Reliability of safety systems and probabilistic risk assessment

Sebastián Martorell, Isabel Martón, Maryory Villamizar
Chemical and Nuclear Department Polytechnic University of Valencia
Camino de Vera, 14 (46022) Valencia, Spain

This article studies the influence of each component reliability in the total system reliability, and their impact on the risk assessment and management of a given accident scenario. The measures considered in this paper to increase the equipment reliability and to reduce the global risk are traditional ones, being among others: redundancy and diversity of safety trains, identification of equipment and failure modes of greatest impact on risk estimation, and the adoption of appropriate testing and maintenance policies.

1. Introduction

The calculation and control of reliability of safety related systems is of vital importance in order to obtain proper safety evaluation and management at industrial installations, and a complete risk analysis. In order to estimate the risk associated with an accident scenario, it is necessary the estimation of, not only the corresponding consequence and damage, but also its frequency of occurrence. Event tree analysis is normally performed to develop the logical model representing the different accident scenarios departing from an initiating event. Such a logic model allows the estimation of the frequency of a particular accident scenario derived as a function of the initiating event frequency and the reliability of each safety system, including those that perform prevention and protection functions, designed to reduce the accident frequency and mitigate the accident consequence (Kalantamira et al, 2009). Fault tree analysis is usually adopted to represent and estimate the failure probability of the safety system, being a measure of the system reliability, as a function of the probability of failure of its components, the last being a measure of the component reliability. The methodology to calculate the reliability and risk is applied in this paper to an ethylene oxide storage plant, considering accident scenarios departing from the loss of the normal cooling system.

2. Systems description

The choice of ethylene oxide is based on its properties and characteristics of storage. It is a flammable, toxic substance and it is stored in liquefied state, so it constitutes a good example for the demonstration of the complementary role of reliability analysis and probabilistic risk assessment for a better risk assessment and safety management. The pressure and temperature storage conditions are four bars and 10ºC, respectively.
It is assumed that the facility, in particular the pressurised and refrigerated storage tank is provided of all necessary safety systems. These include the systems that are directly

affected by the accidental scenario following the loss of the normal cooling system. These safety systems are:

- *Emergency cooling system (ECS):* This system acts after a failure of the normal cooling system.
- *Transfer system (TRS):* This system transfers the ethylene oxide from the storage tank to an auxiliary tank.
- *Spray system (SPS):* This system is responsible of cooling the storage tank after a failure of the normal and emergency cooling systems, given a failure of the transfer system, is produced. Coupled to this system there is an auxiliary water storage that must guarantee the capability of the spray system.
- *Relief valves system (RVS):* It is composed by two safety-relief valves. It provides the last safety measure to prevent a tank explosion due to an overpressure if the previous safety functions have failed. Valves open automatically to keep the pressure under control, although this action means there is a release of gas into the atmosphere

All these systems except the last one are controlled by a safety instrumented system (MDS). This system consists of temperature and pressure sensors and transmitters. The last ones send the signal to logical solvers that are responsible of the actuation of the controlled valves and pumps. The MDS acts in case of a high temperature /pressure beyond the safety limits is detected.

