17th European Symposium on Computer Aided Process Engineering – ESCAPE17
V. Plesu and P.S. Agachi (Editors)

Combining disturbance simulation and safety analysis techniques for improvement of process safety and reliability

Naveed Ramzan, Werner Witt

Lehrstuhl Anlagen und Sicherheitstechnik, Brandenburgishe Technische Universität, Burger Chaussee 2 Lehrgebäude 4/5, Cottbus 03044, Germany,
Email: ramzan50@hotmail.com

Abstract

There is a clear link between safety and reliability in system design and operation. So the knowledge about sources of failure, their physical consequence related to plant operation and the frequency of effects (incident consequence) is of great value for improvement. Next, the selection of best improvement alternative should be justified by complete life cycle cost benefits. In this contribution, a quantitative merged process based on multiobjective decision analysis technique- (Promethee), Extended Hazop methodology (Hazop supported by dynamic simulation), reliability modeling and life cycle cost modeling is presented. A distillation column unit is used as case study.

Keywords: Lifecycle cost, Multiattribute decision analysis, Extended Hazop

1. Introduction

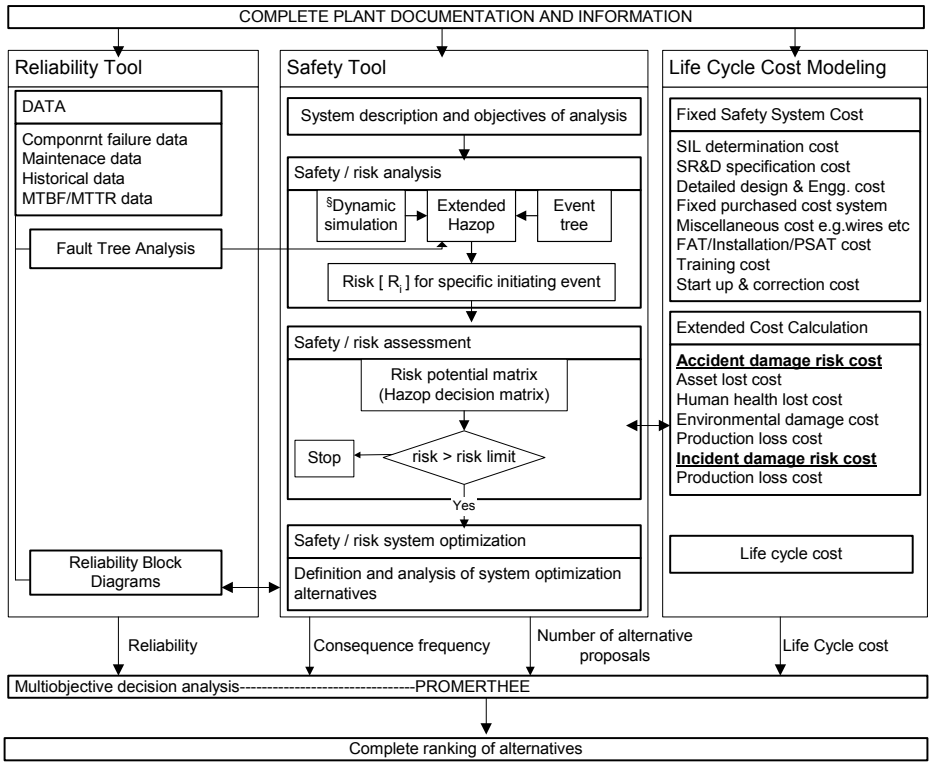
Equipment failures or faults in process occur as a result of complex interaction of the individual components and may lead to events that result in incipient faults, near misses, incidents and accidents in chemical plant [1]. Protection systems are often in place as prevention barriers e.g. alarms, shutdown systems etc. These protective systems e.g. alarms, interlocks may not be available when needed or active when not needed. So the knowledge about sources of failures, their physical consequence and the frequency of effects (incident consequences) is of great value for improvement. The aim of the safety analysis is to identify

