Available online at www.sciencedirect.com
SCIENCE DIRECT®
Journal of Loss Prevention in the Process Industries 17 (2004) 467–475
Journal of Loss Prevention in the process industries
www.elsevier.com/locate/jlp

Comparison of techniques for accident scenario analysis in hazardous systems

Z.S. Nivolianitou [a,*], V.N. Leopoulos [b], M. Konstantinidou [c]

[a] *Systems Reliability and Industrial Safety Laboratory (SRISL), Institute of Nuclear Technology-Radiation Protection, National Center for Scientific Research "Demokritos", Aghia Paraskevi 15310, Greece*
[b] *School of Mechanical Engineering, National Technical University of Athens, Zografou campus, Zografou 157 80 Greece*
[c] *School of Chemical Engineering, National Technical University of Athens, Zografou campus, Zografou 157 80, Greece*

Abstract

In this paper, three accident scenario analysis techniques are presented and compared regarding their efficiency vs. the demanded resources. The complexity of modern industrial systems has prompted the development of accident analysis techniques that should thoroughly investigate accidents. The idea of criteria classification to fulfill this requirement has been proposed by other researchers and is examined here too. The comparison is done through the application of Event Tree analysis, Fault Tree analysis and Petri Nets technique—two relatively simple and a more demanding methodology—on the same hazardous chemical facility in view of analyzing an accident scenario of a hazardous transfer procedure. Accident scenario analysis techniques are essential not only in learning lessons from unfortunate events in the chemical industry but also in preventing the occurrence of such events in the future and in communicating risk more efficiently.

Keywords: Accident analysis; Human factor; PETRI nets

1. Introduction

The severe industrial accidents, which have happened in the last decades (chemical and nuclear sites, aviation, space expeditions), have raised the awareness of the public regarding the negative effects of technology. Risk associated with technology is a crucial element for triggering public protest, so it is of utmost importance to find the origins of risks, to strengthen safeguards and thus preserve the acceptability of hazardous facilities or activities.

The technical community, after many years of improvements in safety methods and system design, has realised that accident rates and system losses have reached a plateau beyond which further improvement seems impossible to achieve. Even in organisations with good general safety records, occasional large-scale disasters do occur and shake public confidence in modern technological systems.

The common factor in both of these areas is the human error, which, as mentioned by Cacciabue (2000), nowadays contributes to accident development with percentages higher than 80% for two main reasons: (a) the very high reliability of mechanical and electronic components and (b) and the new role of human operators in complex systems.

It constitutes a real need then, to provide a coherent strategy to maximise human performance and minimise human error. Accident analysis and forecasting techniques are doing so in complex system with hazardous operations, such as nuclear power stations and chemical production and storage plants but can be both onerous and time demanding.

These techniques were developed in the last few decades for investigating serious accidents in safety—critical systems and can be classified into three broad categories according to their primary focus on: critical events and mechanical failures; human actions and their mechanisms; ergonomic factors and organisational levels.

* Corresponding author. Tel.: 302106503744; fax: +302106533431.
E-mail address: zoe@ipta.demokritos.gr (Z.S. Nivolianitou).

0950-4230/$ - see front matter © 2004 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jlp.2004.08.001

The first category of investigation has received the greatest attention mainly from system engineers with techniques such as fault tree analysis and event tree analysis, which focus on the failures of the technical systems, automatic control systems, barrier mechanisms and mitigation systems and treat the human factor and its erroneous actions in a component—like way.

Some error classifications have resulted in the development of several accident analysis techniques, which focus on the contribution of human agents and conditions of work to the accident sequence starting from Swain and Guttman (1983), to Embrey, Kirwan, Rea, Humphreys and Rosa (1984) followed by Hollnagel (1998) and Kim and Jung (2003) in the recent years.

Event trees and Fault trees are the usual tools of system engineers in Risk Analyses. However, both of these techniques offer a static representation of the system, not quite suitable for the dynamic aspects of an accident sequence. Promising technique to this end, which can be used to represent the dynamic evolution of the system situation leading to an accident, are the Petri Nets. Petri Nets were first used to model complex systems and their operations, but recently many application of Petri Nets in the accident analysis showed their versatility to combine human actions, technical failures and interactions between them in order to construct the accident model. Scope of this paper is to use the aforementioned three Risk analysis/Accident analysis techniques on the same accident scenario of a hazardous transfer operation in an ammonia storage plant and then, based on a taxonomy already developed, to evaluate and compare the traditional event trees and fault trees and the dynamic Petri Nets approach.

In Section 2, a selection of the criteria adequate to make the comparison is presented, while in Section 3, a short overview of the three methodologies is given. Section 4 offers a short presentation of the process plant and the hazardous operation, while sections 57 present the findings of each methodology. In Section 8, a comparison of the three methodologies is attempted and Section 9 concludes this article.