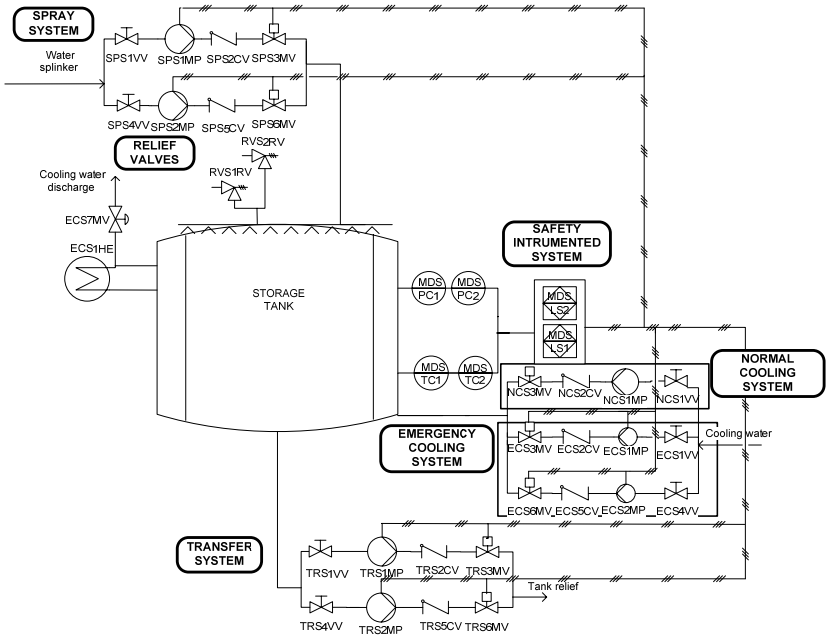

Figure 1. Ethylene oxide storage tank

3. Event tree analysis of accidental scenarios

The accident scenario being studied is caused by a loss of the normal cooling system of ethylene oxide storage tank. Consequently there is an increase in the temperature inside tank. This situation leads to a temperature transient that, simultaneously, generates a gradual increase in the pressure of the tank. At this time, storage conditions would be

out of control and the previous technological safeguards should act.(Bernatik and Libisoka, 2004) The accidental scenarios following the loss of normal cooling are represented with an event tree in figure 2.

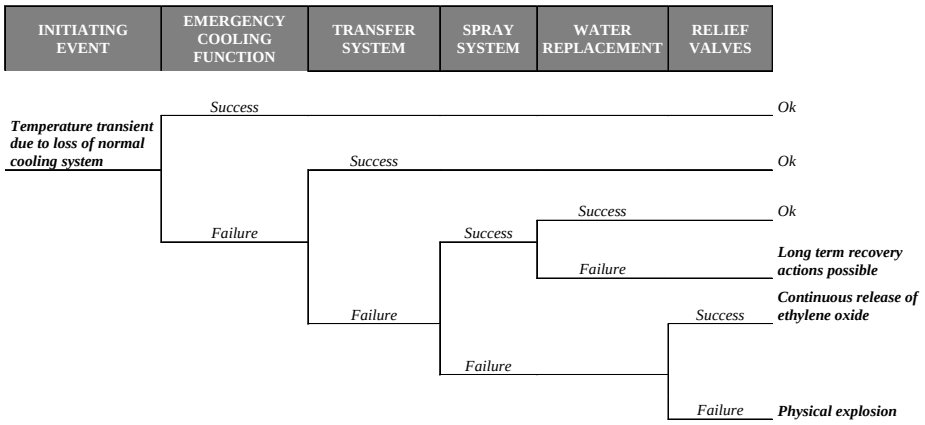

Figure 2. Event tree

4. System reliability modelling using fault trees

System reliability analysis is the step prior to calculate the frequency of a given accident scenario. To calculate the system reliability, one must first calculate the reliability of each component individually, using, an appropriate database which contains real component failure data. Depending on the operation mode of the equipment the database provides the necessary values of failure rates: mission failure rates (λ_M) standby failure rates (λ_S) and per demand failure probabilities (ρ). The following mathematical expressions are used to represent the component reliability depending on the operation mode and failure above:

- *Failure probability in standby:* Components normally in standby that fail when are required to operate. Typically, these devices undertake test with period T to detect hidden failures.

$$P_S = 1/2 \cdot \lambda_S \cdot T \quad (1)$$

- *Failure probability per demand:* It is used when the component is activated to change it state. This type of model has no time-dependent behaviour.

$$P_D = \rho \quad (2)$$

- *Mission failure probability:* It occurs in components which fail during the operation time.

$$P_M = \lambda_M \cdot t_M \quad (3)$$

Table 1, shows the reliability models and data used for several components of the safety systems under study. The reliability of a system depends on both, the individual reliability of each of its components and the logical path in which these components are connected with the system operation. The fault tree analysis technique has been used to

represent the logical path and to estimate the failure probability of safety systems as a function of component failure probability that is derived using the previous formulation and data.

Table 1. Reliability and data of safety systems components

COD	SUBTYPE	GENERAL FAULT MODE	λ_S (hr^{-1})	λ_F (hr^{-1})	ρ	T (h)	t_M (h)	P_S	P_F	P_D
VV	Manual	Fail to remain open			3,00E-05					3,00E-05
MP	Motor driven	Fail to run/Fail to start	1,00E-05	2,88E-05	5,74E-03	8760	8	4,25E-02	2,30E-04	5,74E-03
CV	Self operated	Fail to remain open	1,45E-07			8760		6,35E-04		
MV	Motor operated	Fail to open on demand /Fail to open due to standby failure	9,67E-06		2,48E-03	8760		4,12E-02		2,48E-03
MV	Motor operated	Fail remain closed		8,25E-07			8760		7,20E-03	
TC	Temperature	Fail to function		3,39E-06			8760		2,93E-02	
PC	Pressure	Fail to function		2,51E-06			8760		2,17E-02	
LS	Programable safety system -single system	Fail to function	3,46E-06			8760		1,50E-02		
RV	Self operated	Fail to open on demand	2,73E-06		3,11E-03	8760		1,19E-02		3,11E-03
HE	General	Fail to leackage, plug		2,63E-06			8760		2,29E-02	

5. Assessment of the relevant scenarios

The initiating event is a temperature transient caused by the loss of the normal cooling system. This system consists of a manual valve (NCSVV01), control valve (NCSCV02) and a motorized valve (NCSMV03); and a pump (NCSMP01) arranged in series, as shown in figure 1.