weak points/ failures that could result to accidents, to evaluate the risk induced by them and to purpose risk reduction measures while the goal of reliability analysis is to identify potential contributing factors for the reliability of the component, to evaluate e.g. production losses and maintenance cost induced by failures and to find ways for improving plant reliability.
Hazop is the standard technique most frequently used in the chemical process industry for assessment of new systems as well as modification to existing ones. In recent years, dynamic simulation appears as a powerful tool for safety examinations and several examples for its use for study of operational failures of chemical processes has been documented [2,3]. We have presented recently an Extended Hazop methodology (Hazop supported by disturbance simulation) to determine risk from operational disturbances and to develop effective risk reductions [4]. Reliability block diagrams (RBD), FMEA, FT, ET, Master logic diagrams (MLD) and Reliability-centered maintenance (RCM) are used for reliability analysis. The techniques used to deal with safety analysis and reliability anaylsis have many similar activities so a merged process for safety and reliability analysis has several benefits e.g. less time consumption, better quality of analysis. One example of such a merged qualitative process is HAZROP, which combines Hazop and RCM [5].

2. Methodology

Figure 1 shows the simplified block diagram of the systematic procedure. Reliability analysis is integrated to Extended Hazop methodology for safety analysis at two levels. First at hazard identification stage, where each possible cause e.g. loss of cooling medium for process deviation under study in Extended Hazop is analyzed using quantitative fault tree analysis to identify critical equipment or instrument for reliability as well as process hazards and frequency of the possible cause. The possible causes are simulated using dynamic simulation (Aspen dynamics) to study the operational behavior and physical consequence. Physical and risk related consequences are documented separately in Extended Hazop worksheet. Event tree analyses are constructed to establish the consequence frequency. The risk category of each scenario is determined using order of magnitude risk assessment by risk potential matrix. For order of magnitude risk assessment, numerical rating 0 to 8 corresponding to frequency 10^{0} / yr to 10^{-8} /yr and consequence severity class from 0 to 8 based on rough estimates of consequence (business, safety and environment) corresponding to 10^{0} to 10^{-8} $ is used. An attempt is made to reduce the inherent hazard/risk by eliminating the cause by replacing the critical equipment / instrument with more reliable one or design modification (if possible), in case the risk category of scenario is in dangerous zone. Then, an attempt is made to improve the reliability of the protection system and finally an attempt is made to strengthening the mitigation measure or resistance to exposed “Targets”. All

scenarios are analyzed in similar fashion and alternative proposals are generated to deal risk potential scenarios. Each alternative proposal is evaluated using



i = { financial risk , environmental risk , human health risk }
§ Simulation of process related malfunctions

Figure 1. Quantitative procedure for integrated safety and reliability analysis

pre and post incident event tree. At this stage of safety optimization, reliability block diagrams (modified RBDs) based on all failure modes leading to accident scenario are integrated for reliability analysis of protection systems. To support the decisions, Life cycle cost (LCC) of each alternative is also calculated at this stage. Life cycle cost modeling used here is:

$$LCC = FCCSS + [(ADRC + IDRC).\ (1+ (1+R)^{-N}) / R]$$

Where R = interest rate, N= number of years (life)

First component is the fixed safety system cost (FCCSS), which is given by

$$FCCSS = C_{SD} + \sum_{i=1}^{n} N_{SE,i} \cdot C_{SE,i}$$

Where the first term is cost for safety design (C_{SD}) while the second term is the sum of safety equipment cost. $C_{SE,i}$ is the purchase cost of equipment "i" and $N_{SE,i}$ is the number (count) of that equipment. Maintenance / repair cost are not

considered in this study. Second component of life cycle cost modeling is related to accident damage risk cost (ADRC) and incident damage risk cost (IDRC):

$$ADRC = \sum_{i=1}^{n} \dot{F}_{H,i} \cdot t_{op} \cdot (A_{D,i} \cdot C_{A,i} + C_{D,j} + N_{popeff} \cdot C_{H,life} + t_d \cdot \dot{C}_P) + \sum_{i=1}^{n} \dot{F}_{E,i} \cdot A_{ED,i} \cdot C_{ED,i} \cdot t_{op}$$