2. Taxonomy criteria

Accident analysis techniques are evaluated according to the support they provide in the investigation of complex systems and complex scenarios. The events in progress usually have different chronological and temporal characteristics (timing and duration) affected by many agents, the modeling of which often becomes very complicated. The same applies for accident scenario analysis.

The criteria for the evaluation of the three methods examined here are a selection and not the whole set of the criteria taxonomy proposed by Kontogiannis, Leopoulos and Marmaras (2000), as our scope of analysis is more restricted to accident "prognosis" rather than thorough investigation of a real accident. They are used to examine the adequacy of the methods in the description and investigation of hazardous process accident scenarios sequences, and are the following:

E*vent sequence:* the technique should represent the sequence of events that led to the accident in a detailed level.
E*vent agents:* the graphical representation should facilitate the identification of the agents that participate in every event.
E*vent dependencies:* the technique should allow the visualization of the relationships between the events and examine their dependencies.
E*vent interactions:* interactions between human actions and mechanical failures should be visualized.
M*odeling time and duration:* the graph should model the chronological evolution of the events.
M*odeling assumptions:* the graphical representation should enable marking of assumptions.
M*odeling concurrencies and conflicts:* the graph should allow the representation of multiple events.
M*odeling error recovery:* capabilities for recording "missing" or "misleading events".
M*odeling the context of work:* involve additional events that affected the workload.

3. Description of the methods

Fault trees and event trees are useful for analyzing complex components and systems, especially in identifying system interrelationships such as shared support systems and in identifying common cause failure mechanisms in highly redundant systems (see also Papazoglou, Nivolianitou, Aneziris, & Christou, 1992). Petri nets incorporate more the notion of timing in each sequence. All of these three techniques are shortly presented below.

3.1. Event trees

The event trees provide a systematic method for investigating accident scenarios involving complex systems. An event tree indicates the events after initiation of the accident sequence. As the number of events increases, the picture fans out like the branches of a tree.

These visual representations are graphic models that order and depict events according to the mitigating requirements of each group of initiating events. Events or headings of an event tree can be a safety function

status, a system status, a basic event occurring or an operator action. Event trees can be used to analyse systems in which all components are continuously operating, or for systems in which some or all of the components are in standby mode. The starting point—initiating event—disrupts normal system operation and the event tree displays the sequences of events involving success and/or failure of the system components.

The event tree headings are normally arranged either in chronological or causal order. Chronological ordering means that events are considered in the same order they are expected to occur during the chronological development of the accident. Causal ordering means that events are rearranged on the tree so that the number of omitted branch points is maximized.

3.2. Fault trees

A fault tree provides a structured approach to determining the probability of failure of a complex system. This approach also illustrates the minimum set of events that can cause the failure of a system. In order to evaluate the industrial risk, it is necessary to have an estimation of the accidents probability. This estimation can be obtained from historical data of previous accidents, or more precisely, from the application of the Fault Tree Analysis. The analysis is restrained in a particular undesired event (accident or incident), defined as the *top event* and it is operated by means of a graphic modeling allowing the visualisation of the possible combinations of malfunction and wrong actions that can generate it.

The synthesis of the results is generally presented with a graphical model organised by the logic of the Boolean algebra and its symbols (AND-gates and OR-gates) (CCPs, 1992).

3.3. Petri Nets

Petri Nets are both a formal and graphical language, which is appropriate for modeling systems with concurrency. Petri Nets—developed in the early 1960s—are a general theory of discrete parallel systems with language taken from automata theory. The ability to construct models with these properties makes Petri Nets an attractive tool for modeling operator behavior (Leopoulos, 1984).

A Petri Net is composed of four parts: a set of *places,* P a set of *transitions,* T, an *input function* I and an *output function* O. The input and output functions relate transitions and places. The input function I is a mapping from transition t_j to a collection of places $I(t_j)$ known as the *input places* of the transition. The output function O maps a transition t_j to a collection of places $O(t_j)$ known as the *output places* of the transition. The structure of a Petri Net is defined by its places, transitions, input function and output function.

A Petri Net graph has two types of nodes. A *circle* represents a place and a *rectangular* represents a transition. As a graphical tool, a Petri Net is similar to a chart or flow diagram, but Petri Nets go beyond flow diagrams in that they incorporate tokens that are used to simulate dynamic and concurrent activities. A t*oken* is a primitive concept for Petri Nets and is defining its *marking.* Tokens can be assigned to, and can be thought to reside in the places of a Petri Net. The number and position of tokens may change during the *execution* of a Petri Net, while their flow around the net can be visualized and illustrate the flow of control and data within the same model. A Petri net executes by *firing* transitions. A transition fires by removing tokens from its input places and creating new tokens, which are distributed to its output places. When there are no enabled transitions, the execution halts and the analyst can state whether a sequence is safely or non-safely terminated, or what action(s) could have prevented an accident.