To determine the initiating event frequency, it suffices to sum up the frequency of occurrence of failure for each one of the components in the train. The frequency of this initiating event has been estimated to be approximately once per year.

The present study does not address the frequency of consequences that might result in long-term challenges, since it is assumed one could have available recovery actions, even of the failed systems. The frequencies of accident scenarios leading to continuous release and physical explosion have been calculated. The calculation of the frequency of each accident is derived using the frequency of the initiating event, the corresponding fault trees and the appropriate component reliability models and data as described in the previous section. The results obtained for continuous release and physical explosion are 2, 28E-04 yr^{-1} and 5, 09E-08 yr^{-1}, respectively.

6. Management measures of the relevant scenarios

After performing the previous assessment, the contribution/importance of the minimal cut sets (MCS) and the degree of importance of the component failures involved in the

accidental sequences corresponding to the continuous leakage (table 2 and 3) and the physical explosion (table 4 and table 5), can be obtained.

Table 2. Continuous release minimal cut sets contribution

No.	Freq.	%	Q	Event	Description
1	2,251E-04	98,72	1,000E+00	TT	Temperature transient
			1,500E-02	FMDSLS01S	Failure in standby of the logic solver MDSLS01
			1,500E-02	FMDSLS02S	Failure in standby of the logic solver MDSLS02
2	4,049E-07	0,18	1,000E+00	TT	Temperature transient
			2,175E-02	FMDS01PCF	Failure to function of pressure controller MDSPC01
			2,926E-02	FMDS01TCF	Failure to function of temperature controller MDSTC01
			2,175E-02	FMDS02PCF	Failure to function of pressure controller MDSPC02
			2,926E-02	FMDS02TCF	Failure to function of temperature controller MDSTC02

Table 3. Continuous release importance measures of components failures

No.	ID	Description	Nom.val.	FV	FC	RDF	RIF	Sens.
1	TT	Temperature transient	1,000E+00	1,000E+00	1,000E+00	9,990E+99	9,990E+99	1,000E+02
2	FMDSLS01S	Failure in standby of the logic solver MDSLS01	1,500E-02	9,872E-01	9,872E-01	7,803E+01	6,581E+01	8,862E+01
3	FMDSLS02S	Failure in standby of the logic solver MDSLS02	1,500E-02	9,872E-01	9,872E-01	7,803E+01	6,581E+01	8,862E+01
4	FECS01HEF	Failure in function of the heat exchanger ECSHE01	2,286E-02	6,675E-03	6,571E-03	1,007E+00	1,281E+00	1,065E+00

Table 4. Phsical explosion minimal cut sets contribution

No.	Freq.	%	Q	Event	Description
1	3,167E-08	62,27	1,000E+00	TT	Temperature transient
			1,500E-02	FMDSLS01S	Failure in standby of the logic solver MDSLS01
			1,500E-02	FMDSLS02S	Failure in standby of the logic solver MDSLS02
			1,186E-02	FRVS01RVS	Failure in standby of the relief valve RVSRV01
			1,186E-02	FRVS02RVS	Failure in standby of the relief valve RVSRV02
2	8,304E-09	16,33	1,000E+00	TT	Temperature transient
			1,500E-02	FMDSLS01S	Failure in standby of the logic solver MDSLS01
			1,500E-02	FMDSLS02S	Failure in standby of the logic solver MDSLS02
			1,186E-02	FRVS01RVS	Failure in standby of the relief valve RVSRV01
			3,110E-03	FRVS02RVA	Failure to open on demand of the relief valve RVSRV02

