Merging safety and reliability analysis for process safety and reliability improvement

NAVEED RAMZAN, WERNER WITT

Lehrstuhl Anlagen und Sicherheitstechnik, Brandenburgicshe Technische Universität, Burger Chaussee 2 Lehrgebäude 4/5, Cottbus 03044, Germany,

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 also be justified by life cycle related cost benefits. In this contribution, a procedure that integrates process safety and reliability analysis with disturbance simulation is demonstrated. The quantitative merged process is based on multi-objective decision analysis technique (Promethee), Extended Hazop methodology (Hazop supported by dynamic simulation), reliability modeling and life cycle cost modeling. A distillation unit is used for illustration of procedure

Keywords: Life cycle cost, Multi-objective decision analysis, Extended Hazop, Disturbance simulation

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 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. Next, the safety systems may be justified not only for personal safety reasons, but for reliability and total life cycle cost benefits as well [2].

Qualitative techniques such as What if / Checklist analysis, Process hazard analysis (PHA), Hazard and Operability analysis (Hazop), Failure modes and effects analysis (FMEA) etc. and quantitative techniques such as Fault tree analysis, Event tree analysis etc. are in use for safety/risk analysis. Hazop is the standard technique often used in the chemical processing industry for assessment of new systems as well as modification to existing ones [3, 4]. Reliability block diagrams (RBD), Failure modes and effects analysis (FMEA), Fault tree analysis (FT), Event tree analysis (ET), Master logic diagrams (MLD) and Reliability-centered maintenance (RCM) are common techniques used for reliability analysis [5,6].

The techniques used to deal with safety analysis and reliability analysis have many similar activities so a merged process for safety and reliability analysis has several benefits. Few of them are:

1. better design and operation in terms of both safety and reliability,
2. better cost benefit in relation of analysis.

One example of such a merged qualitative process is HAZROP, which combines Hazop and RCM [6]. In recent years, dynamic simulation appears to be powerful for disturbance analysis safety examinations and several examples for its use for study of operational failures of chemical processes have been documented [7,8].

In this paper the objective is to present a quantitative merged procedure for safety and reliability analysis. The quantitative merged process is based on multi-objective decision analysis technique (Promethee), Extended Hazop methodology (Hazop supported by dynamic simulation), reliability modeling and life cycle related cost modeling. The objectives of the procedure may be:

1. improvement of plant safety and reliability,
2. reduction of environmental impact and overall annualized cost.

The paper is organized as follow. The basic aspects of disturbance simulation, safety and reliability analysis, life cycle related cost calculations and multi-objective decision analysis technique (Promethee) are explained first. Then, the proposed methodology for safety and reliability analysis is presented. Finally, the methodology is applied to a distillation unit.

Basic aspects of methodology presented

Disturbance simulation

Process disturbance simulation means use of dynamic simulation to study physical effects of large variations e.g. flow with respect to maximum/ no flow and loss of cooling water instead of small disturbances for control loop tuning or control system design [9]. Physical effects like under-pressure which results to reverse flow have to be considered in disturbance simulation but may be neglected for control loop tuning (fig. 1).

Safety/risk analysis vs. Reliability analysis:

Figure 2 describes the domain of safety and reliability analysis as well.

In reliability analysis we are looking for the answers of the following questions:

1.What can go wrong?
2.How likely it is?

But the goal is to pin point potential areas for reliability improvement by identifying the most likely failures and appropriate action to mitigate the effect of these failures.

For analyzing safety/risk, we are looking for types of risks we have to evaluate. The underlying concept of safety/risk analysis is to use techniques which offers the answers to following questions:

