FAULT TREE ANALYSIS FOR RISK ASSESSMENT IN THE BOREXINO EXPERIMENT

Antonio C. Caputo
University of L'Aquila, Faculty of Engineering, 67040 Monteluco, L'Aquila, Italy
caputo@ing.univaq.it

Mario Palumbo
University of L'Aquila, Faculty of Engineering, 67040 Monteluco, L'Aquila, Italy
palumbo@ing.univaq.it

Roberto Tartaglia
Gran Sasso National Laboratory, National Institute for Nuclear Physics, Assergi, L'Aquila, Italy
Roberto.Tartaglia@lngs.infn.it

Abstract. *The paper outlines a methodological approach utilizing quantitative risk analyses and cost-benefits evaluations in order to select the most cost effective options for risk reduction in industrial plants including structural changes and preventive maintenance. The methodology includes quantification of top events resorting to fault trees, a sensitivity analysis of the probability of occurrence of top events and a comparison of corrective measures based on cost and effectiveness criteria. The method is applied to a case study represented by the pseudocumene purification plant of the Borexino experiment in order to show its capability. The experiment is located in the Gran Sasso National Laboratory operated by the Italian National Institute for Nuclear Physics.*

Keywords*. Plant safety, quantitative risk assessment, maintenance, fault tree, cost-benefit analysis.*

1. Introduction

The issues of risk assessment and hazard evaluation in facilities subjected to high risk accidents have reached a status of top priority and can not be disregarded on any ground, as witnessed by the intense and coordinated regulatory activity at either national or international level (e.g. the recent EU Directive 96/82 CE "Seveso II"). Plant managers, hence, are forced to increasingly onerous risk assessment and reduction activities, still relying on limited budgets and scarcity of resources. Therefore, the technical-economic optimization of prevention/protection interventions become a priority.

A number of process hazards and risk analysis methods are available to perform safety studies (Tixier et al. 2002), and a thorough description of such methods is available in textbooks (CCPS, 1992 and 2000; Kletz, 1999; Lees, 1996; TNO, 1999). Of course it should be noted that currently no universally agreed standard approach exists as far as the risk assessment procedure is concerned as this is the result of the integration of distinct tools and techniques as required by site specific issues, and always requires the decisional and judgemental contribution of the analyst or plant manager. Although a qualitative risk assessment and hazard evaluation may still be sufficient in several applications, a detailed quantitative risk assessment is required if any kind of economic justification or optimisation of risk reducing measures have to be pursued and when the physical consequences of accidents have to be evaluated.

However, it is well known that conventionally the risk is defined as the product of the probability of occurrence p of an accident and the magnitude M of its consequences. Therefore, when an in-depth safety assessment is required, usually a hazard identification analysis is at first performed resorting to qualitative techniques, aimed at identifying both possible accidents modes - typically materials or energy loss of containment events - and credible scenarios (utilizing techniques such as Hazard and Operability analysis - HAZOP, Failure Modes Effects and Criticality Analysis - FMECA, What-if analysis etc.). This is followed by a probabilistic risk assessment, which aims at both establishing accident causes and quantifying the probability of occurrence of accidents resorting to analytical techniques and reliability theory (e.g. fault trees). Finally, the possible accidents scenarios and consequences are estimated (e.g. resorting to event trees), while quantification of physical effects either on-site and off-site enables to assess the loss to personnel, population, facilities or environment.

When faced with a risk reduction task, technicians have to properly balance preventive and protective approaches. However, the role of maintenance should not be underestimated in pursuing a risk reduction strategy. In fact, while it is largely agreed that a correct management of maintenance is critical to preserve the operability and competitiveness of production systems (Duffuaa et al., 1999) it is also unquestionable that the reliability of plants, of their components and of the control and protection systems, which is largely determined by the effectiveness of the adopted inspection and maintenance practices, has a direct impact on the risk level of the entire system (Lees, 1996).

It follows that there is a very strict link and interdependence among the risk level and maintenance activities, since a correct maintenance policy may effectively contribute to risk reduction as much as other structural choices or other operational and managerial activities. In fact, for monitorable and maintainable systems, the availability and reliability of single components or of the entire plant, factors which directly affect the probability of occurrence of accidents and their magnitude or the capability of loss minimization, may be strongly influenced by the adopted maintenance policy. On the contrary, it often happens that proper preventive maintenance strategies, applied to monitorable and repairable components of the safety and trip systems in order to improve their reliability, together with their redesign from the functional and logic point of view, are economically advantageous respect the simple substitution of critical components with more reliable ones.

Under this perspective quantitative risk assessment techniques, reliability estimation methods, redesign of safety systems and structural changes to the equipment and, finally, maintenance become a strategic lever for safety management and risk reduction, especially when accidents with relevant consequences are involved. In this framework a methodological approach which utilizes quantitative risk assessment techniques, maintenance planning techniques, and cost-benefits analyses extended over the entire life-cycle of the facilities, is presented in order to identify the most effective strategies under the technical-economic point of view able to reduce risk in industrial plants.

