CHEMICAL ENGINEERING TRANSACTIONS
VOL. 31, 2013
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at: www.aidic.it/cet
Guest Editors: Eddy De Rademaeker, Bruno Fabiano, Simberto Senni Buratti

ISBN 978-88-95608-22-8; ISSN 1974-9791
DOI: 10.3303/CET1331074

# Promoting Discussions in Safety Review Activity

Masaki Nakagawa

Senior Researcher, Safety Engineering and Environmental Integrity Group, Production Technology Laboratory, Mitsubishi Chemical Group Science & Technology Research Center 1000, Kamoshida-cho Aoba-ku, Yokohama 227-8502 JAPAN
2109797@cc.m-kagaku.co

Discussion from diversified viewpoints is very important for process safety review. Therefore to promote discussion is essential for improvement of process safety.
Mitsubishi Chemical Corporation has been working to improve process safety by performing safety review (SR) activities. The aim of the SR activity is to improve safety of processes and operations by sharing information from a broad range of perspectives. The SR activities are joined not only by staffs who are familiar with routine operation, but also by staffs who belong to other departments. To strengthen the SR activity, SR Instructor Team was formed. The member of SR instructor team is composed of retired and senior engineers who have abundant knowledge and experience about processes and safety measures. The SR activity becomes a field where experiences, perspectives and knowledge are shared by participants.
To facilitate the SR activity, HAZchart analysis is used for risk evaluation method. It facilitates process of risk evaluation from accident scenario formulation to quantitative evaluation and enables worst-case scenarios to be easily assumed. By using HAZchart analysis supporting software that is called PHA_Organizer, anyone has been able to conduct risk evaluation easily.
This software was privately used at first. But it became clear that PHA_Organizer could facilitate sharing a mutual thinking process and promote discussion at a meeting. Consequently PHA_Organizer was significantly improved to make the tool even easier to use and anyone could easily conduct risk evaluations at a meeting. The main improved points are common cause specific function, minimal cut set display function and redundant system drawing function and improvement of user interface, etc. Promoting discussions in Safety Review Activity is expected by these upgrades.

## 1. Introduction

Chemical plant treats hazardous substances in large quantities. Once an accident occurs, there is a possibility that damage may befall even the environment and the peripheral people.
In the present, Chemical plants have been introducing advanced control technology for the purpose of optimization of low cost or quality. However, since operating staff's opportunity to experience troubles and unsteady operations is decreasing, it has led to the falling of the safety skill of the manufacturing floor. As a result, sufficient response cannot be performed even if abnormalities occur in a plant. Moreover, a veteran operator's retirement increases and loss of the technology and know-how cultivated through a trouble is pointed out. The accident which occurs owing to the staff and operator's deficient knowledge or the shortage of experience is increasing from these problems.
Therefore, making the mechanism of sharing the knowledge and perspective from the veteran staff to the young staff is called for.

Please cite this article as: Nakagawa M., 2013, Promoting discussions in safety review activity, Chemical Engineering Transactions, 31, 439-444 DOI: 10.3303/CET1331074

## 2. Process Safety Review

### 2.1 Activity

SR is an activity of process overhaul to re-check, re-review and re-assess our process safety.

From the point of view of prevention of accidents, SR investigates hazardous factors in chemical plants and takes countermeasures if necessary. It is expected that this activity improves each person's understanding and awareness for chemical plant safety. SR activity is performed as follows,

1. SR activity identifies latent hazards in a target process and takes countermeasures to mitigate them by learning from previous accidents in similar processes across the world.
   In SR activity, a series of the risk identification and mitigation activities are performed in a comprehensive, systematic and continuous way.
2. Re-recognition of hazards
   SR activity re-assesses why existing measures are capable of mitigating hazards.
   SR activity re-recognizes potential hazard when these measures fail to work effectively.
3. Education of safety technologies and their transfer to next generations.
   SR activity includes education and transfer of various safety technologies, such as hazard identification by means of risk evaluation method, hazard mitigation and re-recognition of know-why of mitigation measure, to current and next generation employees. Thus SR aims at improving sensitivity and awareness to maintain safety.