4. Description of the installation

The hazardous installation is an ammonia storage plant with the relevant loading/unloading facilities. The plant is part of a large industrial complex and it serves in feeding an adjacent fertilisers plant with ammonia. The same plant has been used as reference in the context of a European Benchmark Exercise (Amendola et al., 2002) from 1998 to 2002, from which all relevant technical data is obtained. For reasons of simplicity and due to the limited scope of the study, only the sections related to ammonia storage and loading/unloading are considered.

Both refrigerated storage and storage under pressure takes place in the plant. Ammonia is imported by ship, by truck tankers or from an ammonia feed pipeline. From the storage area, ammonia is sent to the fertilisers plant according to demand. A schematic plant operation is presented in Fig. 1.

The ammonia storage plant is therefore divided into the following sections:

(i) Cryogenic ammonia storage
(ii) Ammonia unloading/loading ship terminal
(iii) Ammonia feed pipeline and terminal
(iv) Storage of ammonia under pressure
(v) Loading/unloading station from truck tankers

For our study, we focused on the ammonia unloading/loading ship terminal (mainly on the unloading ammonia procedure from ship to tank), which is located at the river side and handles cryogenic ammonia at $-33\ ^{\circ}C$. Ships arrive from the sea and along the river

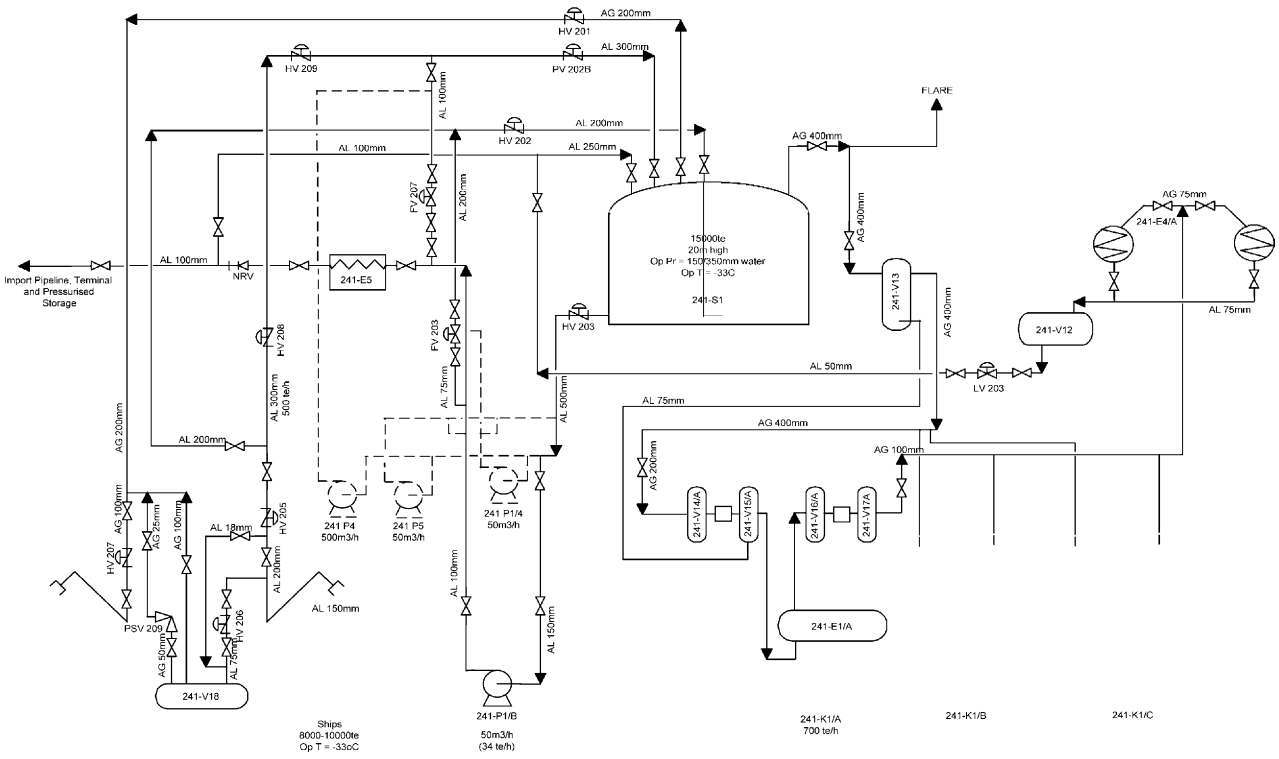

Fig. 1. Ammonia import (ship) and refrigerated storage.

at the terminal and unload ammonia to the cryogenic tank at a rate of about 700 m^3/h. The staff of the cryogenic storage supervises the unloading procedure and any gaseous ammonia can be diverted to a flare located near the cryogenic tank.

A typical ship for refrigerated ammonia transporting has a capacity of 8000–10000 tones, equipped witeight 8 internal tanks (usually double-hull vessels) and the appropriate refrigeration system.

The surroundings of the plant include a densely populated urban area, a small village, an industrial and commercial area (occupied mainly during the day), a stadium (occupied only a few hours per week) and a touristic resort, very crowded during the summer.

