems and yields MCS and their unavailability:

- $MCS_1 = [(BE_8,SSM_1),(BE_6,SSM_1)] = 2.88 \times 10^{-11}$;
- $MCS_2 = [(BE_8,SSM_1),(BE_7,SSM_1)] = 1.4 \times 10^{-11}$;
- $MCS_3 = [(BE_1,SSM_2),(BE_5,SSM_1)] = 4.05 \times 10^{-10}$;
- $MCS_4 = [(BE_1,SSM_2),(BE_3,SSM_1)] = 3.42 \times 10^{-10}$;
- $MCS_5 = [(BE_1,SSM_2),(BE_4,SSM_2)] = 2.1 \times 10^{-9}$;
- $MCS_6 = [(BE_2,SSM_2),(BE_3,SSM_1)] = 2.1 \times 10^{-9}$;
- $MCS_7 = [(BE_2,SSM_2),(BE_4,SSM_2)] = 2.1 \times 10^{-9}$;
- $MCS_8 = [(BE_2,SSM_2),(BE_5,SSM_1)] = 2.48 \times 10^{-9}$.

The redundancy of safety objects can be simulated by AND gate for every MCS. For example, $BE_{71\ldots7n}$ is used for failure of n control valves simultaneously.

After estimating the MCS, we can simulate the unavailability of TE by the combination of MCS, it is obtained about 9.56×10^{-9}.

5.2. Simulator triggering effect

5.2.1. High availability of charging line—Case 2

The concept of SSM promotes a better modeling of the batch process. The simulator can be used to investigate the plant safety and reliability in the specific circumstances. Case study in section 5.1 simulated the LOC as the multiple failure model, which incorporating at least two initiating events, high output of pump P-104 and high temperature near ST-105. Obviously, it seems to be a simple case because only two failures are included for the safety analysis. However, if there are a number of failures occurred during one batch, it will be more complex analysis. Let us make an assumption for this case study, if the maintenance programs are implemented for the charging line part, we can suppose this part is in high reliability and availability, therefore, charging line part is not considered as a contributor to the hazard (LOC). This condition is simulated by setting the SSM_1 to be false therefore, now, the safety analysis for LOC depends on runaway reaction only. SSM represents not only the batch task time sequence, but also shows the status of availability of a batch task. Within a period of time, it is possible for a task is considered as zero failure area, for that reason, it does not take into account in the safety analysis. We obtain the changes of unavailability of MCS structure from this simulation become:

- $MCS_{11} = [(BE_8,SSM_1),(BE_6,SSM_1)] = n/a$;
- $MCS_{21} = [(BE_8,SSM_1),(BE_7,SSM_1)] = n/a$;
- $MCS_{31} = [(BE_1,SSM_2),(BE_5,SSM_1)] = n/a$;
- $MCS_{41} = [(BE_1,SSM_2),(BE_3,SSM_1)] = n/a$;
- $MCS_{51} = [(BE_1,SSM_2),(BE_4,SSM_2)] = 2.1 \times 10^{-9}$;
- $MCS_{61} = [(BE_2,SSM_2),(BE_3,SSM_1)] = n/a$;
- $MCS_{71} = [(BE_2,SSM_2),(BE_4,SSM_2)] = 2.1 \times 10^{-9}$;
- $MCS_{81} = [(BE_2,SSM_2),(BE_5,SSM_1)] = n/a$.

From the above list, the unavailability of TE is 4.2×10^{-9}, and it is lower than Case 1. The “n/a” represents not-applicable for certain condition, the examples show that parts of batch process which have the SSM_1 will be n/a for the safety analysis