1. What can go wrong?
2. What are the consequences?
3. How likely it is?

* *email: ramzan50@hotmail.com, 0049-355-691138*

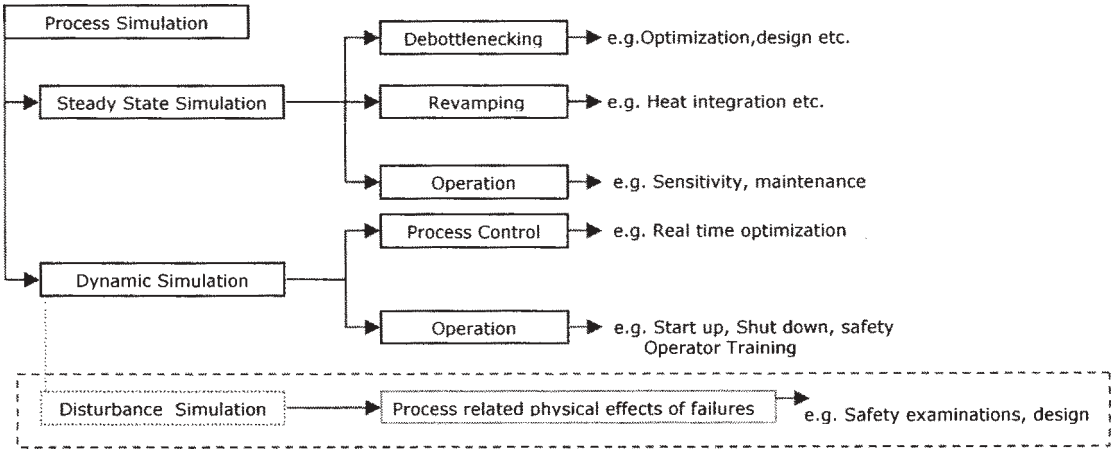


Fig. 1. Process simulation targets

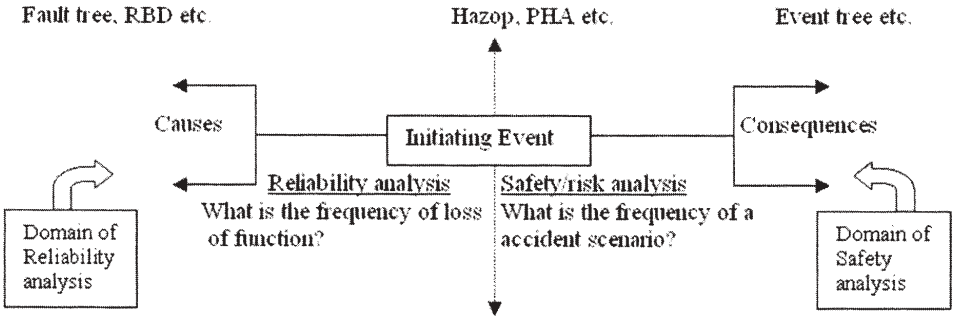


Fig. 2. Domains of Realiabilitz and Safetz analysis

Frequency F (1/yr) \ Consequence C ($)	0 (<10)	1 (10^1 – 10^2)	2 (10^2 – 10^3)	3 (10^3 – 10^4)	4 (10^4 – 10^5)	5 (10^5 – 10^6)	6 (10^6 – 10^7)	7 (10^7 – 10^8)	8 (>10^8)
>10^0	0								
10^{-1} – 10^0	1								
10^{-2} - 10^{-1}	2								
10^{-3} - 10^{-2}	3								
10^{-4} - 10^{-3}	4								
10^{-5} - 10^{-4}	5								
10^{-6} - 10^{-5}	6								
10^{-7} - 10^{-6}	7								
10^{-8} - 10^{-7}	8								
<10^{-8}	9								

Immediate action needed before further operation

Action at next occasion after qualification of analysis for improving system

Optional

No further action needed

Fig. 3. Risk potential matrix [9]

Extended Hazop methodology:

Extended Hazop methodology for safety/risk analysis presented by Ramzan et al. [9] is integrated in the quantitative merged process for safety and reliability analysis. Extended Hazop is performed to generate different safety related proposals along with identification of hazards. Extended Hazop differs from the standard Hazop approach in several aspects such as use of disturbance simulation, classification of risk consequence, classification of frequency, way of documenting the Hazop

discussion results and way of ranking the results. For risk assessment, risk potential matrix is used (fig. 3). 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.

Life cycle related cost modeling:

Life cycle cost requires calculation of initial fixed cost (i.e. cost for designing, purchasing, installing, commissioning and operating the system) and annual costs (i.e. maintenance and other ongoing costs such as incident and accident related costs associated with the system). Life cycle related cost modeling used here is:

$$LCC = FCISS + ADRC + IDRC \quad (1)$$

where

FCISS = Fixed capital investment of safety system

ADRC = Accident damage risk cost , IDRC = Incident damage risk cost

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

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

$$FCISS = C_{SD} + \sum_{i=1}^{n} N_{SE,i} \cdot C_{SE,i} \quad [\$] \quad (2)$$

Where the first term 'C_{SD}' is cost for safety system design, installation and commissioning. While the second term is the sum of safety equipment purchased 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).

$$ADRC = \sum_{i=1}^{n} \dot{F}_{H,i} \cdot t_{op} \cdot (A_{D,i} \cdot C_{A,i} + C_{D,j} + N_{pop,eff} \cdot C_{H,life} + t_d \cdot \dot{C}_p) + \sum_{i=1}^{n} \dot{F}_{E,i} \cdot A_{ED,i} \cdot C_{ED,i} \cdot t_{op} \quad [\$] \quad (3)$$

Here first term is the sum 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 loss 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/equipment and environment damage areas respectively. $N_{pop,eff}$ is the number of people affected. t_{op} and t_d are operation time and down time respectively.