### 2.2 SR instructor

Knowledge sharing from various viewpoints in SR activity raises safety skill. In order to achieve effect in SR activity, SR is performed by taking the viewpoint of third parties other than a manufacturing site, such as staffs from the safety department, maintenance department and other department. SR meeting serves as a place where experience and knowledge are shared by the participants.

SR instructor team which is composed of retired and senior engineers who have affluent knowledge and experience about process safety was established to strengthen SR activity. Each SR instructor is working in each plant site. When a meeting on safety is held at a section, SR instructor participates together and is performing comment and advice. He reports contents of duties to a plant manager periodically. SR instructors are exchanging information by gathering periodically.

## 3. Risk evaluation method

### 3.1 Risk evaluation method

One of the risk evaluation methods currently used for SR activity is HAZchart analysis.

HAZchart analysis is the risk evaluation method which Mitsubishi Chemical Corporation and Mitsubishi Research Institute developed, and it can carry out easily from development of an accident scenario to quantitative evaluation. Furthermore, by using software that is called PHA_Organizer, risk evaluation is efficiently analyzable. This software was privately used at first. But it became clear that PHA_Organizer could facilitate sharing a mutual thinking process and promote discussion at a meeting. Consequently PHA_Organizer was significantly improved to make the tool even easier to use and anyone could easily conduct risk evaluations at a meeting. The main improved points are common cause specific function, minimal cut set display function and redundant system drawing function and improvement of user interface, etc.

### 3.2 HAZchart analysis procedure

The procedure for HAZchart is described in the following example (Figure 1). Material A and B are fed in a certain proportion into the reactor. If the ration of the materials were changed, runaway reaction would occur.

HAZchart analysis consists of four steps. Firstly, one of the equipment which affects fluid in the plant is selected and the fault mode is set in it. Then HAZchart is developed by querying three situations repeatedly. Those queries are the finding of phenomenon, recovery actions, and consecutive phenomenon. After that, a HAZchart is transferred to Fault Tree (FT) and finally the probability of accident is calculated by setting up equipment reliability data and human error data in the FT.

First of all, the equipment that can potentially influence the process fluid is chosen and is set the fault mode in it. In this case FCV1 which controls the mass flow of material B is chosen and the fault mode is selected as excessive opening. After setting the fault mode, querying three situations develops the HAZchart analysis (Figure 2). Next, step is to transfer Fault tree from the HAZchart. Methods of finding phenomenon, recovery actions, and consecutive phenomena in the HAZchart correspond to Fault Tree