Table 5. Physical explosion importance measures of components failures

No.	ID	Description	Nom.val.	FV	FC	RDF	RIF	Sens.
1	TT	Temperature transient	1,000E+00	1,000E+00	1,000E+00	9,990E+99	9,990E+99	1,000E+02
2	FMDSLS02S	Failure in standby of the logic solver MDSLS02	1,500E-02	9,872E-01	9,872E-01	7,803E+01	6,581E+01	8,862E+01
3	FMDSLS01S	Failure in standby of the logic solver MDSLS01	1,500E-02	9,872E-01	9,872E-01	7,803E+01	6,581E+01	8,862E+01
4	FRVS02RVS	Failure in standby of the relief valve RVSRV02	1,186E-02	7,942E-01	7,918E-01	4,802E+00	6,695E+01	2,827E+01
5	FRVS01RVS	Failure in standby of the relief valve RVSRV01	1,186E-02	7,942E-01	7,918E-01	4,802E+00	6,695E+01	2,827E+01
6	FRVS01RVA	Failure to open on demand of the relief valve RVSRV01	3,110E-03	2,082E-01	2,058E-01	1,259E+00	6,695E+01	3,500E+00
7	FRVS02RVA	Failure to open on demand of the relief valve RVSRV02	3,110E-03	2,082E-01	2,058E-01	1,259E+00	6,695E+01	3,500E+00

A result of the previous analysis shows that there is only one minimal cut set with a 98.72% contribution to the frequency of occurrence of the continuous release. In addition the most important basic events are the failure in standby of the logic solver according to the fussel vesely (FV) and risk increase factor (RIF) importance measures. The first of these values indicates the basic event contribution to the continuous release accident frequency, and the second the vulnerability of the facility introduced by those basic events the component failure based on this accident scenario. As observe in tables 2 and 3, the most important basic events identified as major contributors to the accident probability (FV) are also the ones that introduce greater plant vulnerability (RIF).

The analysis of the minimal cut sets and the FV and RIF importance measures corresponding to a physical explosion shows that the percentages in the MCS are distributed in a most equitable way. The basic events of explosion accidental scenario that have major contribution in risk are the failure in standby of the relief valves and the logic solver. The minimal cut sets corresponding the above basic events presents a percentage of 62.27 % to the frequency of physical explosion occurrence. Also, in this

case, the most important basic events identified as major contributors to the accident probability (FV) are also the ones that introduce greater plant vulnerability (RIF), as shown in table 4 and table 5.

To observe the impact reliability improvement, based on the relevant basic events on the reduction of accidents frequency, the following improvements are considered in a sensibility study (Martorell et al, 2005):

1) Redundancy. Another device in parallel is introduced in the design. This actions increase the system reliability.

- *Add a third logic solver*
- *Add a third relief valve*

2) Modification of the test interval from 1 year to six months: When test interval is reduced. Failure probability is reduced according with equation 1.

3) Modification of failure rate: The failure rate of a safety device approximately lowered 10 times to represent a more reliable component.

- *Modification of safety valve failure rate*
- *Modification of motor driven pump failure rate*

4) Combinations of the above options.

- *Add a logic solver and modification of test interval for logic solver only to six months*

The results obtained show that the frequency of accidental consequences is decreased by the proposed measures. The most efficient measure is the last sensitivity study proposed, as shown in the table 6.

Table 6. Frequency results of accidental consequences of the studied measures

	Continuous release (yr^{-1})	*Physical Explosion (yr^{-1})*
System (figure 1)	2,28E-04	5,09E-08
Add logic solver	6,30E-06	1,41E-09
Add relief valve	2,28E-04	7,60E-10
Test interval-6 months	5,74E-05	4,70E-09
Modification Relief valve failure rate	2,28E-04	4,11E-09
Modification Motor driven pump rate	2,26E-04	5,04E-08
Add logic solver-logic solver test interval 6 months	3,35E-06	7,47E-10

7. Conclusions

The combined use of event tree analysis and fault tree analysis allows assessing the risk and impact of the component and safety systems reliability in a given accidental scenario. Using this model it is possible to study quantitatively the improvements in the system components and their impact on reliability and risk minimization.

References

Marorell S., Villanueva J.F, Carlos S., Nebot Y., Sanchez A., Pitarch J.L. and Serradell V., 2005, RAMS +C informed decision-making with application to multi-objective optimization of technical specifications and maintenance using genetic algorithms, Reliability engineering and system safety,87, 65-75.

Bernatik A., Libisoka M, Loss prevention in heavy industry: risk assessment of large gasholders, 2004, Journal of loss prevention in the process industries, 17, 271-278

Kalantamira M., Khan F., Hawboldt K., 2009, Dynamic risk assessment using failure assessment and Bayesian theory, Journal of loss prevention in the process industries, 22, 600-606.