2. Methodological approach

Logic trees (Greenberg et al., 1992) are among the most widely utilized tools to perform quantitative risk assessments. Fault trees enable in fact to estimate the probability of occurrence of a given top event on the basis of reliability data of equipment and of the probability of the base events which logically concur to determine it, the values of which are determined also by the kind of maintenance policy adopted. Moreover fault trees lend themselves to a wide range of sensitivity analyses. As an example the following indexes are widely utilized to characterize the relevance of a given event A within a fault tree:

Birnbaum Index (A) = $(P_{TE} | P_A = 1) - (P_{TE} | P_A = 0)$
Criticality index (A) = $[(P_{TE} | P_A = 1) - (P_{TE} | P_A = 0)]\ P_A / P_{TE}$
Fussel Vesely Index (A) = $\Sigma_i\ MCS_i / P_{TE}$

where P_{TE} is the probability of the top event, P_A is the probability of a given base event A and $MCS(A)_i$ is the probability of the i-th Minimal Cut Set containing base event A. Therefore, while fault trees represent a powerful analytical technique they also enable to gain insights in the logic of the examined system and may be utilized to identify the most effective system modifications. Such parameters in fact define the contribution of single base events or minimal cut set to the occurrence of top events as well as their frequency variation according to changes in the probability of occurrence of the base events.

From the previous discussion it follows that the reliability of a complex system may be increased either adopting structural measures, i.e. by increasing the inherent reliability of the single components and/or changing their interaction logic or, according to a management approach, acting on the maintenance activities, thus exploiting their potential in improving and maintaining the reliability and availability of a system. In the first case the traditional system reliability optimisation techniques (Tillman et al., 1980) have been enhanced by techniques based on fault trees (Andrews, 1994) and genetic algorithms (Pointon et al., 1995; Pattison et al., 1999), which result still scarcely applied in practice. In the second case, since repairable systems are often involved (Ascher et al., 1984), it is effective to implement proper periodic inspection policies (Ben-Daya et al., 1998; Banerjee et al., 1996) and preventive maintenance practices (Barlow et al., 1960; Canfield, 1986; Gertsbakh, 1977; Kobbacy et al., 1995; Makis et al., 1992; Nakagawa, 1977, 1980, 1986; Nguyen et al., 1981; Percy et al., 2000). Under this point of view, the components and the logic of safety systems, especially the measurement, control and alarm equipments, the criticality of which has been recognized from a long time (CCPS, 1993) are particularly sensitive to the design of working logics and to maintenance activities, with ample margins of improvements in real systems. For such subsystems empirical or analytical analysis techniques (Goble, 1998; ISA, 1996) have been recently developed in order to comply with the minimum system integrity level requirements dictated by the most up to date technical standards (American National Standards Institute – ANSI / Instrumentation, Systems and Automation Society - ISA). The technical literature, therefore, clearly states how the risk level in complex systems is strongly influenced by the reliability of the system and by the maintenance activities which this reliability level try to preserve or increase. It can also be observed that several authors propose approaches to the analysis and optimisation of maintenance management which are of great interest and suited to practical implementation (Abdel-Hameed, 1995; Ben-Daya et al., 2000; Dekker, 1995; Murthy et al., 1998; Ozekici, 1996; Scarf, 1997; Pintelon et al., 1992). However, in practice such techniques show a poor degree of application. In many cases, finally, results that maintenance activities are not integrated at all with safety management in spite of the opportunity for interaction and synergy.

In order to contribute to a solution of this problem and to develop a pragmatic approach a systematic methodology to optimised risk reduction in industrial plants based on quantitative reliability-based techniques and cost-effectiveness analysis is proposed here.

The methodology is articulated in the following steps:

- Evaluation of the system's reliability performances in terms of probability of occurrence of accidents, and availability. Typically this kind of analysis shall be carried out resorting to fault trees.

- Ranking of base events criticality relying on specific indices. In particular when the fault tree technique is adopted this may be carried out resorting to the Birnbaum, the Criticality, and the Fussel-Vesely indices. This is aimed at performing a sensitivity analysis by pinpointing components or events which mainly affect the top event in order to identify existing alternatives and effectively deploy corrective measures.
- Identification of a set of applicable corrective measures able to improve the reliability performances of the system. Corrective policies typically include:
  I. Substitution of critical components with more reliable ones.
  II. Structural modifications to the system or changes to the safety systems logic.
  III. Proper maintenance policies.

  Policies may be applied either singularly or in a combined manner.
- Planning the execution of the above defined intervention strategies and evaluation of associated costs.
- Assessment of the global effects of the considered strategies in terms of system's reliability performances.
- Economic analysis of the considered policies and cost-benefits ranking to assess their effectiveness based on proper technoeconomic performance indices.

In the following the approach will be demonstrated resorting to a case study example.

3. Application example: the Borexino experiment purification plant

The proposed method is applied to the Borexino experiment plant housed in the Gran Sasso nuclear physics laboratory in Italy. The entire experiment is installed in a 100 x 20 x 20 m underground hall under the Gran Sasso mountain. The experiment is aimed at studying solar neutrinos resorting to pseudocumene (PC), a toxic and flammable aromatic hydrocarbon (flammability temperature 44 °C, flammability limits 0.9 - 6.4 % vol, and self ignition temperature of 511 °C) acting as a detecting medium, contained in a semispherical process vessel having a diameter of 18 m. Apart from the process vessel the plant includes a separate storage area and a PC purification plant. The latter is made up of three distinct sections, namely a PC distillation unit, a water extraction section and a nitrogen stripping unit. When the Borexino experiment will be fully operational about 1400 t of PC will be stored and utilized. Storage and utilization of PC make Borexino subjected to the Seveso II directive owing to its toxicity (PC is classified as R51/53, i.e. toxic to aquatic organisms and harmful to aquatic environment in the long term). Further details on the Borexino experiment are available elsewhere (Caputo et al., 2002a). This study follows a previous risk assessment based on qualitative techniques (HAZOP and FMECA) and focuses on the purification plant only.