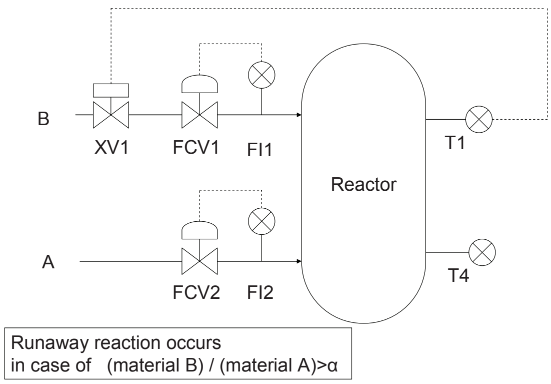



Figure 1: Example Flow

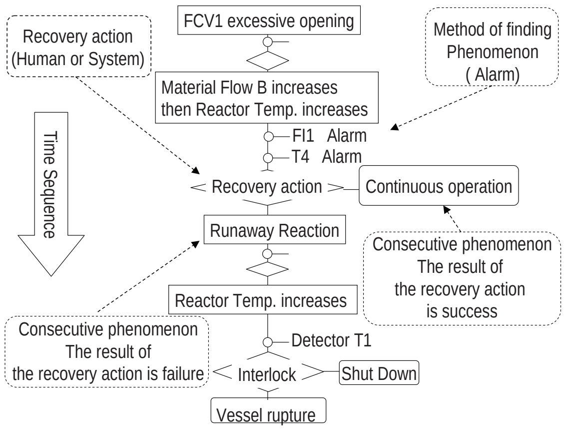



*Figure2 HAZchart*

logic. Thus, it is easy to transfer information from a HAZchart to a FT (Figure 3).This transformation consists of 3 steps. (1) HAZchart is turned upside down. (2) Rectangular parts that indicate consecutive phenomena are arranged on the left side of the FT and diamond parts that indicate recovery actions are arranged on the right side of the FT. (3)The rectangular parts are combined with the diamond parts by an AND symbol. After transformation, branches of FT are divided up to a level that has equipment reliability data or human error data. Then, the equipment reliability data are set up in the FT. Finally, the probability of explosion can be calculated (Figure 4).

**3.3 Common cause specific function**

Risk evaluation is usually performed by what-if analysis or HAZOP analysis. If a scenario which is major accidents, such as fire, explosion, and toxic gas leakage was generated in risk evaluation, detailed evaluation would be performed by Hazchart analysis. The result of the HAZchart analysis is plotted in a matrix and is evaluated.

Common cause is an important factor in the FT calculation. The reason why is that the accident would be underestimated if common cause was not set up by mistake to calculate the probability of an accident. To solve this problem, PHA_Organizer has been improved to calculate the probability of FT that includes common cause by recognizing equipment as the same equipment in case their information are the same.

After FT calculation, the result of the HAZchart analysis can be displayed on the What-if / HAZOP worksheet format. Safeguards on which results of the common cause calculation were reflected can be displayed in the safeguard column.

The explanation of common cause specific function is described in the example flow Figure 1. First of all, What-if analysis is conducted on the what-if work sheet (Figure 5).Then, the accident scenario which results in a major accident is chosen.

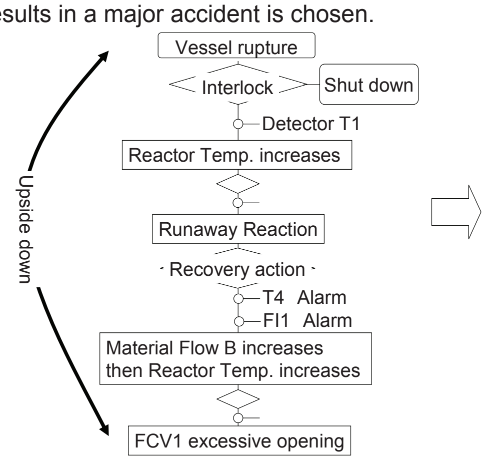



*Figure 3: HAZchart transformation*

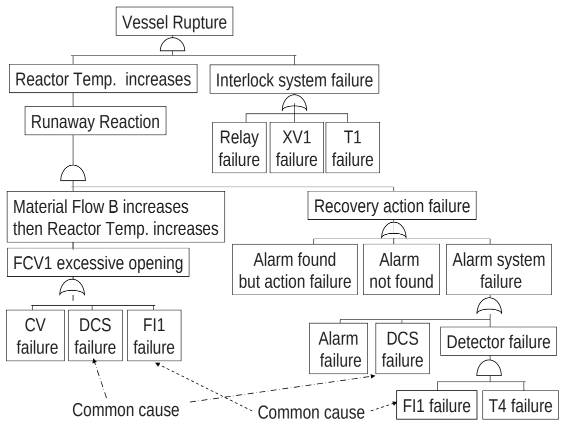



*Figure4: Fault Tree*


Figure 5: What-if work sheet in PHA_Organizer

(a) Before

| Line | Cause | Consequence | HC/FT | Safeguard |
|---|---|---|---|---|
| | FCV1 Excessive Opening | Runaway Reaction → Vessel rupture | | FI1 Alarm<br>T4 Alarm<br>Temp. I/L |