$\dot{F}_{H,i}$ is hazardous accident occurring frequency and $\dot{F}_{E,i}$ is frequency of release of material to environment due to scenario "i".

Third component of life cycle cost modeling is related to incident damage risk cost.

$$IDRC = \left(\sum_{i=1}^{n} \dot{F}_S^{trip} \cdot t_{trip} + \sum_{i=1}^{n} \dot{F}_R^{trip} \cdot t_{dR}\right) \cdot \dot{C}_p \cdot t_{op} \quad [\$] \quad (5)$$

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

F_s^{ttrip} and F_R^{ttrip} are spurious trip frequency and safe shut down frequency when demand of safety system arises.

Multi-objective decision analysis technique (Promethee):

An array of techniques for multi-objective decision analysis have been developed by researchers [10] but very rarely applied to support decisions in the field of process engineering according to our knowledge. The technique integrated in the proposed methodology of combined quantitative safety and reliability analysis to support multi-objective decisions is based on the method of outranking called Promethee (Preference ranking organization method of enrichment evaluation).

Figure 4 shows the implementation procedure of Promethee and relationships used to determine the ranking. The implementation procedure (shown in fig. 4) is built on the basic notation:

- with a set "A" of 'n' alternatives that must be ranked and 'm' objectives that must be optimized,

$A = \{A_1, ... A_k, A_l, ... A_n\}$: Set of 'n' discrete alternatives, i = 1, 2,..., k, l,...., n

$C = \{C_1, C_2 ..... C_m\}$: Set of 'm' relevant objectives, j = 1,2,.... m

then $C_j(A_k)$ represents the value of objective j for alternative A_k . Therefore, the evaluation matrix which represents the multi-objective decision analysis problem is shown in table 1.

- $\Pi(A_k, A_1)$ is the preference index describing the credibility of the outranking relation that ,alternative A_k is better than alternative A_1, for each pair of alternatives.

- $P_j(A_k, A_1)$ is the preference function for the pair of alternatives A_k and A_1 with respect to objective j. Its value ranges between 0 to 1 and calculated by using thresholds $p(C_j)$, $q(C_j)$with respect to objective j. These threshold values for each objective comes from the decision maker or are calculated as follow:

$$p(C_j) = C_j(A_i)_{max} - C_j(A_i)_{min} \quad (6)$$

$$q(C_j) = 0.1 \cdot \{C_j(A_i)_{max} - C_j(A_i)_{min}\}, \quad (7)$$

where choice of 0.1depends on decision maker

- w_j is the weight given to objective j

- $\phi(A_k)$ is the net preference flow of alternative A_k. A higher value of net preference flow gives a higher rank.

Methodology of integrated safety and reliability analysis with cost modeling

Figure 5 shows the block diagram of the proposed systematic procedure.

Table 1

EVALUATION MATRIX

Objectives / Alternatives	C_1	C_2	C_3	-	-	C_m
A_1	$C_1(A_1)$	$C_2(A_1)$	$C_3(A_1)$	-	-	$C_m(A_1)$
A_2	$C_1(A_2)$	$C_2(A_2)$	$C_3(A_2)$	-	-	$C_m(A_2)$
-	-	-	-	-	-	-
A_n	$C_1(A_n)$	$C_2(A_n)$	$C_3(A_n)$	-	-	$C_m(A_n)$