Here first term is the sun of asset lost cost, human health lost cost and production lost cost and second term is environment damage cost. $C_{A,i}$, $C_{D,j}$, $C_{H,life}$, C_P and $C_{ED,i}$ are asset cost ($/area),incident damage cost ($), value of human life ($/fatality), production value ($/h) and environment damage cost ($/area) respectively. $A_{D,i}$, $A_{ED,i}$ are property and environment damage area respectively. N_{popeff} is the number of people affected. t_{op} and t_d are operation time and down time respectively. $F_{H,i}$ is hazardous accident occurring frequency and $F_{E,I}$ is frequency of release of material to environment due to scenario "i".

$$IDRC = \left(\sum_{i=1}^{n} \dot{F}_S^{trip} \cdot t_{trip} + \sum_{i=1}^{n} \dot{F}_R^{trip} \cdot t_{dR} \right) \cdot \dot{C}_p \cdot t_{op}$$

Here t_{trip} and t_{dR} are downtime for spurious and required trip respectively.

$\dot{F}_S^{trip}$ and $\dot{F}_R^{trip}$ are spurious trip frequency and safe shut down frequency when demand of safety system arises. Once the relevent information such as reliability, consequence frequency and life cycle cost of each generated alternative have been obtained then final alternative is selected using MCDA analysis technique- (Promethee).

3. **Case study**

A distillation column unit from hydrocarbon recovery plant is used as case study. The simulation model in Aspen dynamics is shown in figure 2.

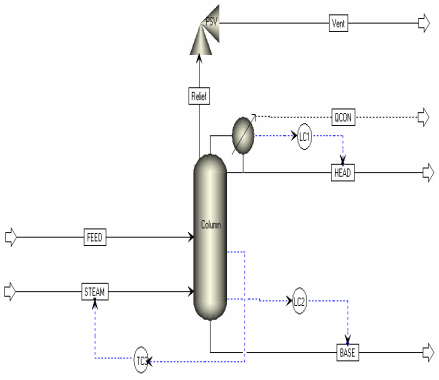
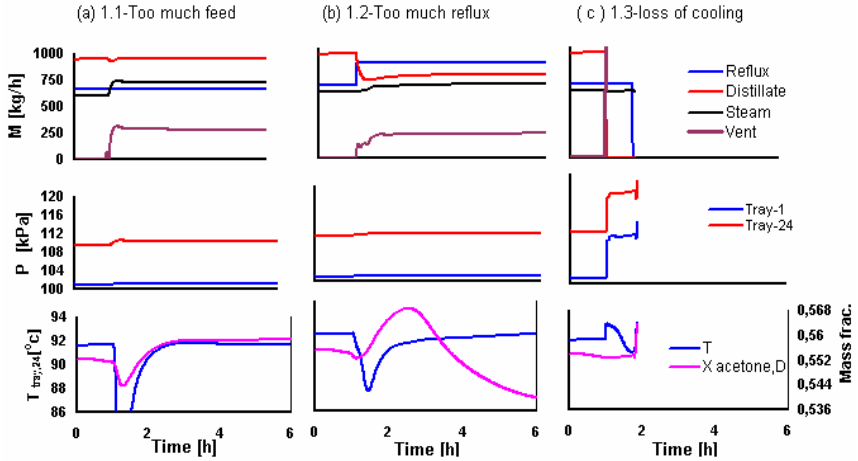


Figure 2 Process diagram

Extended Hazop methodology is applied for identification of operational failures and generation of safety related alternatives. Figure 3(a-c) shows the results of disturbance simulation for scenario 1.1 to 1.3 in Extended Hazop methodology worksheet (Figure 3). Figure 3(a) shows the simulation response for high feed input correspondence to maximum pump capacity (step change from 4000 kg/h to 5239 kg/h).