(b) After

| Line | Cause | Consequence | HC/FT | Safeguard |
|---|---|---|---|---|
| | FCV1 Excessive Opening | Material Flow B increases then Reactor Temp. increases<br>→ Runaway Reaction<br>→ Reactor Temp. increases<br>→ Vessel rupture | | T4 Alarm<br>Temp. I/L |

Figure6: What-if work sheet (expansion version)

In this case FCV1 excessive opening is selected. After transferring to a HAZchart work sheet from what-if work sheet, HAZchart analysis is conducted. When modeling HAZchart, PHA_Organizer would recognize two equipments as the same equipment if their tag No and other information were the same. After finishing modeling, HAZchart is transformed to FT. Figure 4 shows FI1 is common cause. Calculation of a FT can be performed instantly because PHA_Organizer has the mechanism of setting the failure rate of equipment. After calculation of FT, the result of HAZchart analysis is transferred from HAZchart work sheet to what-if work sheet. Then, the detailed accident scenario and related safeguard are displayed on the what-if work sheet (Figure 6).

At first, FI1 alarm was in the safeguard column. But after calculation of the FT, FI1 alarm is deleted in the Safeguard column because FI1 is common cause.

The scenario in the consequence column was very simple. But after analysis, the scenario is transformed to detailed story.

Figure 7 shows these mechanisms. The scenario in the consequence column is constructed by connecting of " consecutive phenomenon" in the HAZchart. Safeguards in the safeguard column are "methods of finding phenomenon" in the HAZchart. The original scenario turns into a more detailed and more intelligible scenario.

### 3.4 Minimal Cut Set display function

A cut set is a combination of basic phenomena which generates the top phenomenon of FT. A minimal cut set is made required to generate a top phenomenon of a system, and is sufficient cut set.

The minimal cut set was often expressed as a set. But this expression form is not so easy to understand intuitively. So the function of displaying minimal cut set relationship on the FT has been developed. By this function, it is easy to understand which basic phenomenon lowers the probability of the top phenomenon occurrence intuitively.

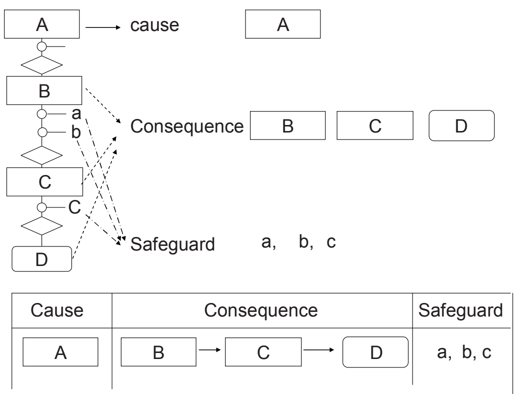



Figure 7: What-if work sheet construction

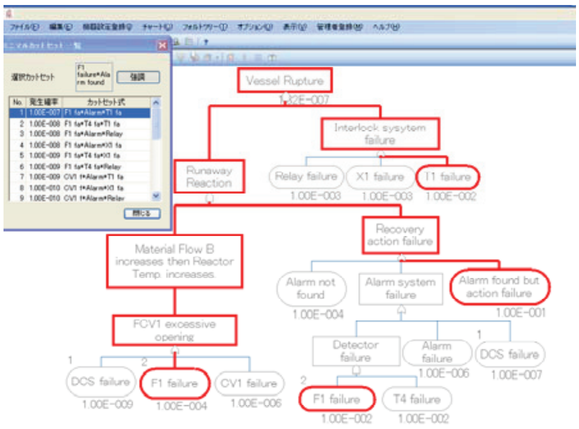



Figure8: Minimal cut set function in PHA_Organizer

Figure 8 shows the PHA_Organizer screen in which minimal cut set display function is operating. Minimal cut sets in the window on the upper left side line up in order of the probability. By specifying the minimal cut set, each minimal cut set combination can be displayed on the FT. The combination of minimal cut set can be displayed on the FT by changing related line's colour in PHA_Organizer.