4.1. Ship loading/unloading terminal

The specific characteristics of the sea terminal unloading arm are Unloading capacity: 500 t/h (730 m^3/h); Operating pressure: 4 bar; Operating temperature: $-33\ ^{\circ}C$; Design pressure: 19 bar; and Design temperature: $-45\ ^{\circ}C$.

The *loading/unloading arm* located at the sea terminal is connected with the storage tank S1 through three lines which transfer liquid ammonia from the ship to the tank (and vice versa) and they are also used to cool down the line.

Pipeline length between the ship and the cryogenic storage is 900 m and it is divided into three approximately equal parts by four valves, namely valve HV-205, valve HV-208, valve HV-209 and valve PV-202B (close to the cryogenic tank). All these valves can be remotely operated from the control room, while valve PV-202B is connected to a pressure indicator and controller (PIC) closing it, when pressure rise in tank S1 occurs. The same controller sends a signal to close also valve HV-205 for the same reason.

Checks and ending of unloading operations: There are specific checklists that have to be double-signed (checked and signed by two different personnel members) before the unloading operation starts but also during it. About 30 min before the end of operations (according to estimated time and the general indications) both on-board and ground personnel perform the final checks of all parameters and prepare to stop the operation.

Gas detectors: In the loading/unloading area, there are a number of gas detectors (approximately 11), which are positioned in a radius of about 30 m from the dock. There are also three monitors, mainly for the protection of the plant from a fire on the ship.

Interruption of unloading in case of emergency: Loading of ammonia from the ship to the cryogenic tank can stop automatically when there is a pressure drop in the pipeline from loading arm to the tank, or a high level of ammonia in the tank. Valves HV-205 and PV-202B close automatically. However, no intervention from the plant personnel to the ship's equipment is possible, only oral communication among operators.

4.2. Ammonia unloading procedure to Storage Tank

Before starting ammonia unloading, the line connected to the ship is cooled down at operating temperature by pumping from tank S1 and circulating ammonia at $-33\ ^{\circ}C$ through the piping and then the loading arm is connected to initiate unloading from the ship.

When loading phase is finished, valves HV-205 and 207 must be closed while the loading arm is put in place by oil-operated valves. The loading arm is later disconnected from the ship, in such a way that the line remains full of liquid ammonia at $-30\ ^{\circ}C$ temperature and at 1.7 kg/cm^2 pressure.

Two of the three compressors available are then stopped and the working compressor manages all boil-off coming from both the storage tank (350 kg/h) and the lines (100–150 kg/h), while condensed ammonia is recycled into the cryogenic tank S1.

4.3. Description of the accident scenario

The accident scenario that was selected for our study is a representative example of a hazardous chemical process, which combines human actions and technical equipment. The unloading from a ship to a tank process is a rather common and frequent one and is taking place in many chemical and process facilities. The accident of a pipe breaking owing to an abrupt pressure built upstream a closed control valve (commonly known as ''water hammer'') is often registered in the process industry giving rise sometimes to ''major'' accidents, like the ''major'' accident of the November 6th, 1991 in Germany, where 1.2 t of ammonia were released from the cooling circuit of an organic chemical industry, as described in the MARS database (http://mahbsrv.jrc.it/mars/default.html).

During the unloading of ammonia from the ship to the tank, the operation of all three compressors is required to maintain ammonia temperature at its operating value and keep the pressure within safety limits. The deviation of the refrigeration safety system from the required operation initiates a transient and requires safety functions to avoid release of ammonia. As soon as pressure increase is registered in the tank, the PIC is activated to close partially valve PV-202B and reduce the flowrate from the ship. At this point, the ship personnel must be notified for the change from the terminal operators in order to reduce the flowrate from the ship to the tank. If no contact is established between the two parts, or if the communication is lost, the safety system will lead to closure of valve HV205 as a result of the pressure drop in the liquid ammonia unloading line. If the loss of contact between ship personnel and terminal operators still persists, the unloading process will continue from the ship leading to a pipe break owing to ''water hammering'' of the pipeline just before valve HV205 of the loading arm and to the releasing of liquid ammonia in the environment.

The same safety system can be activated also in the following cases:

1. Increased flowrate from ship (Flowrate over 500 t/h)
2. Increased ammonia temperature during unloading (Temperature above—$33\ ^{\circ}C$)
3. High level of ammonia in the tank S1

In the first two cases of increased flowrate or increased temperature, the compressors refrigerating capacity is not enough to keep pressure in the tank within the safety limits and pressure in the tank increases.

In the third case, it is not the pressure controller that is activated, but a level alarm and controller (LCAH) which acts on valve PV-202B initiating the above described sequence.

In all cases the release of liquid ammonia will be prevented if the contact between the ship personnel and the terminal operators is uninterrupted.

5. Event tree analysis

The accident sequences depicted with the Event Tree Analysis are as follows.