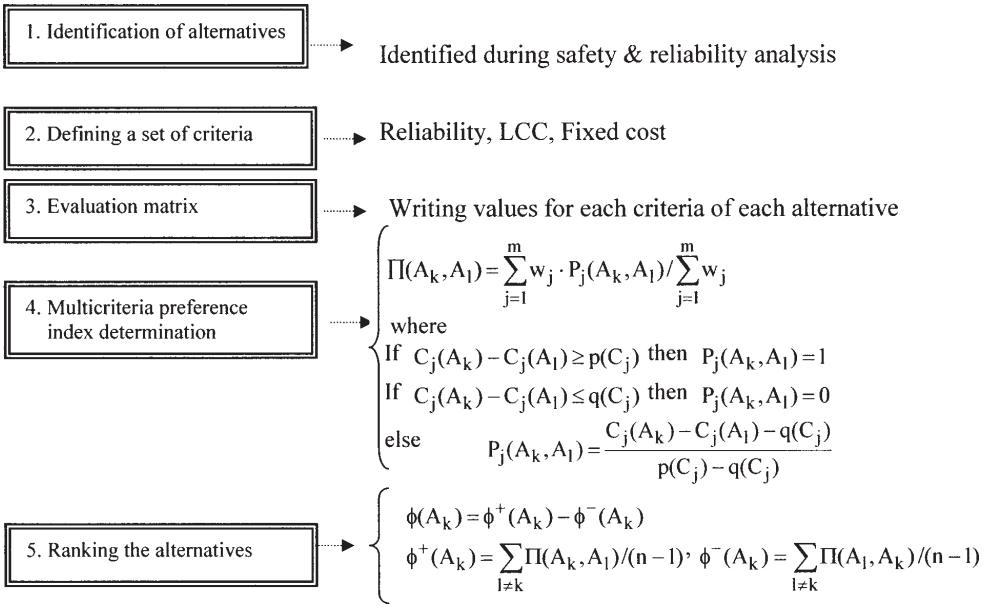


Fig. 4. Implementation procedure of Promethee

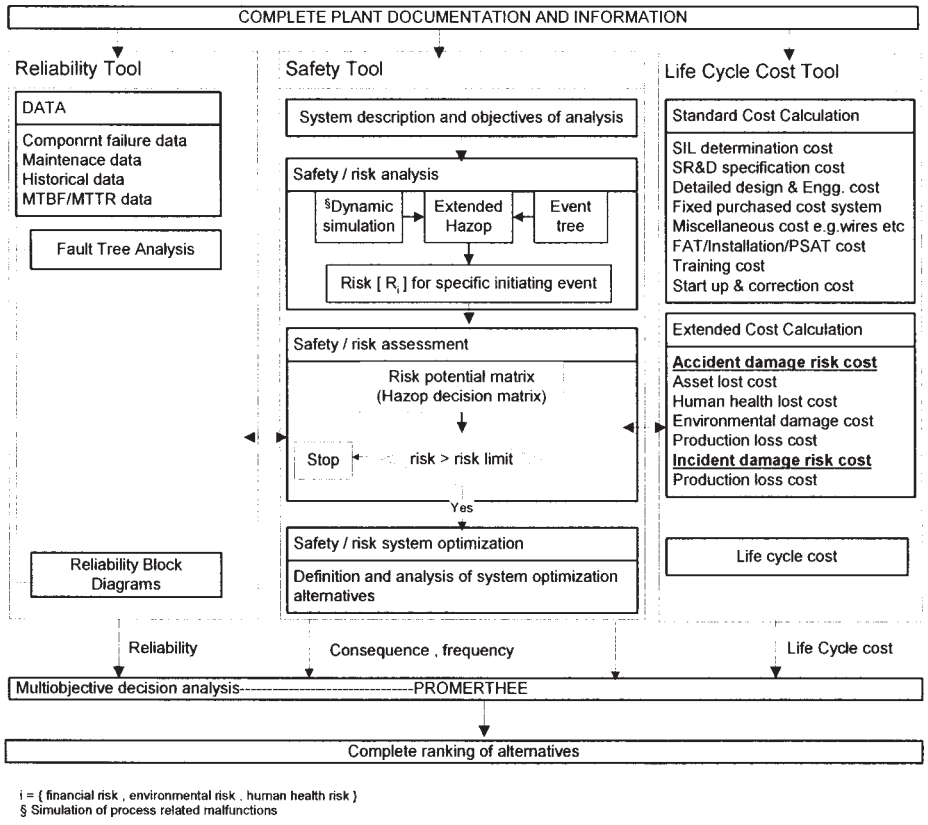


Fig.5. Quantitative procedure for integrated safety and reliability analysis

The reliability tool is used for calculation of reliability values. Within the safety tool incident and accident risks are calculated and evaluated. The life cycle cost tool considers incident (process interruption) and accident (damage) cost calculation.

The reliability analysis is combined with Extended Hazop methodology as follows:

- First, at weak point identification stage to identify critical equipment or instrument for reliability as well as frequency of occurring incident/accident scenarios. These incident / accident frequencies are used to calculate incident (process interruption) and accident related risk costs.

- Then, Hazop decision matrix (risk potential matrix) is used to decide the need of improvement proposals for elimination of both incident and accident scenarios.