At the introduction of high feed, the control tray temperature falls down so to maintain the temperature, steam flow rate increased from 603 to 740 kg/h. The production rate and product quality first slightly disturbs for short moment but then it remains on its steady state value. This scenario will not affect reliability but cause release of material to atmosphere via vent. Figure 3(b) shows the simulation response for disturbance in reflux flow (step change from 666 kg/h to 865 kg/h). The high reflux flow results in decrease of distillate flow and product quality affecting the reliability of process. But again material via vent is released. Figure 3(c) shows the simulation response for total loss of cooling. At the introduction of failure of total loss of cooling, the column pressure raises sharply which results high release rate via vent line and reflux



Plant: DF **Process:** Stripping column						**Page No:** 1	
Equipment: TA01 **Function:** Separate HC's from effluent						**Document:** HI-1	
Volume: V1 **Conditions:** T_{24} = 91.3 °C; $P_{condenser} = P_{atm}$; M_F = 4000 kg/h						**Dated:** ----------	
Nr.	**Process Function/ Parameter**	**Detection**	**Possible Causes**	**Consequences**	**FC**	**Recommended Actions**	**FC**	**Ref Nr.**
1	More P > P_{normal} (bottom pressure)	Not direct	**1.1** [2]Too much feed (max pump cap. ,5239 kg/h)	**Physical effects:** - vapour flow greater then condenser capacity - [1]flooding because of down comer/tray capacity **Risk related consequences:** - production loss - release of material to atmosphere (300 kg/h)	23 58	-[5]pressure alarm - reduction of pump capacity -redundancy in control loop & set point limitation	43 ----	1-1
			1.2 [2]Too much reflux flow (666- 865 kg/h)	**Physical effects:** -change of temperature profile (fc) **Risk related consequences:** - product quality & controllability disturbs - release of material to atmosphere	23 58	[5]pressure alarm -redundancy in control loop & set point limitation	---- 52	1-2
			1.3 [2]Too less or loss of cooling capacity	**Physical effects:** - reflux drum may run dry - condenser capacity (go to zero) **Risk related consequences:** -product quality deteriorate -production loss -release of material to atmosphere via vent line which may or may not safely dispersed (1400 kg/h)	12 14 48	-pressure alarm and examine vent line capacity - [5]automatic ESD system	10 23 65	1-3

1. Short cut calculations 2.Dynamic simulation 3. Fault tree analysis 4. deterministic models 5. Event tree analysis

Figure 3 A sample result of Extended Hazop

and distillate falls to zero. The simulation stops in short time after this disturbance. This scenario is equally relevant for safety and reliability. The results are documented in Extended Hazop worksheet along with actions recommended. Similarly, other process deviations using guidewords are studied. Once this stage is completed, then analyzing the results with the help of risk potential matrix, five safety related modification proposals namely SS-A to SS-E from simple pressure alarm to PLC TMR shutdown systems are generated and evaluated by reliability modeling, life cycle cost modeling and safety analysis according to proposed methodlogy. The final ranking of the alternatives are obtained using Promethee giving equal preference to all objectives instead of traditional cost benefit analysis. Table 1 shows the alternatives generated and ranking obtained using multiobjective decision analysis technique-Promethee.

Table 1. Alternative proposals evaluation results and ranking

Safety alternative description	FR
SS-A:Manual shutdown system with 1oo2D configuration of pressure alarm system	1
SS-B: Remote shutdown system with 1oo2D configuration of pressure alarm system and 1oo2 configuration of shutdown valves	4
SS-C: Automatic shutdown system using Non redundant PLC System with 1oo2D configuration of pressure sensors and 1oo2 configuration of shutdown valves and parallel 1oo1 pressure alarm system	3
SS-D: Automatic shutdown using Relay Logic with 2 trip amplifiers and 4 relays with 1oo2D configuration of pressure sensors and 1oo2 configuration of shutdown valves and parallel 1oo1 pressure alarm system	5
SS-E: Automatic shutdown using PLC TMR System with 2oo3 configuration for sensor and 1oo2 configuration of shutdown valves and parallel 1oo1 pressure alarm system	2

Conclusions

Dynamic simulation is a power full tool for study of operational failures and quantification of Hazop. Safety proposals generated may be justified not only for personnel safety reasons, but also for reliability and total life cycle cost analysis.

References

1. Meel, A et al., 16th ESCAPE & 9th PSE proceedings, (2006) 1167
2. Can,U et al., Separation and Purification Technology, 29(2002) 163
3. Witt, W et al., Chem.-Ing.- Tech. 66,12(1994), 2646
4. Ramzan, N. et al., process safety progress, 26,1(2007) 35
5. Robert L. Post, Dennis C. Hendershot, and Patrick Kers, CEP,(2002),60