5.1. Reduction of the refrigeration capacity during the unloading from ship to tank process

Event tree ET-1, shown in Fig. 2, models the possible response of the storage facility to a reduction of the refrigeration capacity during the unloading of liquid ammonia from the ship to the tank and comprises the following events (headings).

5.1.1. Reduction of the refrigeration capacity (Event R)

Any deviation of the refrigeration safety system from the required operation (all three compressors working) initiates a transient and requires certain safety functions to avoid release of ammonia.

5.1.2. Manual Termination of loading and Communication among operators (Event M)

Following the failure of one or more compressors, the operators at the plant realizing the reduction of the refrigeration capacity, should communicate this fact to the ship operators and should terminate the unloading operation.

5.1.3. Pressure Control System (Event Pl)

This event corresponds to the successful sensing of the pressure rise and the closing of the appropriate valves (PV-202B and HV-205) by the pressure control system.

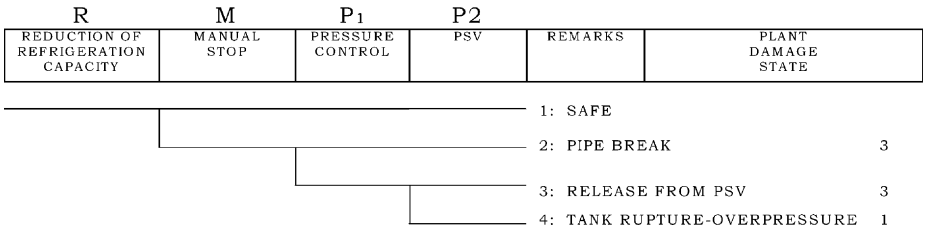

Fig. 2. System Event Tree of the Ammonia Storage Tank S1, during Unloading from ship to tank (Refrigeration capacity reduced).

5.1.4. Pressure Safety Valves (Event P2)

This event models the successful operation of the pressure safety valves mounted on the tank S1 in the event of a continuing pressure rise beyond and above the nominal safety valves set points.

The event tree determines four accident sequences. One of them (#l) constitutes successful termination of the incident. One (#3) results in release of ammonia from the PSVs of the tank S1. One (#2) results in the pipe break and release of substantial amounts of ammonia into the atmosphere. Finally, one sequence #4 leads to tank rupture and release of substantial quantities of ammonia.

Similar Event Trees are constructed for the initiating events ''Increase of flowrate during the unloading from ship process'', ''Temperature rise of liquid ammonia during the unloading from ship process'', ''Level rise beyond safety height during the unloading from ship process'', which all contain a sequence that leads to the pipe break due to the abrupt closing of the ammonia inlet valve (water hammer).

6. Fault tree for the ammonia release

The fault tree for the event pipe break, which leads to an ammonia release, is presented in Fig. 3.

The top event ''liquid ammonia release'' is due to a pipe break just before the valve HV-205 owing to ''water hammering''. The top event is the result of the HV-205 closure and the no manual stop of ship unloading, which can happen either because of the communication failure between the ship and the terminal operators, or because of ship pump failure to stop. The HV-205 closure is a following event of the pressure increase in the tank, or the level increase in the tank, or even a spurious signal from the pressure controller. The level increase is an intermediate event, which can be caused either by a spurious signal from the level indicator, or by a measurement error from the operators. The pressure increase is a subsequent event of temperature increase, which may result from the same reasons, mentioned in paragraph 4.3 plus an external thermal impact.