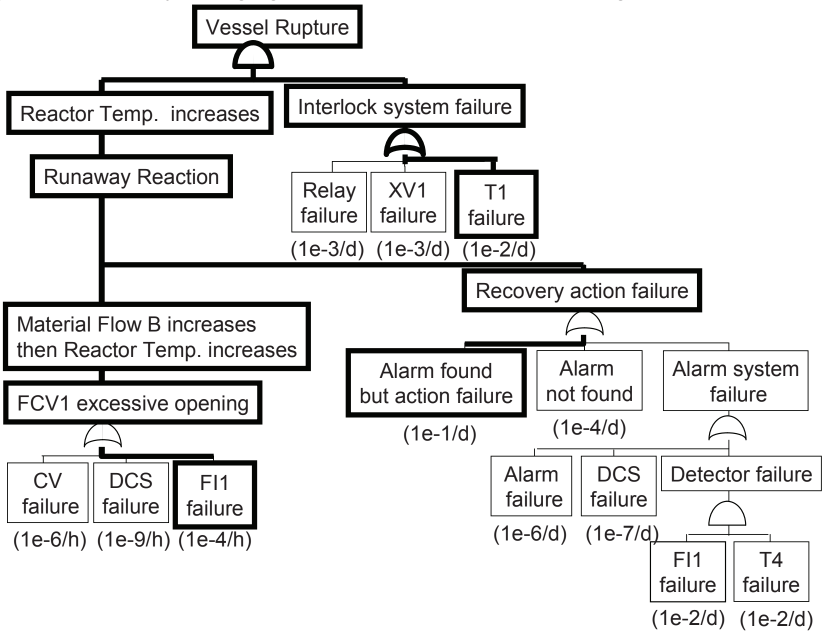



*Figure 9: Minimal cut set function image (expansion version)*

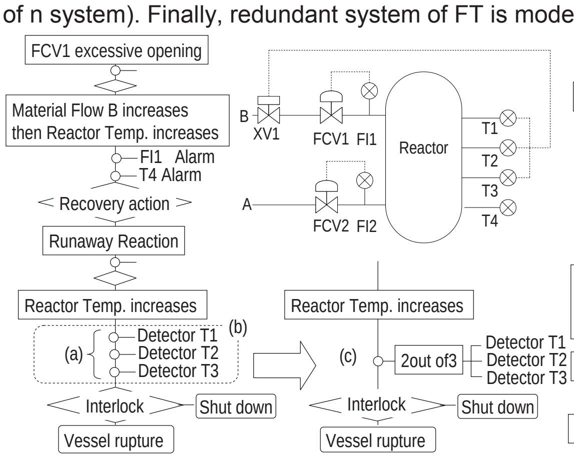
Figure 9 shows the minimal cut set function display image. The minimal cut set is shown in the thick line. Failure rates and demand rates are displayed under each basic phenomenon. The minimal cut set with the highest probability is the combination of “FI1 failure” and ” Alarm found but action failure” and “T4 failure”. The demand rate of "Alarm found but action failure" can not be changed because the probability value of human error depends on time margin. Therefore, the probability of top phenomenon is lowered by adopting a redundancy system to the temperature interlock system.

**3.5 Fault tree assist function**

Redundant system is adopted as one of the means of raising reliability of an interlock system.

The FT that expressed the redundant system had been modeled manually while performing HAZchart. But this work was time consuming and participants got bored while modeling FT manually. So the drawing system that can draw a redundant system easily has been developed.

Figure 10 shows drawing system. Firstly, (a) all detectors that are included in redundant system are drawn in the HAZchart. Then, (b) all of them are selected. After that, (c) they are set as redundant system (m out of n system). Finally, redundant system of FT is modeled (Figure11).