- Next, improvement proposals developed will be analyzed in relation to reliability, risk and life cycle cost.

- Finally, alternatives are ranked using MCDA analysis technique- Promethee.

Case study

A distillation unit from hydrocarbon recovery plant is used for the case study. Water, acetone, methanol, and acetic acid are the main components of the feed stream. The product stream (acetone rich) is separated from the effluent by using live steam injection. The column has a

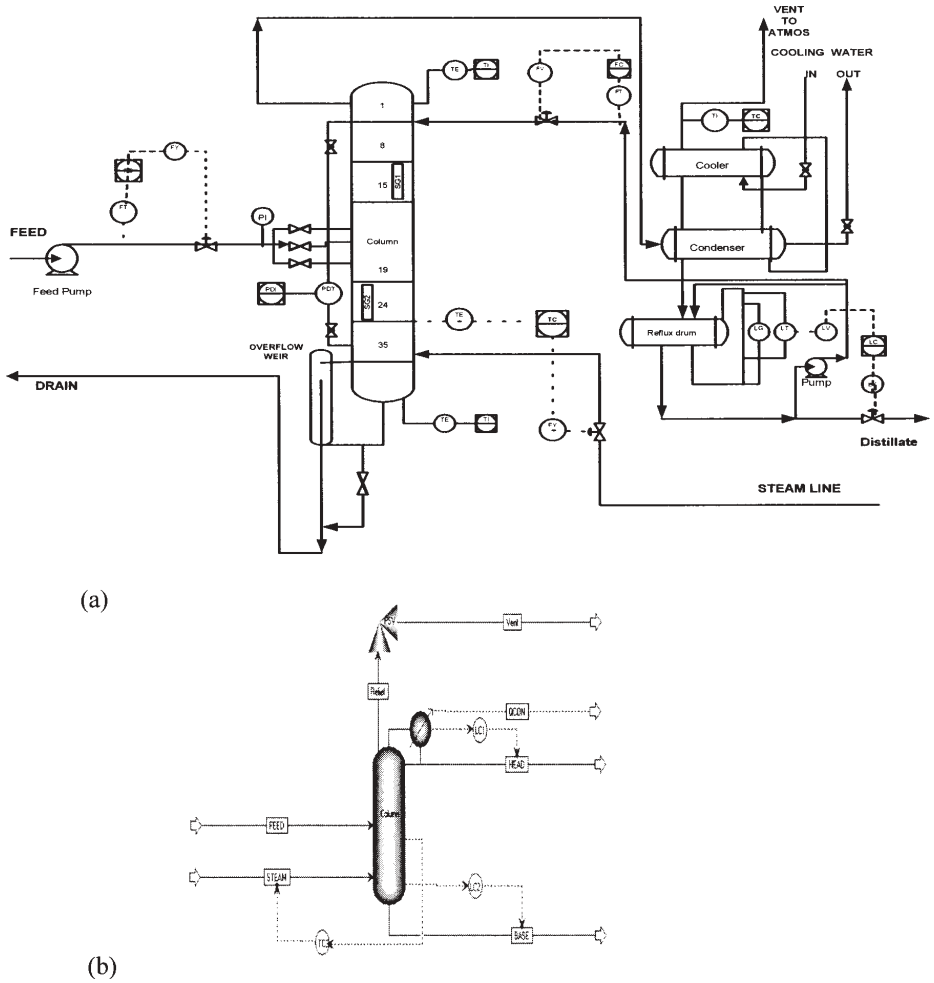


Fig.6. Process flow diagram and simulation model

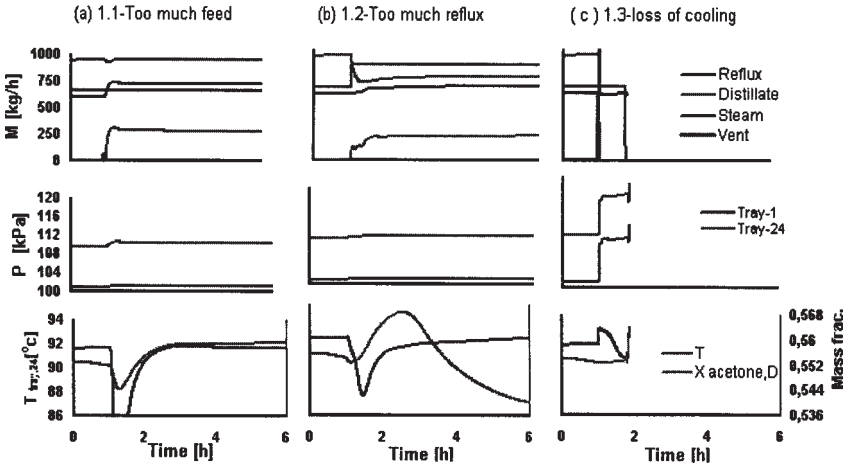


Fig.7. Disturbance simulation results

diameter of 0.728 m and consists of 35 trays. The live steam is entered at stage 35 at a temperature of 141 C and a pressure of 375 kPa. The feed, which is at its bubble point, is entered at stage 16 (the stages are numbered from top to bottom) with a column head pressure of 100 kPa. The separation targets (mass %) are:

Distillate: water < 10%
Bottom: acetone < 2000 ppm, methanol < 2%, acidity < 3%

Where acidity is the sum of the mass fraction of the acids, i.e. acetic acid, formic acid and propionic acid.

The feed rate is about 4000 kg/h. The temperature at stage 24 is controlled via modification of the steam rate. The design temperature of the column is 115 C and design pressure is 190 kPa. The simplified process diagram and simulation model configured in Aspen dynamics is shown in figure 6(a & b). Details of the aspen dynamics model configured can be found at [11].

Extended Hazop methodology is applied for identification of operational failures and generation of safety related alternatives. Figure 7(a-c) shows results of disturbance simulation for scenario 1.1 to 1.3 in Extended Hazop methodology worksheet (table 2). Figure 7(a) shows the simulation response for high feed input

Table 2

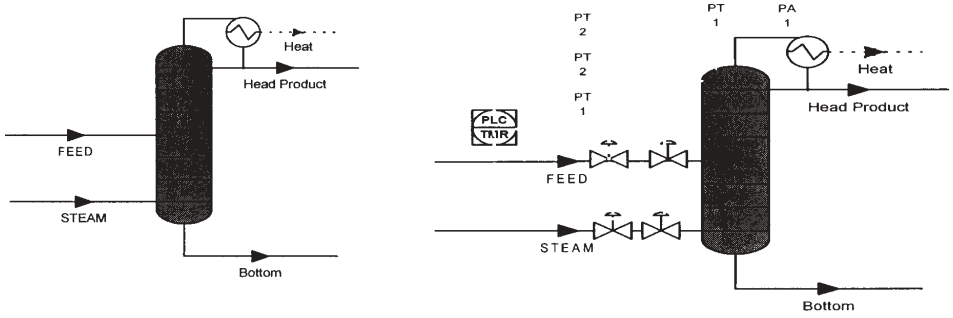
A SAMPLE RESULT OF EXTENDED HAZOP

Plant:	DF	**Process:**	Stripping column	**Page No:**	1