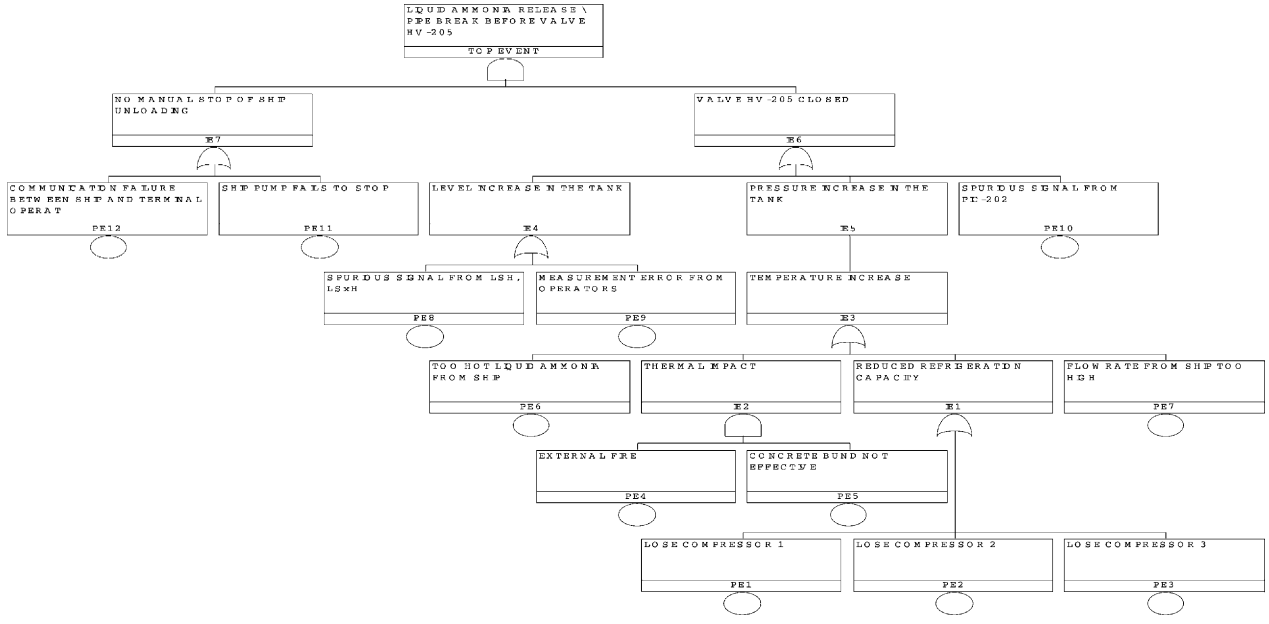

Fig. 3. Fault Tree for the ammonia release.

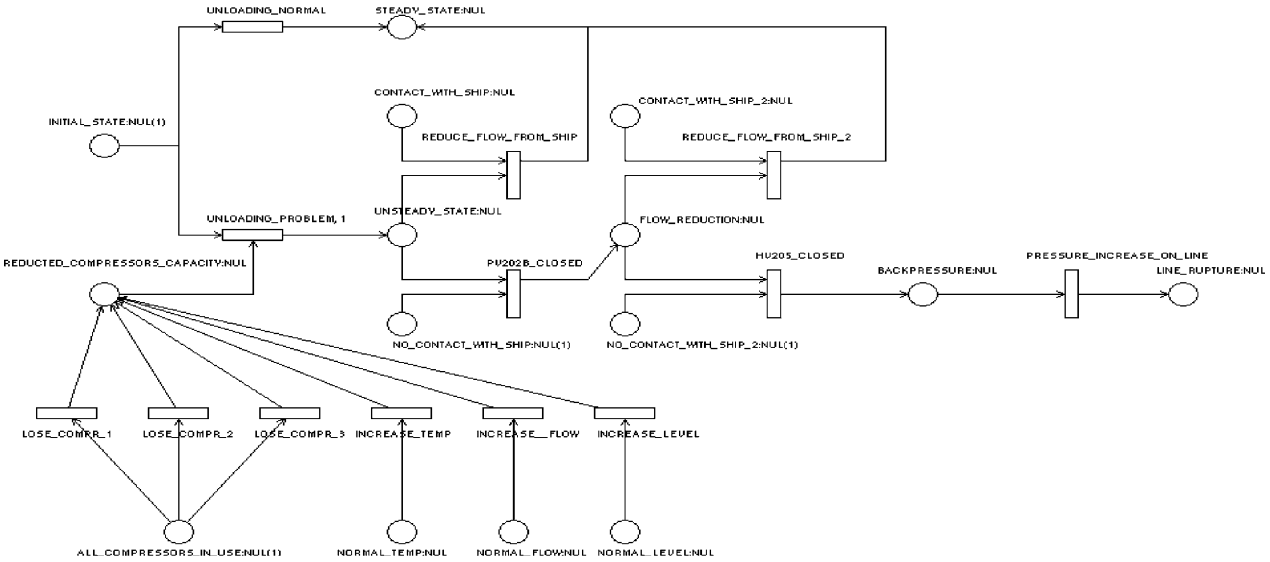

Fig. 4. Petri Net for the ammonia release.

7. Petri Nets

The development of the Petri Net graph was based on the ARTIFEX software package (Artifex, 1997).

The first stage in the development of a Petri Net graph concerns the identification of the physical system, the human agents and the messages communicated (oral and displayed messages) in the course of the events leading to the accident. The key concept is that the physical system, during its operation, sends messages to human operators, through the monitoring and alarm system. These messages initiate human actions, some of which may change the state of the physical system and others not. The Petri Net graph for the ammonia release is presented in Fig. 4, while Table 1, listing Places and Transitions of the Petri Net graph, describes the modeling of the system.

The physical system consists of the tank; the ship; the three compressors; the pressure control system; valve PV-202B and valve HV-205. The messages coming from the monitoring and alarm system are: Pressure increase in the storage tank S1; Level increase in the storage tank S1; Flow increase in the loading arm; Temperature increase of the liquid ammonia and Refrigeration capacity reduced.

The human actions concerned in the accident scenario are the necessary actions in order to keep the contact between the ship and the terminal operators.

It is important to examine the initial state of the system by putting the tokens in the appropriate places. In the initial state, the compressors are all working and the system is in steady state. We assume that no contact is established between the ship and the terminal operators, but this situation is yet unknown. As long as all compressors are working, the unloading procedure is going on normally.