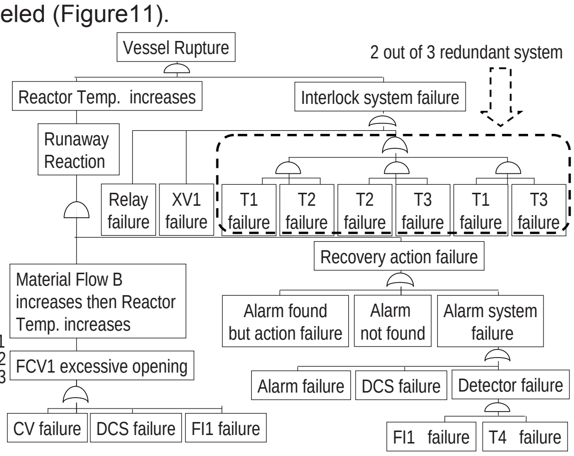




*Figure10: 2 out of 3 I/L system on the HAZchart*

*Figure 11: 2 out of 3 I/L system on the FT*

Because PHA_Organizer has a redundant logic system, it can respond to any redundant system.

**3.6 Promoting Discussion**

When performing safety evaluation at SR meeting, two projectors are used, one set is used for the screen of PHA_Organizer and another set is used for the screen of flow sheets. The state of the process that the participant thinks about is projected on the screen by projected accident scenario. That can facilitate sharing a mutual thinking process. Furthermore, projecting accident scenario induces various questions. Through such discussion, the idea and the fragmentary information which each participant has can be edited and summarized, and can be shared. By asking, the related knowledge and concept that participant has in their mind can be expressed, a participant's idea can be pulled out and the knowledge and concept which are being shared only in each individual and a group can be expressed.

It is important how the redundancy of the information in an organization is promoted and maintained. To build an organization with a redundancy of information is to build an organization that will promote discussion and communication frequently. Such an organization has the foundation which new knowledge and idea can generate among employees.

PHA_Organizer is expected as a tool for providing a field which promotes discussion.

## 4. Conclusion

SR is an activity of process overhaul to re-check, re-review and re-assess our process safety.

The aim of the SR activity is to improve safety of processes and operations by sharing information from a broad range of perspectives.

To facilitate the SR activity, HAZchart analysis is used for risk evaluation method. PHA_Organizer which is HAZchart analysis supporting software was significantly improved to make the tool even easier to use and anyone could easily conduct risk evaluations at a meeting. The main improved points are common cause specific function, minimal cut set display function and redundant system drawing function and improvement of user interface, etc. It is expected that these upgrades contribute to promoting discussion in Safety Review Activity.

### References


Nakagawa M., Iizuka Y., Introduction and application of quantitative process hazard analysis – HAZChart, 11th Intl. Symposium of Loss Prevention and Safety Promotion in the Process Industries, 31 May – 3 June 2004, Praha, Czech Republic, 4388-4394.

Nakagawa M., Mizuta Y., Development of a worst case scenario, 13th Intl. Symposium of Loss Prevention and Safety Promotion in the Process Industries, 6 – 9 June 2010, Brugge, Belgium, 455 - 458.

Lees F.P., 1996, Loss prevention in the process industries second edition, Butterworth-Heinemann, Oxford, UK, Vol.1, 9/18.

Center for Chemical Process Safety (CCPS), 2000, Guidelines for Chemical Process Quantitative Risk Analysis Second Edition. American Institute of Chemical Engineers, New York, NY.

Center for Chemical Process Safety (CCPS), 1994, Guidelines for Hazard Evaluation Procedures. American Institute of Chemical Engineers, New York, NY.

Center for Chemical Process Safety (CCPS), 1993, Guidelines for Safe Automation of Chemical Processes. American Institute of Chemical Engineers, New York, NY.

Martorell S., Martón I., Villamizar M., 2010, Reliability of safety systems and probabilistic risk assessment, Chemical Engineering Transactions, 19,321-326.