Equipment:	T1701	**Function:**	Separates HCs from effluent stream	**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 (4h) release of material to atmosphere (300 kg/h) for 1 h	23 58*	-[5]pressure alarm - reduction of pump capacity -redundancy in control loop & set point limitation	43 75	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	---- 75	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) for short period of time t = 3 min	12 14 48*	-pressure alarm and examine vent line capacity - [5]automatic ESD system	10 23 75	1-3

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

*Worst consequence is documented here from event tree analysis



Base Case SS-E

Fig.8. From base case to optimized system (SS-E)

correspondence to maximum pump capacity (step change from 4000 kg/h to 5239 kg/h).

At change of feed to maximum, the control tray temperature falls down. To maintain the temperature, steam flow rate increased from 603 to 740 kg/h. The product quality slightly disturbs for short moment but then it remains on its steady state value. This scenario caused release of material (approximately 300 kg/h) to atmosphere via the vent. Figure 7(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 is released via the vent. Figure 7(c) shows the simulation response for total loss of cooling. At total loss of cooling, the column pressure raises sharply which results high release rate (1400 kg/h) via the vent. Reflux and distillate streams fall to zero. The simulation stops after this disturbance because of numerical problem. The results are documented in Extended Hazop worksheet (table 2) along with actions recommended. Pre and post incident event trees are constructed to determine frequency class of risk consequences and consequence category for each scenario. Similarly, other process deviations are studied. The results from Extended Hazop worksheets are documented in the risk potential matrix. Scenarios having similar risk category are clustered. Recommended optimization proposals developed are analyzed.