Transitions T2-T7 that lead to ''Reduced compressor capacity'', are enabled but not activated yet. This happens when any of the transitions T2–T7 fires. As soon as that happens, another event sequence initiates which can lead to the accidental ammonia release. Compressor capacity reduced is an output place for six different transitions, namely ''loss of each one compressor'', ''flow increase'', ''temperature increase'' and ''level rise''. If any of these transitions fires, the token from its input place will be moved to the place ''reduced compressor capacity''. As soon as compressor capacity is reduced, the system is entering in unsteady condition. In order to return to steady state, the flowrate from the ship to the tank must be reduced. If contact with the ship is established, the flow from the ship will be reduced and the system will return to its steady state. Otherwise the pressure control system will activate the closure of PV-202B valve with the already mentioned consequences if contact with the ship is still interrupted. Each of the ''no contact'' places, P10 and P13, have already been assigned a token, since ''no contact establishment'' is assumed between ship and terminal operators from the beginning of the scenario. However, if we put a token in the place P12 ''contact with ship'' the transition T11 will be enabled and fired to return the system to its steady state. The event sequence that leads to the accident is then stopped.

If no token is put in the place ''contact with ship'' then the event sequence will continue to close valve HV-205, to create backpressure from the ship and subsequently create a water hammer in the loading pipe which will result in ammonia release.

Table 1
Places and Transitions of the Petri Net graph

Places	Name	Description
P1	Initial state	Initial state of unloading procedure
P2	Steady state	Steady state of unloading
P3	Reduced compressors capacity	Refrigeration capacity from the compressors is reduced
P4	All compressors in use	Three compressors are in use
P5	Normal temperature	Temperature $< -33\ ^{\circ}C$
P6	Normal flowrate	Flowrate $< 500\ m^3/h$
P7	Normal level	Level in tank $< L_{max}$
P8	Unsteady state	System enters in unsteady state
P9	Contact with ship 1	Contact is established within the ship and the terminal operators
P10	No contact with ship 1	No contact is established within the ship and the terminal operators
P11	Flow reduction	Flow reduction in the loading pipe
P12	Contact with ship 2	Contact is established within the ship and the terminal operators
P13	No contact with ship 2	No contact is established within the ship and the terminal operators
P14	Backpressure	Backpressure from the ship
P15	Line rupture	Water hammer in the loading pipe, which leads to line rupture and ammonia release
Transitions		
T1	Unloading normal	Unloading proceeds normally
T2	Lose compressor 1	Compressor 1 does not work
T3	Lose compressor 2	Compressor 2 does not work
T4	Lose compressor 3	Compressor 3 does not work
T5	Temperature increase	Temperature increases $> -33\ ^{\circ}C$
T6	Flow increase	Flowrate increases $> 500\ m^3/h$
T7	Level increase	Level in tank increases $> L_{max}$
T8	Unloading problem	Unloading proceeds with problem
T9	Reduce flow from the ship 1	Ship pumps reduce the flowrate from the ship to the terminal
T10	PV-202 B closed	Valve PV-202B on the loading pipe (near tank) is partially closed
T11	Reduce flow from the ship 2	Ship pumps reduce the flowrate from the ship to the terminal
T12	HV-205 closed	Valve HV-205 on the loading arm is closed
T13	Pressure increase on line	Pressure is increased between the ship and the loading arm

8. Comparison

According to the criteria set in section 2 and the authors' personal views, the results of the application of the three analysis techniques are presented in Table 2. All the three techniques (ETA, FTA and Petri Nets) visualize in a satisfactory level the sequence of events up to accident occurrence. However, the event trees seem to offer a better representation of the event agents that participate in the accident. The other two techniques have a rather average (Petri Nets) or poor (FTA) visualization of the event agents. The agent representation in the event trees is concrete and very clear since the former are represented as headings. Each heading represents a different agent or group of agents. This is not happening though with the representation of events dependencies and events interactions where Petri Nets have a significant advantage compared with the other two techniques. Indeed the Petri Nets were very useful in grouping both human errors and mechanical equipment interactions, as well as in showing the preconditions for the realisation of each event, elements which were not presented in a clear way with the event trees and the fault trees.

Table 2
Comparison results for the three examined techniques.

Criteria	Event Trees	Fault Trees	Petri Nets
Event sequence	Good	Good	Good
Event agents	Good	Sufficient	Average
Event dependencies	Average	Average	Good
Event interactions	Average	Average	Good
Modeling time and duration	Sufficient	Sufficient	Good
Modeling assumptions	Sufficient	Average	Good
Modeling concurrencies and conflicts	Sufficient	Average	Good
Modeling error recovery	Average	Sufficient	Good
Modeling the context of work	Average	Good	Average

Considering the time modeling, only the Petri Nets have the ability to represent the time sequence of the events along with their duration. Even though FTA can be annotated with citations of real time, the problem still remains with the representation of events that have certain duration. Event trees can be arranged in chronological order but there is no way they can represent duration of the events.