The three sections of the purification plant (Figure 1) are contained in two adjoining 3x3x11 m skids located nearby the main process vessel. PC optical transparency and radioactive purity are critical for the experiment success, therefore removal of ions, oxides and salts of metal radionuclides, as well as gaseous radionuclides coming from radon and krypton leaks into the circuit and other chemical impurities such as dissolved oxygen and metal ions, oxides and salts should be periodically removed. Vacuum distillation is utilized for removal of non volatile impurities such as metal ions and salts. Water extraction is effective in removing soluble compounds such as oxygen, oxides and metal radionuclides salts. Water traces and remaining gaseous pollutants are removed via countercurrent nitrogen stripping. A final mechanical filtration is applied to remove particles greater than 0.5 μm. The PC saturated nitrogen stream is then cleaned in an activated carbon bed adsorption plant (Caputo et al., 2002b), while emergency relief streams, mainly collected from rupture disks fitted to the equipments, are handled in a separate blow down vessel consisting in a 10 m^3 quench pool able to process a flow rate of about 19500 kg/h for a duration of up to 10 minutes. Heat input for the purification process is supplied by a hot diathermic oil circuit.

The purification plant may operate in five different modes: distillation, water extraction, nitrogen stripping, distillation and stripping, water extraction and stripping (see Figure 2).

A brief description of the plant operation is given as follows. PC is fed to the purification plant from the feeding tank V-103 at ambient conditions via pump P-101. The nominal flow rate is 1 m^3/h. Flow switching among the process units is accomplished by manually operated valves. The distillation unit C-100 performs a multistage vacuum distillation at a pressure of 0.1 bar maintained by vacuum pump VP-101. At this temperature the PC boiling temperature is about 100 °C. Apart from fresh PC inlet the column is fitted with a further inlet for recirculation of distilled PC. Liquid PC in the column bottom is maintained in boiling conditions by recirculation in the external diathermic oil heat exchanger E-101. Vapor PC extracted from top of the column is condensed in the water cooled exchanger E-104 and conveyed at 30 °C to the receiver V-101 which feeds pump P-102 for final discharge. Contaminated PC is collected in tank V-102 and removed by pump P-103. Rupture disks rated at 3.5 bar_g are installed on V-102 and on the PC vapor discharge line. Countercurrent water extraction at atmospheric pressure conditions is carried out in vessel C-200 where PC is fed from the bottom and recovered from the top of the column in tank V-101 from where it is discharged through pump P-102. Process water before being recirculated is purified by distillation in the evaporating tank V-201 through hot oil exchanger E-201, while water is then condensed in the water cooled exchanger E-202 and collected in the condensate receiver V-202 to feed, by gravity, the extraction column.

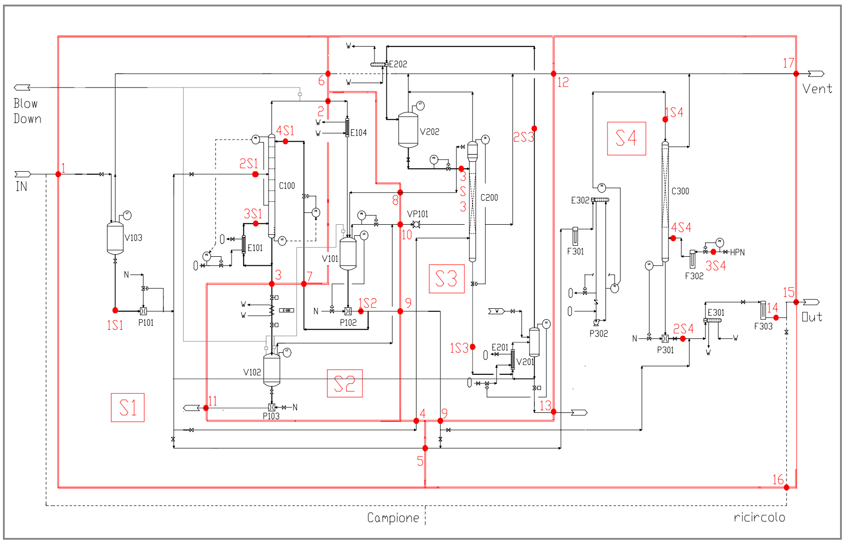

Figure 1. Scheme of the PC purification plant: S1 = Distillation section; S2 = Recirculation section; S3 = Water extraction section; S4 = Nitrogen stripping section.

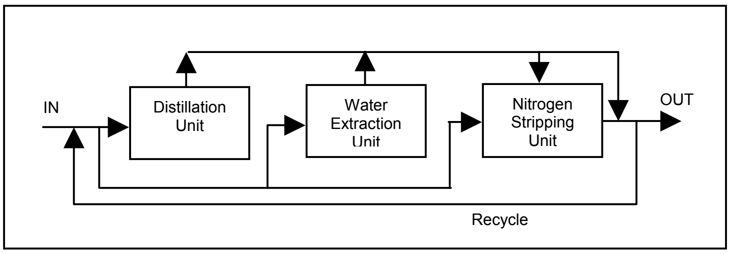

Figure 2. Scheme of possibile operation of the purification plant.