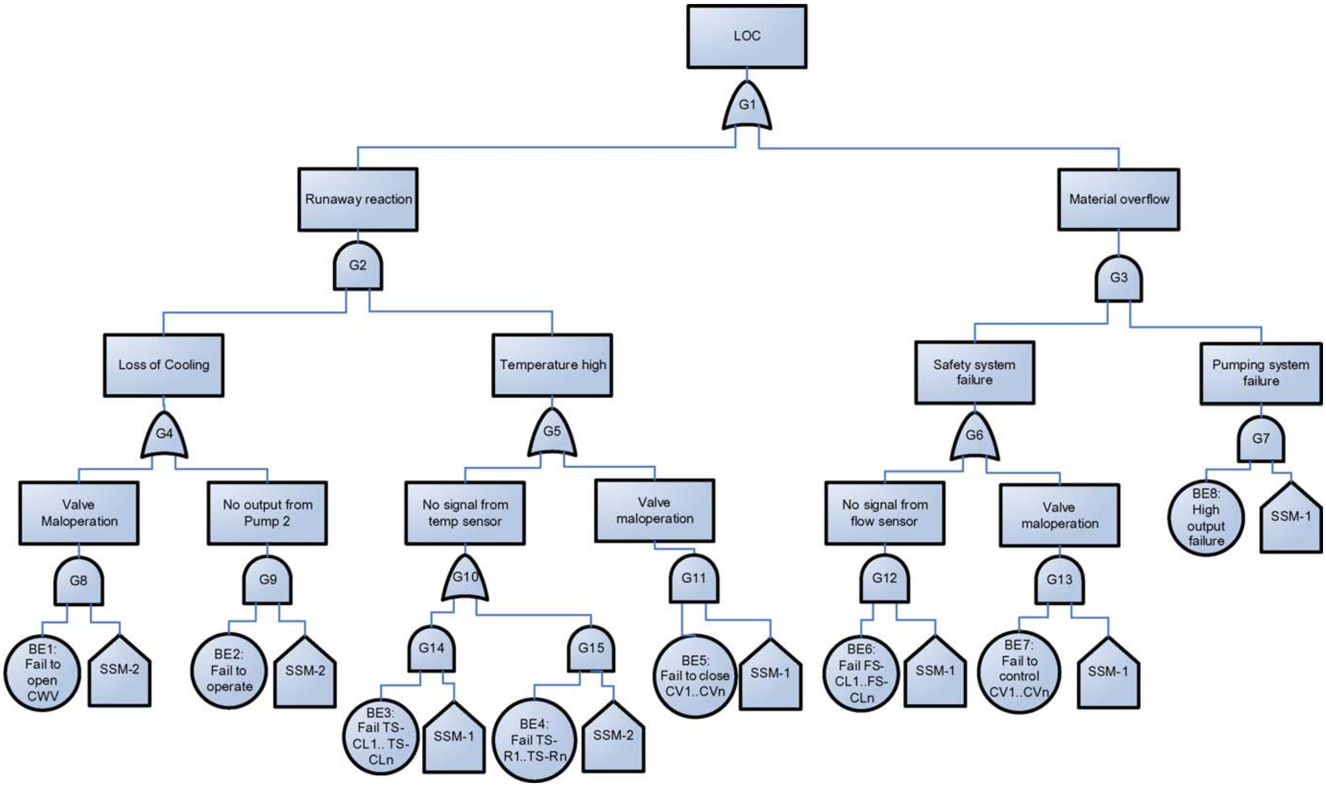

Fig. 9. FTA based on qualitative analysis.

purposes. For detail analysis, the simulation of Case 3 is presented in the following section.

5.2.2. *High availability of cooling water (reaction phase)—Case 3*

The cooling water line is one of the critical part of reaction in the batch process, it maintains the temperature around 60 °C in the reactor, when temperature in the reactor jacket is detected to be increasing, the cooling water will be charged automatically to the reactor. Failure of cooling water can generate the hazardous situation such as runaway reaction and explosion. In this case, SSM_2 is set to be false, which represents the high availability of cooling water part and will not be considered as contributor to the hazardous situation. This restriction will give the results in MCS:

- $MCS_{12} = [(BE_8,SSM_1),(BE_6,SSM_1)] = 2.88 \times 10^{-11}$;
- $MCS_{22} = [(BE_8,SSM_1),(BE_7,SSM_1)] = 1.4 \times 10^{-11}$;
- $MCS_{32} = [(BE_1,SSM_2),(BE_5,SSM_1)] = $ n/a;
- $MCS_{42} = [(BE_1,SSM_2),(BE_3,SSM_1)] = $ n/a;
- $MCS_{52} = [(BE_1,SSM_2),(BE_4,SSM_2)] = $ n/a;
- $MCS_{62} = [(BE_2,SSM_2),(BE_3,SSM_1)] = $ n/a;
- $MCS_{72} = [(BE_2,SSM_2),(BE_4,SSM_2)] = $ n/a;
- $MCS_{82} = [(BE_2,SSM_2),(BE_5,SSM_1)] = $ n/a.

Then the unavailability of TE can be estimated around 4.28×10^{-11}, it is lower than Cases 1 and 2. We obtained from the Case 3 that the probability of LOC due to high flow of material is very low and depend on the SSM_2.

6. PI rank

After implementing the dynamic simulation for the batch plant, then evaluation of process and calculating the unavailability of the process, the final step is to estimate the performance rank of each safety object. This rank gives an advantage to the enterprises to perform maintenance, safety and reliability improvement for the whole process. 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 [18]. The rank of BE based on I_{FV} and RRW for Case study 1 can be seen in Table 4.