For the modeling of assumptions, which is a basic element for the analysis of accidents as dynamic events, and since the analysts may not have all the necessary evidence from the beginning of the analysis, the Petri Nets seem to be the only technique, from the three examined here, that can model assumptions. Assump-

tions can be modeled by initiating new scenarios by putting tokens in different places or by removing them from existing ones. However, the representation of assumptions may be possible in the other two methods by using dotted lines or separate branches in the trees. Concurrencies and conflicts are better represented with Petri Nets, while event trees have no such possibility and Fault trees could possibly do it with the use of specific notation (INHIBIT gate).

Since accident analysis of hypothetical scenarios aims at the identification of factors in the work context that may cause an accident and at the development of error recovery paths, Petri Nets offer a good solution to this end, by representing them visually. Fault trees, on the other hand, can model the work context by going deep into the representation of the surroundings of operators, things that can affect their perception and increase their workload. Additionally, fault trees can be very extended with the primitive causes of an accident and can cover all the possible initiating events of the accident scenario. The simulation that is made with the Petri Nets and the Event trees is more specific and not so extended, as they focus on particular event sequences.

One should also mention, that the simulation efficiency of Petri Nets is traded off by the ability of the analyst to operate a tailor made software package powered by mathematical algorithms, while event trees and Fault trees could even be manually constructed. Additionally, modeling with Petri Net is subjective to the analyst's experience and familiarity both to the plant and to the software. Although the model interface may differ, the results are affected in the same manner as in Fault Tree and Event Tree analysis, where representation is also depending on the subjectivity of the analyst.

9. Conclusions

In this paper, three accident analysis techniques are presented and compared regarding their efficiency vs. the demanded resources. The complexity of modern industrial systems has prompted the development of accident analysis techniques focusing on specialized aspects of the system. Although it is difficult to find a single technique that integrates the different types of analysis (event analysis, human error analysis etc.), accident analysis techniques should provide appropriate input to other techniques such as "classical" risk analysis ones. The idea of criteria classification to fulfill this requirement has been proposed by other researchers and it is used here too. The comparison is done through the application of Event Tree analysis, Fault tree analysis and Petri nets technique—two relatively simple and a more demanding methodology—on the same scenario from a hazardous chemical facility in view of analyzing a hazardous transfer procedure.

As accident scenario analysis techniques are essential in learning lessons in the chemical industry and in preventing the occurrence of such events in the future, all of these techniques proved to be very useful. We found, that the Petri nets offer better time/duration depiction of an accident development, while Event trees present better the agents and Faults tress the primary events that may affect them. Together with the aftermath of the accident or the near-miss, these methodologies can even be used as a means of accident reconstruction, where the human factor is involved, is an urging demand by a variety of people: (a) those involved in it, (b) of their relatives (in the case of death) and (c) of the competent authorities, who are asked to investigate the accident and pronounce the verdict.

Acknowledgements

The Financial support of the EU Commission through project "PRISM" GTC1-2000-28030 to this research is kindly acknowledged.

References

Amendola, A., Christou, M., Fiori, M., Kozine, I., Lauridsen, K., Market, F. (2002). *Assessment of Uncertainties in Risk Analysis of Chemical Establishments* "The ASSURANCE project" (ENV4-CT95-0627), Final report.

Cacciabue, P. C. (2000). Human factors on risks analysis of complex systems. *Journal of Hazardous Materials*, *71*, 101–116.

CCPs of AIChE (1992). *Guidelines for chemical process quantitative risk analysis*. NJ

Embrey, D. E., Kirwan, B., Rea, K., Humphreys, P., Rosa, E. A. (1984). SLIM-MAUD. *An approach to Assessing Human Error Probabilities Using Structured Expert Judgment*. *Vol. 1*, Washington, DC: NUREG/CR-3518 US.

Hollnagel, E. (1998). *Cognitive reliability and Error analysis method*. London: Elsevier.

Kim, J. W., & Jung, W. (2003). A taxonomy of performance influencing factors for Human reliability analysis of emergency tasks. *Journal of Loss Prevention in the Process Industries*, *16*, 479–495.

Kontogiannis, T., Leopoulos, V., & Marmaras, N. (2000). A comparison of accident analysis techniques for safety critical man-machine systems. *International Journal of Industrial Ergonomics*, *25*, 327–347.

Leopoulos, V. N. I. (1984). *Similateur pour les Reseaux de Petri Temporises*. Research Report 371 INRIA, France.

Papazoglou, I. A., Nivolianitou, Z., Aneziris, O., & Christou, M. (1992). Procedural steps for probabilistic safety analysis in chemical installations. *International Journal of Loss Prevention in the Process Industries*, *5*, 181–191.

Swain, A. D., & Guttman, H. E. (1983). *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*. Washington, DC: US NUREG.

Tutorial Artifex 4.1 (1997). Torino: Artis s.r.l., Italy.