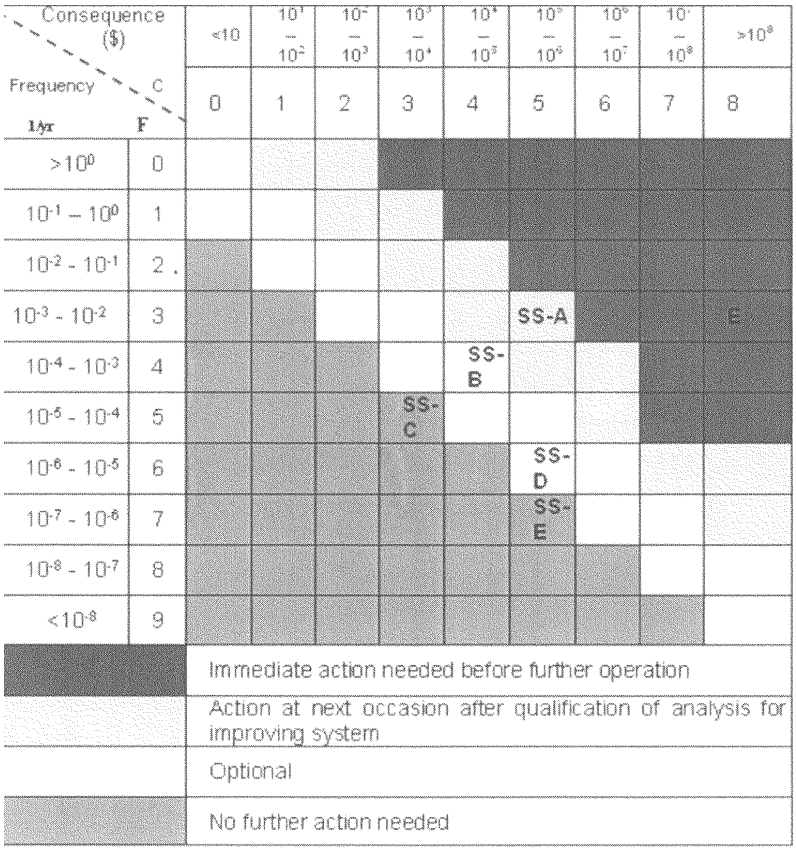
For further discussion we will rely on the most serious scenarios (cause 1.1, FC 58; cause 1.2, FC 58; cause 1.3, FC 48) mentioned in table 2. For these scenarios, five safety related modification proposals from simple pressure alarm system (SS-A) to PLC TMR shutdown system (SS-E) are developed. Figure 8 shows the PLC TMR shutdown system. table 3 describes all of the alternative proposals along with accident frequency obtained after implementation. Figure 9 shows the risk potential for the worst scenarios.

Reliability of each modification proposal is evaluated by drawing modified reliability block diagrams (RBD). Figure 10 shows RBD for alternative proposal SS-A.

Life cycle cost modeling and safety analysis according to proposed methodology is carried out for each safety

Table 3
ALTERNATIVE BASE CASE TO OPTIMIZED SYSTEM (SS-E)

Safety alternative description	Accident frequency 1/yr
SS-A: Manual shutdown system with 1oo2D configuration of pressure alarm system	2.9×10^{-3}
SS-B: Remote shutdown system with 1oo2D configuration of pressure alarm system and 1oo2 configuration of shutdown valves	5.1×10^{-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	3.6×10^{-5}
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	9.46×10^{-6}
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	1.12×10^{-6}



E...represents base case

Fig. 9. Risk potential matrix

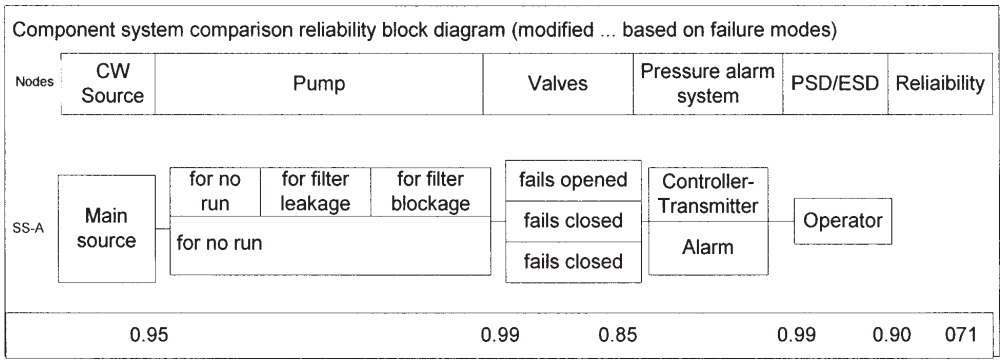


Fig. 10. System Reliability calculation for Case SS-A

alternative generated. Table 4 gives the evaluation matrix obtained after safety analysis, reliability modeling and life cycle cost modeling.