From Table 2, BE_2 (failure to operate pump in cooling water system) and BE_4 (failure of sensor to detect high temperature in reactor) are considered for further investigation because these objects have first and second rank among the other safety objects. For Cases 2 and 3, the rank of PI are different from Case 1,

Table 4
Indices of FV–RRW and rank of each safety objects for Case 1

	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

Table 5
Indices of FV and rank of each safety objects for Cases 2 and 3

	FV index	Rank
Case 2		
BE_1	0.5	2
BE_2	0.5	2
BE_4	1	1
Case 3		
BE_6	0.673	2
BE_7	0.327	3
BE_8	1	1

because in Cases 2 and 3, the single failure model is implemented.

Table 5 shows the different rank/prioritization index for safety objects, for Case 2, BE_4 (failure of temperature sensors in reactor) should be prioritized to be improved in maintenance program and in Case 3, BE_8 (failure of pump: high output at VCM charging line) is indicated as a major contributor to the top event and should be investigated for further safety and reliability program.

7. Conclusion

The dynamic simulator is proposed to improve safety and reliability of batch chemical process. To analyze the batch process, it is required to incorporate the time sequences or scheduling mechanism as an integral part of the safety assessment. The concept of SSM has advantages: (i) shows the nature of batch processes which are performed by the task scheduling, without the SSM, the dynamic behavior of batch cannot be integrated. In addition, the SSM is the task activation oriented, thus, time and location of abnormality can be easily determined, (ii) reduces the complexity of safety analysis by neglecting the high availability process (e.g. after regular maintenance program is implemented) and focusing to the unreliable process.

The dynamic simulation is developed to evaluate the safety objects and to support the optimal policy for improvement the systems availability. The 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 result can be considered as valuable input to safety and reliability design stage for chemical process system engineering.

References

[1] N.J. Scenna, Some aspects of fault diagnosis in batch process, J. Rlb Eng. Syst. Saf. 70 (2000) 95–110.

[2] Y. Shimada, H.A. Gabbar, K. Suzuki, Operation decision support system using plant design information, in: Proc. ESCAPE 12, 2002, pp. 793–798.

[3] H.A. Gabbar, S. Shinohara, Y. Shimada, K. Suzuki, Experiment on distributed dynamic simulation for safety design of chemical plants, J. Sim. Model. Prac. Theory 11 (2003) 109–123.

[4] R. Srinivasan, V. Venkatasubramanian, Multi-perspective models for process hazards analysis of large scale chemical processes, J. Comp. Chem. Eng. 22 (1998) S961–S964.

[5] M. Shacham, N. Brauner, M.B. Cutlip, Open architecture modelling and simulation in process hazard assessment, J. Comp. Chem. Eng. 24 (2000) 415–421.

[6] A. Collins, D. Keeley, Loss of Containment Incident Analysis, HSL, England, 2003.

[7] Y. Shimada, K. Suzuki, H. Sayama, Computer-aided operability study, J. Comp. Chem. Eng. 20 (1995) 905–913.

[8] K. Suzuki, Y. Shimada, P. Heino, Computer-aided hazard identification system and design of safety interlock system, in: Proc. of the 10th European Conference on Safety and Reliability, September 1999, 1999.

[9] D. Rizal, K. Suzuki, Batch chemical plant safety analysis based on fault propagation approach, in: Proceedings of the10th Asia Pacific Confederation of Chemical Engineering Conference, Kitakyushu, Japan, October 2004.

[10] Instrument Society of America, ANSI/ISA-S88.01-1995. Batch control part 1: models and terminology, ISA, North Carolina, 1995.

[11] D. Rizal, K. Suzuki, A concept of modelling PVC batch plant in object oriented approach for safety analysis, J. Lec. Note Comp. Sci. 2718 (2003) 271–276.

[12] L. Hub, Simulation program for hazard training and safety evaluation of chemical processes, Chem. Eng. Technol. 22 (1999) 740–742.

[13] R.A. Faust, Toxicity Summary for Vinyl Chloride, Oak Ridge National Laboratory, Oak Ridge, Tennessee, 1993.

[14] B.W. Bequette, Process Dynamics, Modelling Analysis and Simulation, Prentice-Hall, Inc., New Jersey, 1998.

[15] F.I. Khan, S.A. Abbasi, A criterion for developing credible accident scenarios for risk assessment, J. Loss Prev. Proc. Ind. 15 (2002) 467–475.

[16] CCPS, Guidelines for Chemical Process Quantitative Risk Assessment, AIChE, New York, 1989.

[17] M. Cepin, B. Mavko, A dynamic fault tree, J. Rlb Eng. Syst. Saf. 75 (2002) 83–91.

[18] R.M. Sinnamon, J.D. Andrews, Improved accuracy in quantitative fault tree analysis, J. Qly. Rlb Eng. Int. 13 (1997) 285–292.

[19] E.J. Henley, H. Kumamoto, Reliability Engineering and Risk Assessment, Prentice-Hall, Inc., New Jersey, 1981.