Nitrogen stripping is carried out in column C-300 at atmospheric pressure. PC is fed by pump P-101 or pump P-102 depending whether the stripping is carried out following distillation or water extraction steps. PC, after being filtered in F-301 and being heated to 30 °C in the hot oil exchanger E-302 enters into column top and descends in countercurrent with a nitrogen stream to be recovered at column bottom. Nitrogen vapors saturated by PC and containing dissolved impurities are conveyed through a vent line to the adsorption plant. PC is instead discharged by pump P-301. Before exiting the purification plant PC is further cooled to ambient temperature in the exchanger E-301. A recirculation loop is also available through tank V-103.

Main measurement instruments and alarms installed, all integrated by a digital control system in charge of controlling and regulating process parameters, are resumed in Table 1. Emergency shutdown is triggered by manual panic buttons, by fire sensors, or by high temperature in C-100 and high pressure in V-101.

Table 1. Existing sensors and alarms.

	Pressure		Temperature		Level		Flow rate		Notes
Unit	High	Low	High	Low	High	Low	High	Low	
C 100	●	●	●	●	●	●			Temperature sensed at top, bottom, interior and exterior.
C 200					●	●			Water-PC interface level
C 300			●		●		●	●	Nitrogen flow and level
V 101	●				●	●	●		
V 102					●				
V 103					●	●			
V 201					●	●			Water level
V 202					●	●	●		Water level and flow
E 104			●						
E 202			●						
E 302			●						
E 301			●	●					

As far as the PC purification plant is concerned (Figure 1), following a preliminary HAZOP analysis, a quantitative study has been attempted utilizing the presented methodological approach adopting probabilistic risk analyses and cost-benefits evaluations in order to select the most cost effective options for risk reduction. The methodology includes quantification of identified top events resorting to fault trees, a sensitivity analysis of the probability of occurrence of top events and a comparison of corrective measures based on cost and effectiveness criteria.

Based on the preliminary HAZOP study and findings of the Major Hazard Incidents Data Service data base (MHIDAS, 2002), eight different types of top events have been identified and considered, mainly related to loss of containment events (release of liquid or vapour PC in the laboratory environment or in the gas venting pipes, overpressure in the containment vessels, loss of gaseous nitrogen, release of diathermic heating fluid from the distillation unit, and fire). Assuming that most of such top events may occur in any of the four different plant sections, all of the corresponding fault trees have been developed and quantified resorting to commercial software tools (Relex, 2002). In greater detail the analysed cases are shown in the experimental matrix of Table 2.

Table 2. Fault tree experimental matrix

Section	TOP 1 Hot liquid PC indoor release	TOP 2 Cold liquid PC indoor release of	TOP 3 Overpressure in process equipment	TOP 4 Hot PC vapors in vent line	TOP 5 Liquid PC in vent line	TOP 6 Nitrogen indoor discharge	TOP 7 Indoor release of hot diathermic oil	TOP 8 Fire in purification plant
S1	●	●		●	●	●	●	●
S2	●	●		●	●	●		●
S3		●	●	●	●		●	●
S4		●	●	●	●	●	●	●

Indoor release of hot PC vapors produced in the distillation section has not been considered. As the process is carried out in near vacuum conditions, leaks in the equipment may cause inflow of ambient air. This pressure rise if not controlled should trigger the interruption of hot oil flow to the reboiler E-101 and the automatic plant shut-down. However, in case of malfunction of the control system a mixture of PC vapors and air may form into the vessel and a leak of vapors to the indoor environment might occur. Nevertheless, this is not considered to be a likely event because at ambient pressure PC vapors would immediately condense (distillation is carried out at 100 °C, while the PC boiling temperature at ambient pressure is 170 °C). Therefore the leak of PC vapors outside the distillation column would not result in a release of a cloud of hot PC vapors in the indoor environment and no fault tree has been built for this kind of event. The considered top events are briefly described in the following and the main analysis results will be pointed out. However, space limitations prevent to present and discuss the fault trees owing to their large size. A complete discussion of fault trees is available elsewhere (Tobia, 2002).

3.1. TOP 1: Indoor release of hot liquid PC (T = 100 °C)

Hot liquid PC is present in the exchanger E-101 and the bottom of the distillation column C-100 in plant section S1. Leaks may occur through flanges, joints and gaskets of the circuit or the column while a major discharge may occur following the catastrophic failure of the column caused by excess internal pressure (the column operates at 0.1 bar but is rated at 3.5 bar). As the system operates in nearly vacuum the PC outflow from column leaks is likely only in presence of a contemporary failure of the depressurization system. Column overpressure may be caused by excess liquid or vapor PC inflow, owing to flow control failure, and the failure to open of the column rupture disks. In all cases the top event requires also the failure of the pressure sensors and the automatic shut-down procedure. The major contributors to the top event resulted the leaks from circuit (probability of occurrence $p = 1.7\ 10^{-2}\ y^{-1}$) since the leaks or discharge from the failure of the column resulted much less likely ($p = 3.9\ 10^{-5}\ y^{-1}$). Furthermore the higher criticality was shown by base events represented by failure of gasketed joint according to the analysis performed.

3.2. TOP 2: Indoor release of cold (T = 15 ÷ 30 °C) liquid PC

Release may occur in all plant sections in correspondence to piping flanges and welded joints. Catastrophic failure of equipment is highly unlikely as all vessels are equipped with rupture disks opening at 0.49 bar_g. Excess liquid levels in vessels may occur in case of failure of the level monitoring devices and the emergency shut-down procedure. Nearly all sections contribute in roughly the same manner to the likelihood of the top events with the most critical base events represented by leaks of flanged joints of the control valves.

3.3. TOP 3: Overpressure in equipments

This top event has been considered separately only for section S4, as the overpressure event had already been considered as an intermediate event in the TOP 1 pertaining to sections S1 and S2. Overpressure in the water extraction section S3 is unlikely as it is directly connected to the vent line and the blow down system. In the stripping section S4 the overpressure may be caused by failure of the mass flows controls or by flow obstructions (failure close of valves, filter clogging, etc.) together with failure of the pressure sensing devices and the emergency shut-down system. In particular the pressure of the nitrogen supply line (4 bar) may be reached and even if this may not cause direct damage to the stripping column and related piping (rated at 8 and 16 bar respectively) the overpressure may be transmitted upstream to the recirculation section and the distillation column according to the specific operating mode and the status of the valves sectioning the different plant units. The failure of the shut-down resulted far more critical that that of the piping line. Therefore modification of the control system logic seems required. In particular failure of the nitrogen flow controller resulted having a criticality of 1 meaning that a given percentage variation of the probability of occurrence of this failure immediately reflects in the same percentage variation of the probability of the top event. The same occurs for the blockage of the check valve installed on the connection to the vent line.

3.4. TOP 4: Hot PC vapors in the vent line

In the examined plant nitrogen is utilized for inertization of piping and vessels and for stripping, giving rise to mixtures with PC vapors. Such polluted streams are collected and conveyed through the vent line to the adsorption unit for PC removal. The adsorption system has been sized to operate with a polluted stream at ambient temperature, while the presence of hot PC vapors would interfere with the cleaning process and increase the PC equilibrium concentration in the stream thus giving rise to exit concentrations higher than the allowed limits. In this top event definition the emergency relief through the blow down unit of the high temperature and high flowrate exhaust stream caused by sudden pressurization of the equipments following a fire event is not included. The top event would be caused by a fire or a hot vapor release by any of the plant sections. However, the fire event has been developed in a separate fault tree. Hot PC vapors, may be generated by excessive preheating in exchanger E-302, without this deviation being sufficient to stop the stripping process, while in the water extraction section the event may occur if liquid PC reaches the water distillation section and column C-200 has been emptied in presence of failure of the emergency shut-down. In the PC distillation section venting of hot PC vapors may occur in case of ineffective condensation in E-104 (caused by excess PC vapor inflow or reduction in cooling water flow rate) and simultaneous failure of the sensors triggering the plant shut-down. The top event resulted much more likely in the water extraction section. In particular severe criticality has been shown by the failure of the water/PC interface level sensor and the water flow controller at the inlet of column C-200.

3.5. TOP 5: Leakage of liquid PC in the gas venting line

This top event implies flooding of the vent line and the carbon adsorption unit with liquid PC coming from sections S1, S2, S3. In particular PC buffer tank V-103 and columns C-200 and C-300 are directly connected to the vent line without the interposition of valves or rupture disks, in order to convey the PC vapors released during normal plant operations. Events may occur in case vessels are flooded and level controls fail, therefore the flow and level controllers are the critical items. An excess of nitrogen flow rate in C-300, owing to flow control equipment failure, would also cause re-entrainment of liquid drops in the vent line. The event is more likely in sections S3 (probability on a 10 years period p = 0.661) and S4 (p = 0.431).

3.6. TOP 6: Indoor nitrogen release

Nitrogen release may be dangerous to operators in case a local saturation of the atmosphere occurs thus decreasing the oxygen content. Furthermore irritant PC vapors may be dissolved in the leaking stream. Nitrogen leaks are more likely in sections S1, S2, S4, where nitrogen driven pumps are utilized and where several nitrogen flow control valves and filters are located as well as in the stripping column. Critical leaking points are flanges and joints.

3.7. TOP 7: Indoor release of hot diathermic oil

Release of hot oil may cause fires in case a concurrent PC leaks occurs in the same area. Leaks may happen from flanges and joints in sections S1, S3, S4 where hot oil exchangers E-101, E-201, E-302 are utilized.

3.8. TOP 8: Plant fire

Fire event results from the concurrent start of a fire and the failure of the fire fighting equipment. Fire initiation occurs when an effective source of ignition is in contact with PC above the flash point. Ignition of vapor PC has not been considered as it is not a likely event owing to the above description of plant operation. In fact vapor PC may only exist in the vacuum distillation column, but would readily condense in the indoor environment, or dissolved in the nitrogen stream, besides in the vent line.

After building the fault trees the probabilities of occurrence of the top events have been computed, obtaining the values shown in Table 3. The analysis has been carried out over a foreseen life of the experiment of 10 years, resulting in rather high probability of loss of containment (Table 3).

Table 3. Result of quantitative risk assessment (PC purification plant)

Top event	Probability of occurrence (t= 10 years)	# of expected events (year^{-1})	MTBF (years)
1. Release of hot liquid PC	0.017016	4.98 10^{-3}	200
2. Release of cold liquid PC	0.081634	2.41 10^{-2}	41
3. Overpressure in vessels	0.010769	3.15 10^{-3}	317
4. Hot PC vapors in vent line	0.480571	5.59 10^{-2}	18
5. Liquid PC in vent line	0.807225	1.41 10^{-1}	7
6. Nitrogen leaks	0.119013	3.63 10^{-2}	28
7. Release of hot diathermic oil	0.303520	8.76 10^{-3}	114
8. Plant fire	4.9 10^{-6}	Negligible	Not significant

A study has been then undertaken to explore the possible strategies to increase the safety of the examined plant. At first a fault tree sensitivity analysis has been performed in order to pinpoint the single basic events or components which, by varying their failure rate, have the higher influence on the variability of the probability of occurrence of the top event (Fussel-Vesely criterion). Results are shown in Table 4.

Table 4. Result of criticality analysis

Top event	Critical components	Fussel-Vesely index
1. Release of hot liquid PC	Flanges metal gaskets	0.9863
2. Release of cold liquid PC	Valves flanges	0.0836 ÷ 0.1252
3. Overpressure in vessels	Vent line check valve	1
	Nitrogen flow controller	1
	C-300 Level controller	0.7758
	PC filter	0.2932
	Human error	0.1825
4. Hot PC vapors in vent line	Liquid interface controller C-200	1
	Flow controller	1
	Sensors and transducers	0.4252
	High pressure alarm	0.2061
	High temperature alarm	0.2061
5. Liquid PC in vent line	Level controller C-300	0.5068
	Level controller V-101	0.5512
	Flow controller C-300	0.5512
	Liquid interface controller C-200	0.5512
6. Nitrogen leaks	Flanged joints	0.1143 ÷ 0.1990
	Nitrogen filter	0.2828

Afterwards, several possible improvement strategies have been devised for each top event according to the following typology:

I. changing the components showing the higher impact on the top events with similar components having a 10% lower failure rate, in order to reduce the probability of the top event;
II. acting on the system's logic by adding back up components or enhancing the trip systems by adding safety components such as new sensors;
III. adopting preventive maintenance programs to increase the reliability of the maintainable and monitorable components of the trip systems.

System's response in terms of reliability increase has been then evaluated considering such strategies enforced either separately and in combination.

Considered interventions, along with their reliability improvement potential are summarized in Table 5.

Following, the results have been ranked considering the reliability increase and the corresponding cost, in order to identify the most cost-effective strategy for each top event (Table 6). It resulted that strategy type I) is the worst performer, with a failure probability decrease of only 5 to 10%, while a proper combination of strategies types II) and III) may lead to reduction in the probability of occurrence of the top events of 42% to 99.9% with costs ranging from 4500 to 106000 €.

Finally the overall selection of the most cost effective improvement strategy has been done by relative ranking the best interventions for each top event. At this preliminary stage of the research a global technical economic index having an intuitive meaning has been chosen. However, it should be noted that the ranking index may be an arbitrary objective function were the various parameters may be properly weighed and expressed on a normalized basis according to specific user's needs.

Table 5. Performances of improvement strategies

STRATEGY	DESCRIPTION	NEW TOP EVENT PROBABILITY (t=10 years)	% probability reduction
TOP 1			
S I	Gasket substitution	0.0153	9.9
S III	Periodic inspection and preventive maintenance	0.0013	92.3
S III.1	Continuous monitoring and breakdown maintenance (requires installation of sensors on potential leak sources)	0.000096	99.4
TOP 2			
S I	Gasket substitution	0.0791	3
S III	Periodic inspection and preventive maintenance on all potential leakage components	0.01257	84.6
S III.1	Continuous monitoring and breakdown maintenance (requires installation of sensors on potential leak sources)	0.05766	29.4
TOP 3			
S I	Components substitution	0.00878	18.4
S II	New pressure sensor in C-300 triggering emergency shut-down	0.00039	96.3
S II.1	New line to vent duct bypassing check valve (two check valves in parallel	0.00036	96
S II + II.1	Combination of strategies	0.000013	99.9
S III	Inspection and preventive maintenance	0.0087	18.4
S I + S III	Combination of strategies	0.000290	97.3
TOP 4			
S I	Components substitution	0.45761	4.8
S II	New PC vapor flow sensor and alarm at C-100 outlet triggering automatic shut-down	0.45552	5.2
S II.1	New PC sensor in C-200 water drain line	0.15546	67.6
S II + S II.1	Combination of strategies	0.11474	76.1
S III	Inspection and preventive maintenance	0.12287	74.4
S I + S III	Combination of strategies	0.11989	75.0
TOP 5			
S I	Component substitution	0.77350	4.2
S II	New PC sensors along connections of V-103, C-200 and C-300 to vent line	0.46709	42.1
S I + S II	Combination of strategies	0.44390	45
S III	Inspection and preventive maintenance	0.22132	72.6
TOP 6			
S I	Components substitution	0.11326	4.8
S II	New oxygen sensor close to possible location of N_2 leaks	0.02245	81.0
S III	Inspection and preventive maintenance on joints	0.04662	60.8
S II + S III	Combination of strategies	0.00692	94.2

Table 6. Comparison of improvement strategies (PC purification plant, 10 years period)

Top event	Probability of occurrence - Before (t= 10 years)	Probability of occurrence - After (t= 10 years)	% unreliability variation	Best strategy	Cost (Euro, present value)
Release of hot liquid PC	0.017016	0.001314	-92.3	SIII, PM on main flanges	106500
Release of cold liquid PC	0.081634	0.012572	-84.6	SIII, PM on all flanges	106500
Overpressure in vessels	0.010769	0.000013	-99.9	SII, addition of bypass line and new pressure sensor in vessel	4500
Hot PC vapors in vent line	0.480571	0.114744	-42.1	SII, new flow meters and PC sensors in trip system	> 8000
Liquid PC in vent line	0.807225	0.467093	-42.1	S II, New PC level sensors in vent line	4800
Nitrogen leaks	0.119013	0.006921	-94.2	SII+SIII, new low oxygen sensors + PM on flanges	N.A.

PM = Preventive maintenance; SII = Type II) strategy; SIII = Type III) strategy, N.A. = Not Available.

In this case the index value for a generic *i-th* strategy has been assumed to be directly proportional to the probability reduction and to the relative top event probability with reference to the most probable top event, and indirectly proportional to the relative cost of each improvement strategy respect the one with the greatest cost.

$$RI_i = \frac{\Delta p_i \dfrac{p_i}{p_{max}}}{\sqrt{\dfrac{C_i}{C_{max}}}}$$

where Δp_i is the percent reduction in the probability of occurrence of the *i-th* top event after the strategy has been adopted, p_i is the initial top event probability, p_{max} is the probability of the most probable top event, C_i is the cost of the adopted strategy and C_{max} is the cost of the most costly strategy.

In the present case study the ranking index RI values are shown in Table 7, indicating that it is most cost effective to act on top #5 (presence of liquid PC in the vent line) by adopting the S II type of strategy which enables a fairly high probability reduction on a kind of event having the highest probability of occurrence at a reasonable cost.

Table 7. Ranking results

TOP EVENT	RI
1	0.019
2	0.086
3	0.043
5	2.256

Based on such information the management could easily make the best decision, based on improving the reliability of the trip systems (even by modifying their logic) and applying a preventive maintenance policy where feasible, rather than trying to improve the reliability of the process plant equipments subject to failure.

Therefore the proposed methodological approach showed the effectiveness of systematically adopting quantitative risk analyses with managerial decision based on cost-benefits analysis in order to provide the best guidelines when choosing the most cost effective strategies in safety enhancement programs for high risk industrial plants. The suggested approach will be further refined in future works. In particular the method may be associated with techniques aimed at determining an exhaustive list of candidate improvement strategies in order to rely less on subjective judgements, while features enabling the optimisation of each single strategy from an economic point of view shall be included. As an example the optimization of the preventive maintenance planning and the inclusion of spare parts inventory management criteria would be a useful addition. Finally, alternative expressions for the ranking index could be explored in order to properly determine the preferred one according to specific requirements, in particular by including some of the proven multicriteria decision techniques available.

4. Conclusions

In this paper a methodological approach utilizing quantitative risk analysis and cost-benefits evaluations is presented aimed at selecting the most cost effective options for risk reduction in industrial plants. The methodology includes: quantification of top events resorting to fault trees, a sensitivity analysis of the probability of occurrence of top events to identify system’s criticalities, the identification of possible improvement strategies (including the increase of sensitive components reliability, the change of system’s operating logic especially pertaining to safety control and instrumentation equipment, and the adoption of proper preventive maintenance strategies), and a comparison of corrective measures based on cost and effectiveness criteria. The method has been successfully applied to the case study represented by the purification plant of the Borexino experiment showing its capabilities and enabling plant managers to define the preferable safety improvement strategies to be adopted. In future works the methodology will be further expanded to automatically define a list of applicable improvement strategies and to plan in an optimised manner the candidate interventions. Also a comparison of different ranking criteria or the adoption of more sophisticated multicriteria decision techniques will be carried out. Finally it is foreseen the integration of this risk assessment approach with computerized maintenance management systems.

5. References

Abdel-Hameed, M., 1995, “Inspection, Maintenance and Replacement Models”, Computers & Operations Research, 22-4, 435-441.

Andrews, J.D., 1994, “Optimal Safety Systems Design Using Fault Tree Analysis”, Proc. Instn. Mech. Engrs, J. of Process Mechanical Engineering, 208 Pt E, 123-131.

Ascher, H., Feingold, H., 1984, “Repairable Systems Reliability”, Dekker.

Banerjee, P.K., Chuiv, N.N., 1996, “Inspection Policies for Repairable Systems”, IIE Transactions, 28, 1003-1010.

Barlow, R.E., Hunter, L.C., 1960, “Optimum Preventive Maintenance Policies”, Operations Research, 8, 90-100.

Ben-Daya, M., Duffuaa, S.O., Raouf, A., 2000, “Maintenance Modeling Optimization”, Kluwer.

Ben-Daya,M., Hariga, M., 1998, “A Maintenance Inspection Model: Optimal and heuristic solutions”, Int. J. of Quality and Reliability Management, 15, 481-488.

Canfield, R.V., 1986, "Cost Optimization of Periodic Preventive Maintenance", IEEE Transactions on Reliability, R-35, 78-81.

Caputo, A.C., Pelagagge, P.M., Tartaglia, R., "Safety Management in Hazardous Experimental Environment: The Borexino Case", *Process Safety Progress*, vol. 21, n. 1, pp. 55-66, March 2002.

Caputo, A.C., Pelagagge, P.M., Tartaglia, R., "VOC Control in an Underground Experimental Facility: Technical and Safety Issues", *Proc. 95th Annual Conference of the Air & Waste Management Association*, Baltimore, USA, June 23-27, 2002.

CCPS-Center for Chemical Process Safety, 1992, "Guidelines for Hazard Evaluation Procedures", Center for Chemical Process Safety, American Institute of Chemical Engineers, New York.

CCPS-Center for Chemical Process Safety, 1993, "Guidelines for Safe Automation of Chemical Processes", AIChE, New York.

CCPS - Center for Chemical Process Safety, 2000, "Guidelines for Chemical Process Quantitative Risk Analysis", AIChE, New York.

Dekker, R., 1995, "On the Use of Operations Research Models for Maintenance Decisions Making", Microelectronics and Reliability, 35, 1321-1331.

Duffuaa, S.O.,Raouf, A., Campbell, J.D., 1999, "Planning and Control of Maintenance Systems: Modeling and Analysis", Wiley.

Gertsbakh, I.B., 1977, "Models of Preventive Maintenance", North Holland, Amsterdam.

Goble, W.M., 1998, "Control System Safety Evaluation and Reliability", ISA, Research Triangle Park, NC, USA.

Greenberg, H.R., Slater, B.B., 1992, "Fault Tree and Event Tree Analysis", Van Nostrand Reinhold, NY.

ISA-Instruments Society of America, 1996, "Application of Safety Instruments Systems for the Process Industries", ANSI/ISA-S84.01.1996, ISA, Research Triangle Park, NC, Usa.

Kletz, T.A., 1999, "Hazop and Hazan: Identifying and Assessing Process Industry Hazards", 4th ed., Hemisphere Pub.

Kobbacy, K.A.H., Percy, D.F., Fawzi, B.B., 1995, "Sensitivity Analyses for Preventive Maintenance Models", IMA J. Of Mathematics Applied in Business & Industry, 6, 53-66.

Lees, F.P., 1996, "Loss Prevention in Process Industries", Butterworth, London.

Makis, V., Jardine, A.K.S., 1992, "Computation of Optimal Policies in Replacement Models", IMA J. of Mathematics Applied in Business & Industry, 3, 169-175.

MHIDAS, 2002, Major Hazard Incident Data Service (MHIDAS), AEA Technology plc, Thomson House, Risley, Warrington, Cheshire, UK.

Murthy, D.N.P., Asgharizadeh, E., 1998, "Optimal Decision Making in Maintenance Service Operations", European J. of Operations Research, 116, 259-273.

Nakagawa, T., 1977, "Optimum Preventive Maintenance policies for Repairable Systems", IEEE Transactions on Reliability, R-26, 168-173.

Nakagawa, T., 1980, "Replacement Models with Inspection and Preventive Maintenance", Microelectronics and Reliability, 20, 427-433.

Nakagawa, T., 1986, "Periodic and Sequential Preventive Maintenance Policies", J. of Applied Probability, 23, 16-21.

Nguyen, D.G.,Murthy, D.N.P., 1981, "Optimal Preventive Maintenance Policies for Repairable Systems", Operations Research, 29, 6, 1181-1194.

Ozekici, S., (Ed.), 1996, "Reliability and Maintenance of Complex Systems", NATO ASI Series, Springer, Berlin.

Pattison, R.L., Andrews, J.D., 1999, "Genetic Algorithm in Optimal Safety Systems Design", Proc. Instn. Mech. Engrs, J. of Process Mechanical Engineering, 213 Pt E, 187-197.

Percy, D.F., Kobbacy, A.H., 2000, "Determining Economical Maintenance Intervals", Int. J. Production Economics, 67, 87-94.

Pintelon, L.M., Gelders, L.F., 1992, "Maintenance Management Decision Making", Eur. J. of Operations Research, 58, 301-317.

Pointon. L., Campbell,J., 1995, "Genetic Algorithms in Optimization of Systems Reliability", IEEE Trans. on Reliability, 44, 2, 172-178.

Relex, 2002, Relex 7 Reference Manual, Relex Software Corporation, Greensburg, PA, USA.

Scarf, P.A., 1997, "On the Application of Mathematical Models in Maintenance", European J. of Operations Research, 99, 493-506

Tillman,F.A., Hwang, C., Kuo, W., 1980, "Optimization of Systems Reliability", M. Dekker, New York.

Tixier, J., Dusserre, G., Salvi, O., Gaston, D., 2002, "Review of 62 Risk Analysis Methodologies of Industrial Plants", J. Loss prevention in the Process Industry, 15, 291-303.

TNO, 1999, "Guidelines for Quantitative Risk Assessment", Department of Industrial Safety, Purple Book (CPR 18E), Apeldoorn, Netherlands.

Tobia, M., 2002, Valutazione del Rischio Mediante Tecniche Quantitative: Il Caso degli Impianti di Stoccaggio e Trattamento dello Pseudocumene, Master Thesis in Mechanical Engineering, Faculty of Engineering, University of L'Aquila, Italy (in Italian).