Next, a pair wise comparison is made and a preference index matrix is developed (table 5). Equal weights are given to all objectives for calculation of preference index matrix.

Table 4
EVALUATION MATRIX

	SS-A	SS-B	SS-C	SS-D	SS-E	P	q
Reliability	0.71	0.75	0.79	0.78	0.79	0.08	0.008
LCC	6456674	3736396	3225816	3191037	3208455	3265637	326563
FCISS	35000	58000	93000	88000	115000	80000	8000

Table 5
PREFERENCE INDEX MATRIX

	SS-A	SS-B	SS-C	SS-D	SS-E
SS-A	0	0.2715	0.3294	0.3333	0.3313
SS-B	0.2715	0	0.0209	0.0248	0.0228
SS-C	0.5648	0.2731	0	0.0093	0
SS-D	0.4954	0.2037	0	0	0
SS-E	0.6667	0.3981	0.0648	0.0972	0

Table 6
FINAL RANKING OF ALTERNATIVES

Safety alternative description	Entering preference flow	Leaving preference flow	Net preference value	Final Ranking
SS-A	0.3164	0.4861	- 0.1697	4
SS-B	0.0715	0.2866	- 0.2151	5
SS-C	0.2118	0.1038	0.1080	2
SS-D	0.1748	0.1162	0.0586	3
SS-E	0.3067	0.0885	0.2182	1

The final ranking of the alternatives from this preference index matrix is obtained by calculating the net preference flow. Higher value of this flow gives high rank. Table 6 shows the final ranking and net preference flow values calculated.

Conclusions

In this paper, an integrated methodology for safety and reliability analysis, life cycle cost calculation and optimization is presented. The methodology is illustrated with a distillation unit case study. The main conclusions drawn from the case study are:

- The combination of reliability modeling, life cycle cost calculation and safety risk analysis techniques (methodology applied) with the help of the optimization technique Promethee did result in qualified ranking.
- The methodology applied gives more insight into process design and helps in making multi-objective decision.
- The most complex part of the methodology is the safety risk analysis.
- As far as results from safety risk analysis are known, the methodology can be automated.
- The methodology can be applied to other unit operations as well.

References

1.MEEL, A. et al., Real time failure prediction for chemical processes: Plant wide framework",16th ESCAPE & 9th PSE proceedings, 2006, p. 1167

2.GRUHN, P.E. PAUL., HARRY, L.,CHEDDIE, P.E., Safety Instrumented Systems: Design, Analysis and Justification, ISA-The instrumentation, systems, and automation society,2nd Ed., 2006, p. 241

3.*** CCPS-Center for Chemical Process Safety, Guide lines for Hazard Evaluation Procedures, Center for Chemical Process Safety, American Institute of Chemical Engineers, New York ,1992, p. 131

4.GROSSMAN, G., FROMM, D., HAZOP, Proof Ammonia Plant: A new way of defining a safe and reliable design" Plant/Operations Progress, 10, nr. 4,1991, p. 223

5.ANDREWS, J. D., MOSS. T. R., Reliability and risk assessment, 2nd Ed., Professional Engg. Publishing, U.K., 2000

6.ROBERT L. P., HENDERSHOT, D.C., KERS, P., Synergistic design approach to safety and reliability yields great benefits" CEP, 2002, p. 60

7.CAN, U., JIMOH, M., STEINBACH, J., WOZNY G., Simulation and Experimental Analysis of Operational Failures in a distillation column, Separation and Purification Technology, 29, 2002, p. 163

8.DEERBERG, G., SCHLÜTER, S., STEIFF, A., WITT, W., Simulation of Operational failures in two-phase semi batch processes, Chem. Eng. Sci., **51**, nr. 11, 1996, p. 3113

9.RAMZAN, N., COMPART, F., WITT, W., Methodology for generation and evaluation of safety system alternatives based on extended Hazop and event tree analysis process safety progress, 26, nr. 1,2007, p. 35

10.KANGAS, A., KANGAS, J., PYKÄLÄINEN, J., Outranking methods as tools in strategic natural resources planning, Silva Fennica research articles, 35, nr. 2, p. 215

11.RAMZAN, N., COMPART, F., WITT, W., Application of extended Hazop and event tree analysis for investigating operational failures and safety optimization of distillation column unit" accepted for publication in process safety progress

Manuscript received: