



Université d'Oran 2
Institut de Maintenance et de sécurité Industrielle

THESE

Pour l'obtention du diplôme de Doctorat « L.M.D »
En Sécurité Industrielle et Environnement

Simulation of Industrial Accidents Due to Uncontrolled Pressures

Présentée et soutenue publiquement par :
Mr. Taleb Berrouane Mohammed

Devant le jury composé de :

Zebirate Soraya	PR	Université d'Oran 2	Président
Lounis Zoubida	PR	Université d'Oran 2	Directeur de thèse
Hassini Abdelatif	PR	Université d'Oran 2	Examineur
Sakhri Larbi	PR	Université d'Oran 1	Examineur
Haffaf Hafid	PR	Université d'Oran 1	Examineur
Benabadji Nouredine	PR	Université Mohamed Boudiaf USTO	Examineur

Année 2016 - 2017

List of publications

➤ Reviewed Journal Articles

1. **Talebberrouane, M.**, Lounis, Z., 2016. Safety assessment of flare system by fault tree analysis. *Journal of Chemical Technology and Metallurgy*. 51-2: 229-234.
2. **Taleb-berrouane, M.**, Khan, F., Lounis, Z., 2016. Availability analysis of safety critical systems using advanced fault tree and stochastic Petri net formalisms. *Journal of Loss Prevention in the Process Industries* 44: 193-203.
<http://dx.doi.org/10.1016/j.jlp.2016.09.007>

➤ Reviewed Conference Proceedings

1. **M. Taleb-Berrouane.**, Z. Lounis., 2014. Etude & Simulation Du Phénomène De B.L.E.V.E Sur Un Réservoir De Stockage D'ammoniac (In French). *International Conference on Engineering of Industrial Safety and Environment*.
2. **M. Taleb-Berrouane.**, Z. Lounis., 2015. Safety Performances Assessment of a LNG Flare System. *Colloque International sur l'Environnement et le Développement Durable*.
3. **M. Taleb-Berrouane.**, Z. Lounis., 2015. *Using fault tree analysis in probabilistic safety assessment. Sixièmes Journées de Chimie - EMP-Alger*.
4. **M. Taleb-Berrouane.**, Z. Lounis., 2016. Risk Assessment Indicators Of Process Systems By Using Bwo-Tie Method. *Colloque National Maintenance - Qualité CNMQ-16*
5. Fatima Benomar, **Mohamed Taleb Berrouane**, Zoubida Lounis., 2015. Les enjeux de la cyber sécurité des systèmes industriels. *Ière Conférence Internationale sur la Sécurité Interne d'Etablissement (CISIE'1-2015)*. IHSI- UNIVERSITE DE BATNA, Algérie.
6. Zoubida lounis, Benomar Fatima, **Mohammed Taleb Berrouane.**, 2016. Hazard Study Of Underground Gas Storage Tanks Using Method MAD'S MOZAR. *Colloque National Maintenance - Qualité CNMQ-16*.

Acknowledgements

I would like to express my sincere and profound gratitude to my supervisor, Pr. Zoubida Lounis and co-supervisor Dr. Faisal I. Khan for their guidance and untiring support throughout my doctorate research at the *Maintenance and Industrial Safety Institute – University of Oran 2* and *Centre For Risk, Integrity and Safety Engineering (C-RISE) - Memorial University of Newfoundland*. I must assert that I have benefitted immensely from their versed expertise in the field of my research. Their advices and resourceful suggestions have made my program a fruitful one. I am thankful to other professors and researchers, Pr. Larbi Sakhri and Dr. Ming Yang for their critical comments and constructive remarks in improving the quality of my research papers.

I am highly grateful to my parents and wife for being there for me through thick and thin. I am especially indebted to my brotherly friends and family members, Adel Dehane, Dr. Assem Hassan, Alaa Hassan, Lorinda McCarthy, and Yassine Hannit for their kindness during my research program.

Dedicated to

*Almighty Allah for His infinite mercy and guidance in my life, my mother,
father, wife, siblings and friends*

TABLE OF CONTENTS

List of publications	I
Acknowledgements	II
Dedicace.....	III
List of Tables	IV
List of Figures	V

General Introduction

Objectives of the Research	3
Organization of the Thesis	5

Chapter 1: Risk Assessment and Accident Modelling

1.0 Introduction	7
1.1 Process component failure	7
1.2 Techniques for failure prevention.....	8
1.3 Important notions in safety analysis.....	9
1.3.1 Safety analysis.....	9
1.3.2 Safety and risk assessment.....	10
1.3.3 Difference between safety and dependability	11
1.3.4 Difference between modelling and simulation	11
1.4 Literature review.....	12
1.5 Conclusion.....	16

Chapter 2: Risk Assessment Using Logical Diagrams

2.0 Introduction.....	19
2.1 Types of logic diagrams.....	19
2.1.1 Fault tree.....	19
2.1.1.1 Procedure for top-down approach to identify the cutsets.....	27
2.1.1.2 The procedure for bottom-up approach to identify the cutsets.....	28
2.1.1.3 Importance factor estimation.....	29
2.1.2 Advance fault trees.....	30
2.1.2.1 Dynamic fault tree.....	31

2.1.2.2 Fault tree driven Markov process.....	31
2.1.2.3 Fault tree coupled with Binary Decision Diagrams.....	32
2.1.2.4 Dynamic fault tree coupled with Markov process.....	32
2.1.2.5 Boolean Logic Driven Markov Process (BLDMP).....	32
2.1.3 Event tree.....	32
2.1.3.1 The steps of ETA.....	33
2.1.4 Reliability Block Diagrams.....	34
2.1.4.1 Definition and basic concept.....	34
2.1.4.2 Construction of a reliability block diagram.....	38
2.1.4.3 RBD simplification.....	40
2.2 Conclusion.....	41

**Chapter 3: Risk Assessment of Gas Flare Systems by
Fault Tree Analysis “LNG Flares”**

3.1 Abstract.....	46
3.2 Introduction.....	46
3.3 Experimental.....	47
3.3.1 Case study	47
3.3.2 Analysis of flameout incident.....	48
3.4 Results and discussion.	52
3.5 Conclusions.....	52

Chapter 4: Risk Based Modelling Using Advanced techniques

Part 1: Bayesian Networks

4.0 Introduction.....	55
4.1. Definitions and basic concept.....	55
4.1.1 The conditional probability.....	56
4.1.2 The Bayes’ rule.....	56
4.1.3 The conditional independence.....	59
4.1.4 Evidence and data updating.....	60
4.2 Types of Bayesian Network.....	60
4.2.1 Static Bayesian Networks.....	60

4.2.2 Dynamic Bayesian Networks.....	60
4.2.3 Influence Diagram.....	61
4.3 Advantages of the Bayesian network.....	61
4.4 Disadvantage of the Bayesian networks.....	62
4.5 Applications.....	62
4.5.1 Application on offshore drilling operations.....	62
4.5.2 Application on dynamic safety barriers assessment.....	65
4.6 Conclusion.....	68
Part 2: Petri Nets	
4.7 Introduction.....	70
4.8 Definitions and basic concept.....	70
4.8.1 Places, Transitions and Arcs.....	71
4.8.2 Marking.....	71
4.8.3 Transition firing	72
4.8.4 Autonomous and non-autonomous Petri Net.....	72
4.9 Special Petri Nets.....	73
4.9.1 Particular structures.....	73
4.9.1.1 State Graph.....	73
4.9.1.2 Event graph.....	73
4.9.1.3 Conflict free PN.....	73
4.9.1.4 Free choice Petri Net.....	74
4.10 Simple Petri Net.....	74
4.11 Pure Petri Net.....	75
4.12 Generalized Petri Nets.....	75
4.13 Finite Capacity PNs.....	76
4.14 Extended Petri Nets.....	76
4.15 Priority Petri Nets.....	77
4.16 Petri Nets modelling power.....	82
4.17 Limitations of Petri Nets.....	83
4.18 GSPN with predicates and assertions.....	83

4.19 Conclusion.....	84
----------------------	----

Chapter 5: Applications of Risk Based Assessment Using Petri Nets Formalisms

Part 1: Risk Based Assessment of Gas Flares Systems by using Time Petri Nets

5.0 Introduction.....	87
5.1 Removal Liquid System.....	88
5.1.1 Knockout Drum.....	88
5.1.2 Liquid overflowing occurrence.....	89
5.2 Petri Nets Modeling.....	92
5.2.1 Petri nets.....	92
5.2.2 Time Petri nets.....	93
5.2.3 TiNA tool.....	94
5.3 Case Study.....	94
5.3.1 Liquefaction Natural Gas (LNG) cold flare.....	94
5.3.2 Liquid overflowing modeling.....	95
5.3.3 Removal liquid system modeling.....	98
5.3.3.1 Normal operating modeling	98
5.3.3.2 LSH failure with poorly monitoring.....	100
5.3.3.3 Failure of LSH and LI.....	100
5.3.3.4 Pump failure with poorly monitoring.....	100
5.4 Results And Interpretations.....	101
5.4.1 Results.....	101
5.4.2 Results interpretation and recommendations.....	101
5.5 Conclusion And Future Works.....	102

Part 2: Risk Based Availability Analysis of Gas Flares Systems Using Advanced Fault Tree and Stochastic Petri Net Formalisms

5.6 Introduction.....	104
5.7 Brief description of FTDMP.....	107
5.8 Overview of PNs and GSPN.....	109
5.9 Application Of The Formalisms.....	112

5.9.1 Problem statement.....	112
5.9.2 FTDMP Model.....	113
5.9.3 Stochastic Petri Nets modelling.....	117
5.10 Results & Discussion.....	121
5.11 Conclusions.....	123

List of Tables

Table 1.1 - Literature survey on the use of GSPN with predicates and assertions.....	14
Table 2.1 -The different kind of FT gates.....	22
Table 2.2 - The different kind of event's presentation.	22
Table 2.3 – Logic gates' calculation formulas.....	26
Table 2.4 – The probability rules.....	26
Table 2.5 – The top-down approach to identify the cutsets.....	29
Table 2.6 – Results of the bottom-up approach.....	30
Table 3.1 Occurrences probabilities (λ) of elementary events.....	49
Table 3.2 Results of the FTA study.....	52
Table 4.1 Probabilities tables in BN modelling.....	58
Table 4.2 - conditional probabilities tables.....	66
Table 4.3 The UVC consequences and their probabilities.....	67
Table 4.4 - The pointing parts and their descriptions.....	78
Table 4.5 - Quantitative results using Time Petri network.....	80
Table 4.6 - Comparative analysis.....	80
Table 5.1 Occurrences probabilities and durations of initiators events.....	95
Table 5.2 Places and their meanings.....	96
Table 5.3 Transitions and their meanings.....	97
Table 5.4 Scenarios and their causes.....	97
Table 5.5 Occurrences times of the different scenarios.....	101
Table 5.6 Scenarios and their implicated elements.....	102
Table 5.7 Preventive maintenance planning.....	102
Table 5.8 Accident consequences.....	115
Table 5.9 Basic events and their periodic maintenance parameters.....	116
Table 5.10 Elementary events and their occurrence rates (exponential distribution).....	117
Table 5.11 Average event occurrence frequency for 30 years of service.....	121
Table 5.12 Selected additional frequencies given by GSPN at 90% confidence interval.....	123

List of Figures

Figure 1.1 - Classification of risk assessment methods.....	11
Figure 2.1 - System safety analysis procedure.....	20
Figure 2.2 - Fault tree components.....	21
Figure 2.3 – Basic terminology for the fault tree.....	23
Figure 2.4 - The fault tree development.....	25
Figure 2.5 - A standard fault tree.....	27
Figure 2.6 - Example of an initiating event and related safety functions.....	33
Figure. 2.7 Example of a series RBD.....	35
Figure. 2.8 Example of RBD for Active Redundancy.....	36
Figure. 2.9 Example of RBD for a Series Combination of Active Redundancy Groups (series-36 parallel).....	36
Figure. 2.10 Example of RBD for Standby Redundancy.....	37
Figure. 2.11. Representation of Series Function with n elements.....	38
Figure. 2.12 Representation of Redundant Functions with n elements.....	39
Figure. 2.13. Parallel combination of active redundancy groups (parallel-series).....	40
Figure 2.14. Equivalent structures in RBD.....	41
Figure 3.1 - Steam assisted flare system (Ling., 2007).....	48
Figure 3.2 - Flameout fault tree.....	50
Figure 3.3 - Flame detachment fault tree.....	51
Figure 3.4 - Pilot pressure fault tree.....	51
Figure 4.1 - Simple example of a Bayesian network.....	58
Figure 4.2 - Example of a dynamic BN.....	61
Figure 4.3 – BN application on well control failure scenarios and consequences.....	63
Figure 4.4 – Data from the BN model of offshore drilling operations.....	64
Figure 4.5 – Results from the BN model of offshore drilling operations.....	65
Figure 4.6 - Static Bayesian network for safety barriers response.....	65
Figure 4.7 – Dynamic Bayesian network for the safety barriers.....	68
Figure 4.8 – An example of a simple structure of a Petri network.....	71
Figure 4.9 – transition firing demonstration of a simple Petri network.....	72

Figure 4.10 – Example of unmarked Petri network.....	73
Figure 4.11 – An example of a conflict situation in a Petri network.....	73
Figure 4.12 – An example of a simple Petri network.....	74
Figure 4.13 – Example of an impure net.....	75
Figure 4.14 – An example of the firing process in the Petri networks.....	75
Figure 4.15 – An example of the firing process in a looping network.....	76
Figure 4.16 – An example of the firing process with inhibition arcs.....	77
Figure 4.17 – An example of the priority in Petri networks.....	77
Figure 4.18 - Qualitative modelling using Petri Nets.....	78
Figure 4.19 - Pointing the strong points of PN modelling.....	78
Figure 4.20 - Quantitative modelling using Time PN.....	79
Figure 4.21 - Pointing the characteristics of the Stochastic PN with predicates and assertions.....	83
Figure 5.1 - Flare Knockout Drum.....	89
Figure 5.2.a Start of the flaring event.....	90
Figure 5.2.b Liquid fall out and flaming rain from flare flame.....	91
Figure 5.2.c Flaming liquid engulfs flare stack.....	91
Figure 5.3 - Time Petri net model for the liquid overflowing incident.....	96
Figure 5.4 Time Petri net model of normal operating.....	98
Figure 5.5 State classes of normal operating.....	99
Figure 5.6 State classes graph of normal operating system.....	99
Figure 5.7 Graph of occurrences times.....	101
Figure 5.8 Markov model of periodically tested component.....	108
Figure 5.9 Glossary of PN notations.....	109
Figure 5.10 Mapping approach from FT to GSPN with predicates.....	112
Figure 5.11 A simplified P&ID of the flare system.....	113
Figure 5.12 Fault tree of the flare liquid overflowing.....	114
Figure 5.13 Event tree of the flare liquid overflowing.....	115
Figure 5.14 Example of Markov model to be embedded in the fault tree.....	116
Figure 5.15 PN of Draining pumps.....	118
Figure 5.16 Sensor 1 behaviour modelling using PN.....	119
Figure 5.17 PN modelling of the top event.....	120

Figure 5.18 PN modelling of top event consequences.....	120
Figure 5.19 Mean availability of flare system given by (a) GSPN (b) FTDMP.....	122

SIMULATION OF INDUSTRIAL ACCIDENTS DUE TO UNCONTROLLED PRESSURES

General Introduction

Risk Assessment (RA) is nowadays a commonly used term in many different disciplines (e.g. economy, industry, human resources, IT). Its goal is firstly to identify risks (e.g. of a machine operation, human behaviour or of a whole system), which can cause harm to properties, persons or environment. Secondly the RA should evaluate probabilities and severities of these unwanted events and propose measures for their elimination or a reduction of their impact. This whole process should be periodically repeated to assess influences of the measures of a risk control on detected risks. If the risks are mitigated insufficiently, then there should be additional measures proposed.

This general interdisciplinary approach could be split into three parts or phases. This Ph.D. thesis focused on its first phase: the risk analysis, there are few commonly used traditional risk analysis methods in the industry area e.g. Fault Tree Analysis (FTA) or Event Tree Analysis (ETA). These methods were developed many years ago, so their original definitions do not meet today's requirements for analysis of large and complex systems or accidental scenarios with different types of dependencies and dynamic changes. Different industrial areas have developed their own narrowly focused methods during this last years, even though there could be, for selected tasks, used some of the mentioned common, but slightly modified methods.

Based on the stated facts, this Ph.D. thesis is focused on the analysis of traditional methods (FTA, ETA and Bayesian networks), and non-traditional methods (Petri Nets), on a detection of their specific problems and mainly on a proposal of new alternative universal methods which are able to solve the mentioned problems. These new methods should integrate more than two phases of the RA together and they have to be practically usable. As a framework for a design of new methods, Petri nets (PN) were chosen. They are often used for a modelling and analysis of discrete event systems (DES), but they are still not common in the area of the RA.

It's worth noting that the process industry and especially the oil and gas industry are based on the fluids pressure dynamics. It means that the pressure is the dominant and the most hazardous parameter to be controlled and supervised carefully. In order to demonstrate and highlight the abovementioned methods, we conducted our study on several case study, one of our applications is conducted on a LNG gas flares in Arzew industrial area (Talebberrouane and Lounis., 2016). As an example, we used of FTA to assess the performances of a flare system in

SIMULATION OF INDUSTRIAL ACCIDENTS DUE TO UNCONTROLLED PRESSURES

process industry. The goal of the analysis is to illustrate the methodology of FTA while proposing some new feature to it. The second part of the thesis introduces the Bayesian Networks with their mathematical basics, their different concepts and applications. The third part of the thesis introduces a concept of the PN as a tool for a solution of selected problems of traditional RA methods. The Stochastic Petri Nets have been selected for modelling and simulation of accidents in process industries. The final part of the thesis presents a the Generalized Stochastic Petri Nets with predicates as an alternative approach for risk modelling. This formalism is able to model the whole accidental scenario without use of the traditional FTA and ETA. It extends a classical approach with an ability to easily model dependencies and dynamic changes of an event sequence in the scenario. This method is fully usable and is supported by existing commercial software tools.

This doctoral thesis demonstrates that the GSPN with predicates are still a little bit overlooked but powerful framework for risk analysis and management and offer new possibilities for modelling, simulation and analysis.

Objectives of the Research

The main objective of this research is to develop a methodology for modelling and simulation of complex systems' failures caused by uncontrolled pressures, their occurrences, progresses and consequences. We propose to conduct a critical analysis of the conventional modelling techniques in safety analysis such as Faut tree analysis, Event tree analysis and Bayesian networks. These techniques are still largely used and based on their modelling results, important decisions related to the safety sector, are taken. This focus obliges us to detail their modelling features and propose an alternative modelling technique. At this stage, we propose an extended formalism of Petri Nets as the suitable technique for safety analysis and accident modelling. In process industry, these failures can lead to devastating industrial accidents. The methodology is based on the probabilistic risk assessment methods. Figure 2 presents the three pillars of this work. The analysis and applications of these three probabilistic methods allow the identification of the appropriate approach to model the industrial accidents in process industries.

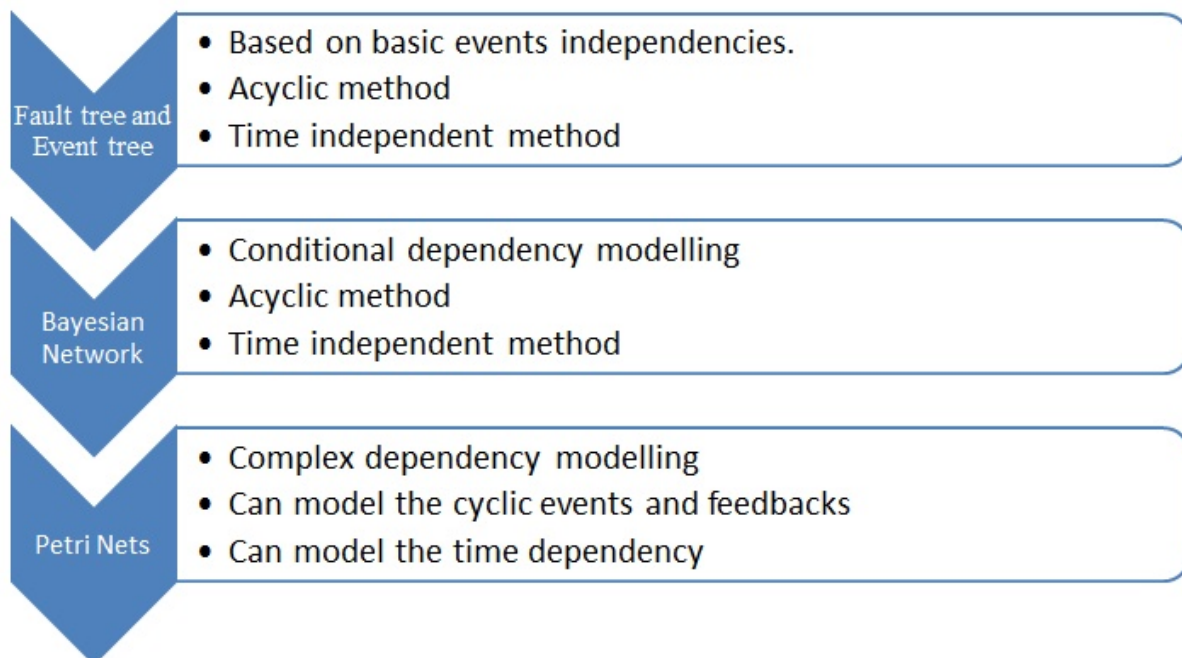


Figure 1 - The probabilistic risk assessment methods and their characteristics.

SIMULATION OF INDUSTRIAL ACCIDENTS DUE TO UNCONTROLLED PRESSURES

The first research area was the Fault Tree Analysis (FTA) and its application in safety analysis of process industry that led us to think about the accuracy of this method facing the complex process systems. Then, little by little, the idea of targeting techniques of higher modelling levels took shape. From Bayesian Networks (BN) to Timed Petri Nets (TPN) until extended form of Stochastic Petri Nets (SPN), our investigation to find the formalism that fit the best to this sensitive research area.

Organization of the Thesis

The outlines of the following chapters are presented below:

- Chapter 1 discusses safety related notions such as, modelling, simulation and risk assessment. It presents and introduces the quantitative risk assessment techniques. The international standards related to some modelling techniques are also detailed.
- Chapter 2 discusses the use of the logical diagrams as fault trees and event trees analysis for risk assessment. A detailed explication of each step of the methodology is provided. The qualitative and quantitative results are highlighted and discussed. The study is extended to the advance hybrid formalisms, their novelties and applications.
- Chapter 3 presents one of our research works, related to the application of Fault tree analysis in safety analysis.
- Chapter 4 discusses the use of Bayesian network in probabilistic risk assessment. This comprises a full description of the BN modelling and several illustrations via examples. The probabilities updating as new information are available was also treated in this chapter.
- Chapter 5 presents the use of Petri Nets in probabilistic risk assessment. Different categories of PN are detailed as simple PN, Timed PN and stochastic PN. A comparative study between FT, BN and PN is also provided.
- Chapter 6 presents one of our research works, related to the development of Time Petri Nets (TPN) and their application. This research work was submitted to a scientific journal and it is in review process, however we aimed to present this work to show the application of this Petri Nets formalism in risk assessment.
- Chapter 7 presents one of our research works, related to the development of Petri networks and their application in RAMS analysis.

SIMULATION OF INDUSTRIAL ACCIDENTS DUE TO UNCONTROLLED PRESSURES

- The presentation of this entire thesis work ends in a general conclusion summarising the different contributions which have come from it and which should provide a better understanding and rational use of stochastic Petri Nets in safety analysis. At least, we hope so. Whilst there is still a lot of work to be done, there is also the perspective for later studies.

Chapter 1

Risk Assessment and Accident Modelling

1.0 Introduction

The terms ‘safety’ and ‘risk’, which are often associated, are familiar to us, because they are largely present in our daily lives. It is, however, clear that they are given many different meanings and therefore many definitions. This significant heterogeneity can be explained by the varied and sometimes variable perception of the people being questioned, due to the diversity of their personal concerns, their training, their profession, their experiences and their local and time-related context, not to mention influence factors. It is therefore natural that these notions have, for many years, been the source of many different projects and reflections which produced multiple works and publications in all domains of knowledge relating to law, sociology, medicine, economics or sciences and techniques (Amalberti et al., 2003). The topic of safety and risk is therefore vast and complex. If questions of safety seem to make the headlines more and more, it is because they are always linked to our society’s concerns and aspirations at the time. They are not a new phenomenon and only really emerge when they are sparked off by social rebuff. The conditions that expose such a rebuff are well-known: the triggering event for this social reaction must be perceived as unfair and abnormal. Even though we have to admit that occupational accidents no longer catch people's attention as a priority, even though they are covered by sustained legislative actions. Major technological accidents (Directive SEVESO II, 1996) continue to be perceived as unacceptable due to their generally disastrous consequences on peoples’ lives, on the environment and on the economy. It is then easy to understand that to meet society’s safety aspirations, the competent authorities had to provide legislation by firstly relying essentially on the post-analysis of how accidents occurred and what their consequences were. In order to simplify our point, we might consider that this approach to safety and the different ensuing regulations are the result of a certain materialisation of acquired experience, i.e. of experience feedback.

1.1 Process component failure

All components are undergoing deterioration with time due to natural and assignable causes. Through years of process service, this deterioration can manifest suddenly by failure of one or more system’s components which can be followed by a sequence of events with increased complication degrees. It lasts for a period of time and causes damages on human, environment

and materials with direct and indirect loss of profits. Failures can also be caused by third party damage such as seismic acceleration, material and fabrication defects, and human factors. However, studies indicate that majority of failures are contributed by time-dependent structural degradations (Faber, 2002; Khan et al., 2006). The quantification of component integrity can be established by understanding the physics of time-dependent failure processes and its adverse consequences. Traditionally, the codes and standards that are used for inspection and maintenance are prescriptive rules based on experience. Most of the time they have been formulated in response to significant failure cases. They neither take into account all types of failures, nor the various sources of uncertainty arising from degradation processes associated with the facility's operation. API 581 (2000) highlighted the need to develop an industry failure database and software to support the risk based inspection planning and expands the program to fit into several industry initiatives. Leaks and rupture are the principal causes of hydrocarbon release, fire, and explosions in process facilities. Studies indicate that corrosion is the principal cause of about 15% of leakage occurrences (HSE UK, 2002). Good inspection and maintenance optimization need a reliable determination of degradation mechanisms and their consequences. This can be achieved with risk analysis by combining the stochastic degradation modelling with consequence analysis (Faber, 2002).

1.2 Techniques for failure prevention

The time-dependent mechanisms which describe the failure of process components are random processes and hence it will have large uncertainty in the degradation data. Thus, it is appropriate to use stochastic models to accurately describe these mechanisms. Due to this uncertainty in determining the failure mechanisms, there will always be a certain probability that a given component of the process facility fails during its operation. The life cycle integrity threats may be reduced through well established procedures of design, fabrication, quality assurance and quality control and stringent policies and regulations. However, once the offshore process facility is operational, the age-related or time-dependent degradation processes reduce its strength and material. Therefore, during the operational stage, the best way to predict failure is through inspection and prevent failure is through maintenance. In recent years, risk based inspection has emerged as an area of interest in asset integrity management (Faber, 2002; Khan et al., 2006). Risk based inspection can be classified as qualitative, semi-quantitative, and fully

quantitative. A robust, quantitative risk based inspection model based on reliable, probabilistic structural degradation mechanisms and consequences analysis of offshore process components is not yet published in literature. The various maintenance strategies include reactive and proactive maintenance programs. Reactive maintenance is based on the principle "fix it as it fails", which is costly due to abrupt commodity loss and unplanned shutdowns. The recent developments in maintenance are total productive maintenance (TPM), reliability centred maintenance (RCM) and the condition based maintenance (CBM). However, their applications are limited as they focus on likelihood of failure only. Failures result in direct economic consequences such as loss of commodity, loss due to shutdown, spill clean-up and environmental damage costs. Inspection and maintenance also have direct and indirect economic consequences. Hence, optimizing maintenance on the basis of actual condition and failure consequences is to be investigated. Risk based integrity management models are emerging as a rational choice.

1.3 Important notions in safety analysis

Despite the affluent safety terminology, the basic concepts suffer from misunderstanding and improper usage. We consider that divergences in the use of terms and the resulting confusion of interpretations are a barrier to the sharing of safety knowledge and safe practice. This problem becomes impractical when an industrialist prepares to develop the risk analysis files of the global system and is forced to collect a range of risk analysis studies relating to subsystems performed by contractors each with his own terminology, method and expertise.

1.3.1 Safety analysis

If the hazard exists everywhere at different levels, the adapted safety measures should be there as well. Through the statistical history, process industries shown that they have been continuously prone to incidents and accidents in multiple forms. Safety is defined as the absence of non-tolerated risks, which means that trying to eliminate every residual risk or the maximum of it is not an appropriate approach. "Risk zero" cannot be defined as an objective and cannot be reaching. The general concept of the appropriate approach or the most adapted approach till now is the definition of acceptable thresholds of residual risks. These acceptable thresholds can be estimated by the standards. Various international standards are used to verify compliance with legal requirement for organization/system. IEC 61508 (generic standard applicable to all

industries) and IEC 61511 (applicable to only process industry) are used as a benchmark for acceptable good practice for industry by worldwide Safety regulators for industry. For estimating reliability of a Safety Instrumented System (SIS), the IEC standard describes a number of possible calculation approaches including analytical formula, reliability block diagrams, fault tree analysis, Markov modelling and petri nets (Innal 2008). IEC standard do not mandate one particular approach or a particular set of formulas, but leave it to the user to choose the most appropriate approach for quantifying the reliability of a given system or function (IEC 2000). The standard specifies the risk and measures in the design of safety functions. It provides the functional safety requirements covering random hardware failure, systematic failure and common cause failures. IEC 61508 and IEC 61511 guides all necessary activities during the entire lifecycle of the systems for the *management of functional safety*. IEC 615081 entails to consider only random hardware failures and further recommends a proper safety management program to control systematic failures. Since systematic failures do not follow the same failure processes as random hardware failures (Jin et al., 2012). The standard gives a number of requirements to reduce the systematic failures.

1.3.2 Safety and risk assessment

The notions of safety and risk assessment are widely used in the industrial context, because they are largely present and occupied the authorities, the industrial companies and the large public as well. It is, however clear that they are having several meanings and several misunderstandings. Depending on the perception that professionals give to those notions according to their positions and backgrounds.

The managers will define it as the policies and procedures applied to ensure the safety and health of the employees within the workplace. It involves hazard identification and control according to government standards.

The safety staff will define it as the act to eliminate or minimize as possible as we can any source of potential damage, harm or adverse health effects on something or someone under certain conditions.

Scenario expecting does not mean it will indeed occur, but that there is a reasonable probability that it would occur (Khan et al., 2002). To study these accidents scenarios, we have a panel of methods shown in figure 1.

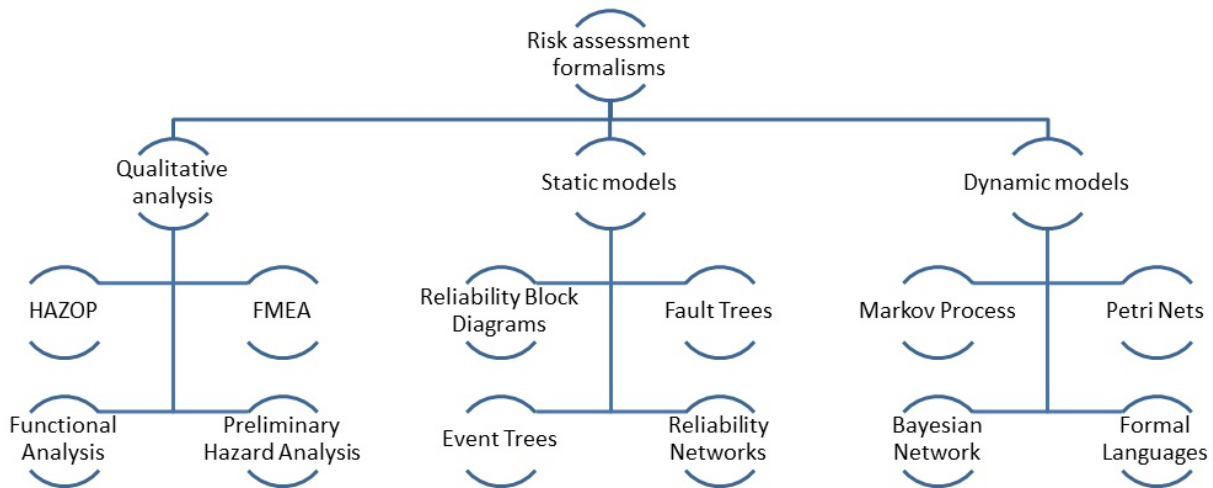


Figure 1.1- Classification of risk assessment methods.

1.3.3 Difference between safety and dependability

A system is considered operational if it can fulfill its designed missions or functions. We usually defined it as “required functions” as a function or multiples functions mandatory for the accomplishment of a service or an output in general.

Dependability, as a concept, is not a final goal at itself, but a means (methods, approach, tools, etc.) that make it possible to manage the risk. In other words, risk management is the goal, dependability is a mean to reach it. According to Heurtel (Heurtel, 2003), dependability is defined as qualitative and quantitative engineering task, a rich range of methods and concepts in service of the risk management. In other words and more formally, the dependability is defined as the ensemble of measured parameters based on probabilistic approaches. From the most used, the fault tree analysis (FTA), the event tree analysis (ETA) and reliability block diagrams (RBD).

1.3.4 Difference between modelling and simulation

The terms modelling and simulation are widely used in the modern engineering disciplines, without differentiation between them. In fact, the terms modelling and simulation are often used

to refer a same meaning which is a presentation or an imitation of a system. However in the specialised field, the two terms are used to two different meanings:

- **The modelling** is the act of producing or generating a model. The model is considered as a product that can be physical (i.e architecture mock-up) or digital (computer based) that represents a system. The model aims to imitate reality of the system as closer as possible, this makes the models similar to the represented systems with some simplifications or assumptions. Some models are imitating the graphical and design aspect of the model. For example, the buildings and infrastructures mock-ups. Others are more conceptual based and try to imitate the behaviour or the dynamic process. For example the CFD modelling or the probabilistic models as the case in this research work.
- **The simulation** is the operation or the procedure of using the generated model to study the system qualitatively or quantitatively in different aspects. The simulation can be executed multiple times to test the performance or any characteristic of the system without undergo the real cost, time, consequences and hazard of the experimental methods. In the last two decades, the simulation became the dominant technique for the optimization, training, prediction and other applications.

1.4 Literature review

In terms of managing risks, complete elimination is not entirely feasible and so the approaches aim to reduce them. When possible, risk reduction is conducted as far upstream as possible from the danger process, meaning at the source or as close to it as possible. To illustrate this, let us consider a production unit within a transformation or process industry. Risk identification methods try to reveal the sources of danger and the Undesired Event(s) (UE) likely to be caused or initiated by the process. The criticality for each UE places it in a two-dimensional risk space (probability, severity) and means we can appraise the extent of the efforts to be deployed to bring it to an acceptable or tolerable level. This reduction concerns, primarily, the probability of occurrence of the relevant UE and it is often obtained by successively laying several layers of protection between the danger source (the process) and potential objectives (persons, the installation itself, and the environment). There is a wide variety in the typology of the layers, ranging from control system which regulates the process with conventional safety

devices, such as valves or sensors (for pressure, temperature, level, etc.) which trigger an alarm and is then followed by the appropriate operator intervention. All these layers should be modelled properly in their behaviours, different phases in their life such as undetected failure phase, phase after detection, periodic maintenance phase and so on.

During the literature study, it was observed that there is a lack of literature on the use of GSPN with predicates and assertions in uncertainty analysis. This is due to the fact that this formalism was recently developed and just a couple of software package handle this kind of formalisms. The GSPN with predicates (Talebberrouane et al., 2016), started getting attention and approved for reliability studies in 2010, where the standard IEC 61508-6 (2010) defined and approved them. We have undertake a large investigation looking for papers using this Petri Nets formalism and we concluded our study in form of table summarizing all the papers dealing with this method, Table 1.1 is provided for this purpose.

Table 1.1 Literature survey on the use of GSPN with predicates and assertions.

Reference	Title	Type of study	Aim	Contribution
Hamzi et al., 2013	Performance Assessment of an Emergency Plan Using Petri Nets	Application on emergency plan	Risk based reliability assessment	<ul style="list-style-type: none"> • Assessment of performance indicators based on timed threshold of emergency response plan (ERP). • Demonstration of the utility of the timed variable “time()” in the transitions’ guards and assignments.
Cacheux et al., 2013	Assessment of the expected number and frequency of failures of periodically tested systems	Solving modelling constraint	Functional safety assessment	<ul style="list-style-type: none"> • Solving the problem of discontinuity on the availability curves • Demonstrating the superiority of GSPN with predicates on the other formalisms. • Provided the mathematical reasoning related to the modelling constraint
Signoret et al., 2013	Make your Petri nets understandable: Reliability block diagrams driven Petri nets	Development of new framework	Implementing a graphical improvement on the PN	<ul style="list-style-type: none"> • Attempted to improve the readability and the understandability of the formalism. • Presented a hybrid formalism mixing PN and reliability block diagrams • Provided a detailed illustrative application on a Safety Instrumented System (SIS)
Nývlt et al. 2015	Complex accident scenarios modelled and	Application on two	Accident scenario	<ul style="list-style-type: none"> • Modelling the dynamic behaviour of systems during the accident escalation.

	analysed by Stochastic Petri Nets	accident scenarios	modelling	<ul style="list-style-type: none"> • Provided the application of the formalism step by step through two different complication levels. • Provided additional presentation tool using blocks
Silva et al., 2015	Intermodal terminal cargo handling simulation using Petri nets with predicates	Application on container terminal	Availability analysis	<ul style="list-style-type: none"> • Highlighted the power of the formalism in solving complex logistic processes. • Provided a complete simulation of the whole system. • Observation of multiples outputs in the same time.
Brissaud and Luiz., 2015	Average probability of a dangerous failure on demand: Different modelling methods, similar results	Comparative computational study	Functional safety assessment	<ul style="list-style-type: none"> • Provided detailed calculation of probability of failure on demand (PFD) as required by IEC 61508 • Studied simple and redundant systems in several configurations (1oo2 and 2oo3). • Provided a comparative study at multiple levels

Table 1.1 presents a global literature overview of the work done using or dealing with the GSPN with predicates and assertions. These selected papers are connected with the topic of the thesis in their type of study and the contributions provided in these research work.

1.5 Conclusion

The main objective of this first chapter has been to provide some clarification regarding misinterpretations and misunderstanding when using the safety related terms and the differentiation between them. The main critique is that the meaning of these terms are usually not common everywhere and keep changing from place to place and from standard version to another. Additionally, the definitions are not sufficiently clear. It is an issue that relates to the importance of adequate risk communication. It also relates to different ways of interpretations with meaningful content. Besides, there are several associated terms, such as for example ‘critical failure’, ‘dangerous failure’, ‘detected failure’ and ‘critical dangerous failures’, which also to some extent attribute meaning to the term. This chapter discusses, explains and clarifies the relationship between the term “modelling” and the term “simulation” which are often considered as having the same meaning whilst leading to some misunderstandings. At the same time, several of the terms have been in use for a long time, and it is highly challenging to change their range of meanings by proposing more robust interpretations.

According to the previous statements and the literature survey on the use of GSPN with predicates and assertions, it can be concluded that this formalism has a great strength in the ability to model the dysfunctional state of a system and the operational state as well. It can be used for any kind of systems. Strong dependences among components can be modeled with reconfigurations over time, using deterministic or stochastic transitions: exponential, Weibull, triangular, uniform or any other law you may have programmed.

References

- API 580., (2002). Risk Based Inspection: API Recommended Practice 580. American Petroleum Institute, Washington DC, USA.
- Brissaud, F. and Luiz, F., 2015. Average probability of a dangerous failure on demand: Different modelling methods, similar results. 11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference, Jun 2012, Helsinki, Finland. 8, pp.6073-6082 *arXiv:1501.06487*.
- Cacheux, P.J., Collas, S., Dutuit, Y., Folleau, C., Signoret, J.P., Thomas, P., 2013. Assessment of the expected number and frequency of failures of periodically tested systems. Reliab. Eng. Syst. Saf. 118, 61e70. <http://dx.doi.org/10.1016/j.ress.2013.04.014>.
- Faber, M. H. (2002). Risk based inspection planning: the framework. Structural Engineering International 3: 186-194.
- Hamzi, R., Innal, F., Bouda, M. A., Chati, M., 2013, Performance Assessment of an Emergency Plan Using Petri Nets, Chemical Engineering Transactions, 32-2013.
- Heurtel, A. (2003). La gestion des risques techniques et des risques de management. CNRS - IN2P3/LAL.
- ISBN 978-88-95608-23-5; ISSN 1974-9791
- HSE UK (2002). Guidelines for Use of Statistics for Analysis of Sample Inspection of Corrosion. TWI Report fo r Health and Safety Executive, Research Report 016, Norwich, UK.
- IEC. 2000. "Functional Safety of Electrical/electronic/programmable Electronic Safety Related Sys-tems." International Electrotechnical Commision.
- IEC 61025., Fault Tree Analysis (FTA). Technical report. International Electrotechnical Commission; 2006.
- IEC 61508-6, 2010. Functional Safety of Electrical/electronic/programmable Electronic Safety Related Systems. International Electrotechnical Commission, Switzerland.

- IEC 62502., Analysis techniques for dependability — event tree analysis. Technical report. International Electrotechnical Commission; 2010.
- IEC 61078., Analysis techniques for dependability — Reliability block diagram and Boolean methods. International Electrotechnical Commission; 2006. Innal, F., 2008. Contribution to Modelling Safety Instrumented Systems and to Assessing Their Performance Critical Analysis of IEC 61508 Standard. PhD thesis. University of Bordeaux.
- Innal, F., 2008. Contribution to Modelling Safety Instrumented Systems and to Assessing Their Performance Critical Analysis of IEC 61508 Standard. University of Bordeaux.
- Jin, H., M. A. Lundteigen, and M. Rausand. 2012. “Uncertainty Assessment of Reliability Estimates for Safety-Instrumented Systems.” Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability 226 (6): 646–55. doi:10.1177/1748006X12462780.
- Khan, F., Haddara, M. M., Bhattacharya, S. K., Risk based integrity and inspection modeling (RBIIM) of process component s/system. Risk Analysis, 2006; 26(1): 203-221.
- Nývlt, O., Haugen, S. and Ferkl, L., 2015. Complex accident scenarios modelled and analysed by Stochastic Petri Nets. *Reliability Engineering & System Safety*, 142, pp.539-555. <http://dx.doi.org/10.1016/j.ress.2015.06.015>
- Signoret, J.P., Dutuit, Y., Cacheux, P.J., Folleau, C., Collas, S. and Thomas, P., 2013. Make your Petri nets understandable: Reliability block diagrams driven Petri nets. *Reliability Engineering & System Safety*, 113, pp.61-75. <http://dx.doi.org/10.1016/j.ress.2012.12.008>
- Silva, C.A., Guedes Soares, C. and Signoret, J.P., 2015. Intermodal terminal cargo handling simulation using Petri nets with predicates. Proceedings of the Institution of Mechanical Engineers, Part M: Journal of Engineering for the Maritime Environment, 229(4), pp.323-339.
- Talebberrouane, M., Khan, F., Lounis, Z., 2016. Availability analysis of safety critical systems using advanced fault tree and stochastic Petri net formalisms. *Journal of Loss Prevention in the Process Industries* 44: 193-203. <http://dx.doi.org/10.1016/j.jlp.2016.09.007>

Chapter 2

Risk Assessment Using Logical Diagrams

2.0 Introduction

The risk is usually initiated by one or more abnormal operation caused by component failure, human error and/or other external events (i.e environmental). The elementary causes are considered as root events triggering a chain of events affecting the whole system; these sequences are called “accidents’ scenarios”. The simplest and the most used methods to describe and to analyze the accidents scenarios, are the fault tree analysis (FTA) (IEC 61025., 2006) and the event tree analysis (ETA) (IEC 62502., 2010). Reliability Block Diagrams (RBD) (IEC 61078., 2006) are another kind of logical diagrams, they are widely used for reliability and availability studies. A reliability block diagram is a pictorial representation of a system’s reliability performance. It shows the logical connection of functioning components needed for a successful operation if the system (IEC 61078., 2006). Fault Tree Analysis (FTA) is one of the most important logic and probabilistic techniques used in the probabilistic risk assessment (PRA) and system reliability assessment (Stamatelatos and Vesely, 2002). The fault tree analysis is a logical diagram to identify and extract, in a structural way, all possible combinations leading to a predefined undesired event. Then, the main purpose of the fault tree analysis is to help identify potential causes of system failures before the failures actually occur. It can also be used to evaluate the probability of the top event using analytical or statistical methods. These calculations involve system quantitative reliability and maintainability information, such as failure probability, failure rate and repair rate. The numerical output of an analysis is a probability of the occurrence of the top event. They are operating in the context of systems functioning and its surrounding environment that can lead to the undesired state of the system. The latter can be a complete failure, partial failure or a critical and unwanted state of the system.

2.1 Types of logic diagrams

2.1.1 Fault tree

FT has been emerged by Bell Telephone Laboratories in the early sixties; later many engineering disciplines adopted it, including aviation, medicine, nuclear

and safety. Fault tree analysis was one of the methods to assess risk and reliability used by the US aerospace and missile programs. In the Apollo project, the fault tree was used to calculate and to analyze the probability of successfully sending astronauts to the moon and returning them safely to the land. FT is a deductive top-down method that aims to compute the occurrence's probability (P) of the top event as function of basic events' probabilities (Xi). The latter represent likelihood of components' failures and/or occurrence of random incidents (i.e natural catastrophe or power outage). The conventional FT is still used in some applications even in the development of some other forms of it (i.e dynamic fault tree and fuzzy fault tree). Sometimes, it is useful to describe graphically the process sequence by a preliminary model. Then other formalisms take place to finish the modelling (i.e Bayesian networks or Markov chains).

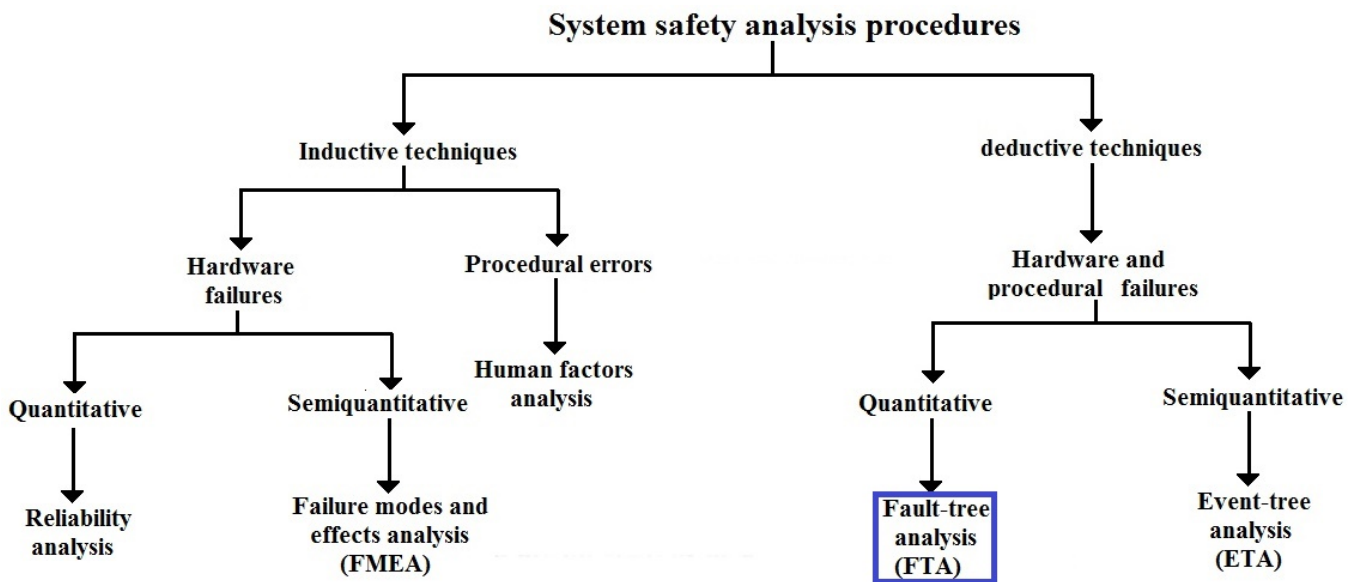


Figure 2.1 -System safety analysis procedure.

Fault tree construction:

To do a comprehensive FTA, follow these steps:

1. Define the fault condition, and write down the top level failure.
2. Using technical information and professional judgments, determine the possible reasons for the failure to occur. Remember, these are level two elements because they fall just below the top level failure in the tree.

3. Continue to break down each element with additional gates to lower levels. Consider the relationships between the elements to help you decide whether to use an "and" or an "or" logic gate.
4. Finalize and review the complete diagram. The chain can only be terminated in a basic fault: human, hardware or software.
5. If possible, evaluate the probability of occurrence for each of the lowest level elements and calculate the statistical probabilities from the bottom up.

Fault tree represents the hierarchical relationships among the events and the unwanted top event in a graphical way. These relationships are described using logic gates that can be:

- And gate: means that the failure of all components will lead to the activation of the next level gate.
- Or gate: means that the failure of one of the components will lead to the activation of the next level gate.

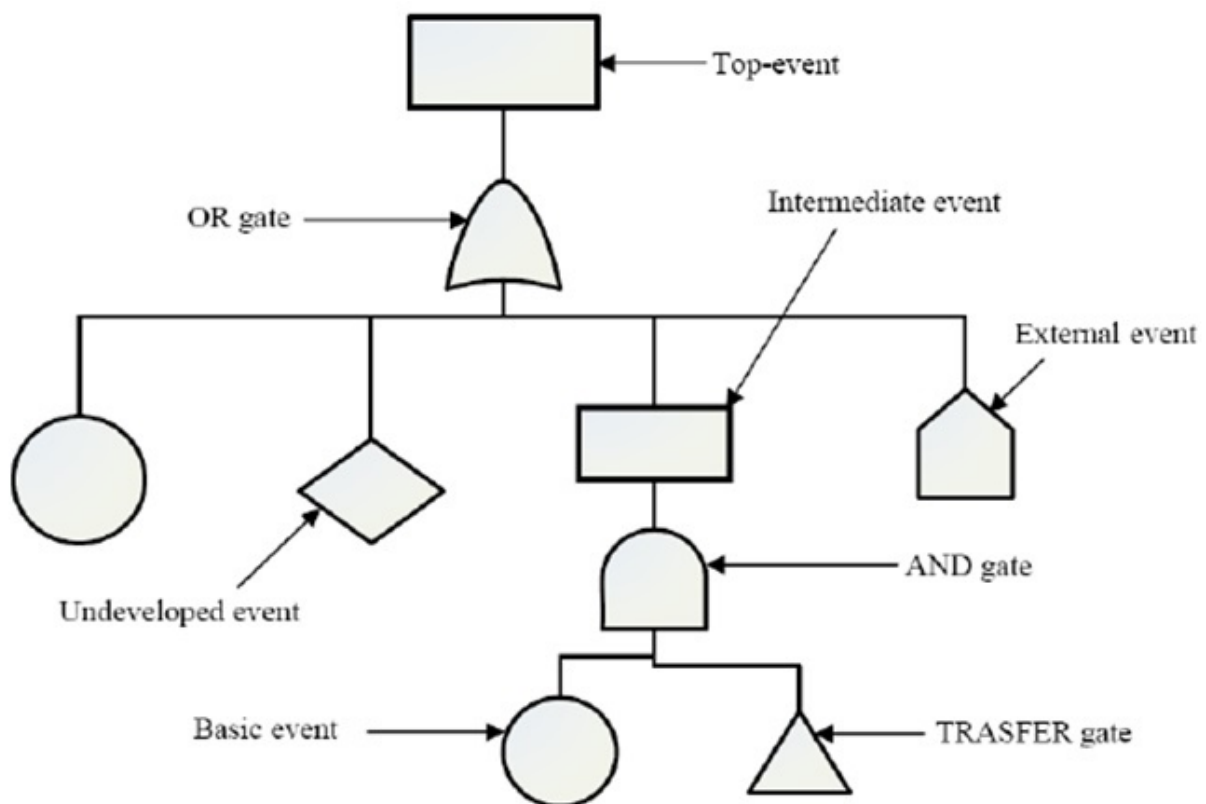


Figure 2.2 - Fault tree components.

Table 2.1 -The different kind of FT gates.

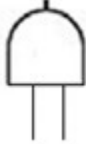

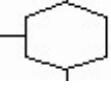
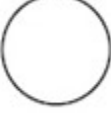



	AND GATE	The output (event) from this gate will occur only when all input occurs
	OR GATE	The output (event) from this gate will occur only when all input occurs
	INHIBITION GATE	The output (event) from this gate will occur only when doesn't input occurs

Table 2.2 - The different kind of event's presentation.

	Basic event	The lowest level of the FT, where no more details is given
	Undeveloped Event	An event that cannot be further developed due to lack of information
	Top/Intermediate Event	An output of a gate
	Transfer Gate	Transfer the connection from or to another fault tree

Depending on the fault tree is advanced, it can contain other gates:

- KoutofN gate: means that the failure of (K) components out of (N) which is the number of all the components, will lead to the activation of the next level gate.
- Inhibition gate: means that the failure of these components/occurrence of these events, will lead to a desactivation or inhibition of the next level gate.
- Transfer gate: means that this gate is transferring the connection from or to another fault tree.

In order to better understand the FTA concept, some definitions are provided below:

- Cut Set: A cut set is combinations of basic events; if all these basic events occur; the top event is guaranteed to occur.
- Minimal Cut Set: A minimal cut set is a special case of a cut set, where if one of basic event is removed from the set, the remaining events collectively are no longer a cut set. That's mean that all the basic events in this cut set are necessary to activate the next level gate.
- Path Set: A path set is a collection of basic events; if none of the events in the sets occur, the top event is guaranteed not to occur.
- Minimal Path Set: A minimal path set is a path set such that if any basic event is removed from the set, the remaining events collectively are no longer a path set.

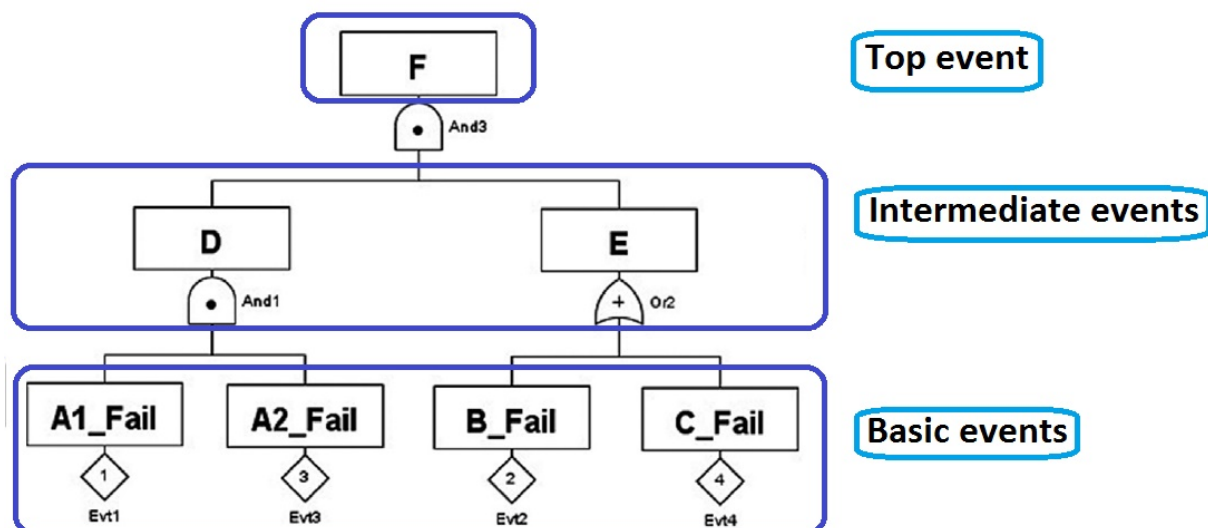


Figure 2.3 - Basic terminology for the fault tree.

The fault tree analysis (FTA) starts with identifying the top events then step by step reveals the basic or the root causes of top-events in deductive way. Two or more basic events are related by a logic gate (i.e “And” or “Or” gate) to form an intermediate event, as shown in the Figure 2.3. Then two or more intermediate events are related by a logic gate to form another intermediate event or the top event. In this

way the structure of the fault tree is built step by step. Other terminology can be used as follow:

- **Initiating event:** Any unwanted, unexpected or undesired event (e.g., system or equipment failure, human error or a process upset, toxic or flammable release).
- **Precursor events:** The events following the initiating event are termed as precursor events or sometimes termed only as the events for the event tree (e.g., ignition, explosion, release drifting).
- **Outcome events:** The possible effects, the scenarios or outcomes of an initiating event, are known as outcome events (e.g., fireball, vapor cloud, explosions).

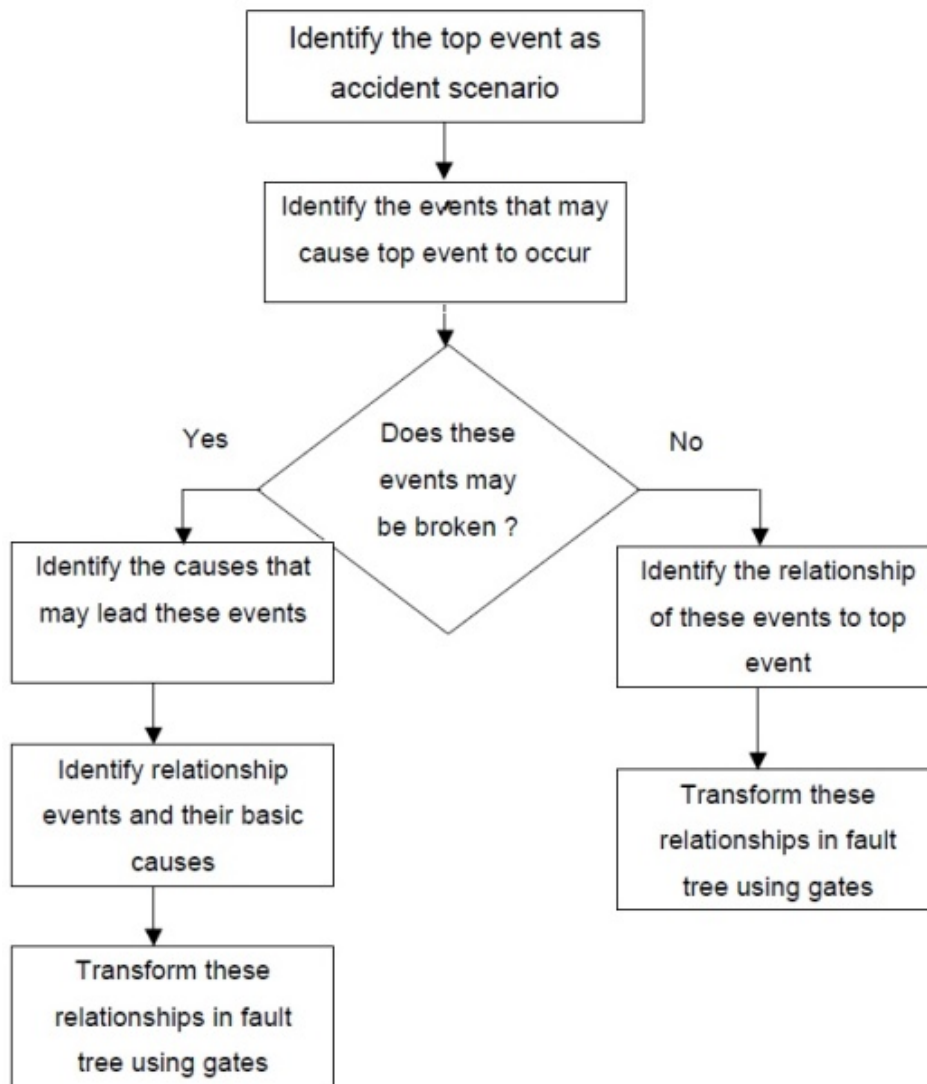


Figure 2.4 - The fault tree development

The development of the fault tree structure is following the algorithm shown in Figure 2.4 above. It consists of identifying the top event, which is the study subject. Then the direct events causing these events and going in details till the basic events that cannot be details more. Or for our study purpose, we are not interested to detail it. So it takes the shape of undeveloped event as shown in Table 2.2.

If the fault tree analysis is getting that importance, it is because of its double aspects, qualitative and quantitative, easy to implement and discuss (Talebberrouane and Lounis., 2016).

The qualitative aspect of the FTA is as follow:

- Describing the relationship using a logical structure.
- Identification of the system’s weakest links through the calculation of the cutsets and the minimum cutsets.
- Identification of the path sets and the minimal path sets.

Table 2.3 – Logic gates’ calculation formulas.

Gate	Input pairing	Output calculation
OR	P(A) “OR” P(B)	$P(A \cup B) = P(A) + P(B) - P(A)P(B)$ $= P(A) + P(B)$ [If P(A) and P(B) are small]
AND	P(A) “AND” P(B)	$P(A \cap B) = P(A)P(B)$

Table 2.4 – The probability rules.

<u>Commutative rule</u>	
$P_1 \cdot P_2 = P_2 \cdot P_1$	$P_1 + P_2 = P_2 + P_1$
<u>Associative rule</u>	
$P_1 \cdot (P_2 \cdot P_3) = (P_1 \cdot P_2) \cdot P_3$	$P_1 + (P_2 + P_3) = (P_1 + P_2) + P_3$
<u>Distributive rule</u>	
$P_1 \cdot (P_2 + P_3) = (P_1 \cdot P_2) + (P_1 \cdot P_3)$	$P_1 + (P_2 \cdot P_3) = (P_1 + P_2) \cdot (P_1 + P_3)$
<u>Idempotent rule</u>	
$P_1 \cdot P_1 = P_1$	$P_1 + P_1 = P_1$
<u>Rule of absorption</u>	
$P_1 \cdot (P_1 + P_2) = P_1$	$P_1 + (P_1 \cdot P_2) = P_1$

The quantification aspect of the FTA is as follow:

- The calculation of the probability of occurrence of an accident (top event) based on the failure probabilities of the basic events, through the logic gates.

- The calculation of the system's weakest links through the cutsets and the minimum cutsets.
- The evaluation of the common-mode failures.
- The calculation of the system's weakest links through the cutsets and the minimum cutsets.
- The importance factor estimation
- Calculation of the most probable sequence (MPS), which is correspond to the minimal cut set with the highest probability.

2.1.1.1 Procedure for top-down approach to identify the cutsets

The top-down approach to identify the cutsets is based on the unique identification of all gates and basic events. The procedure is executed in five steps:

- 1- Place the top gate in the first row of a matrix.
- 2- Replace all gates by basic events either using a or b.
- 3- Replace an "OR" gate by vertical arrangement.
- 4- Replace an "AND" gate by horizontal arrangement.
- 5- Delete all supersets (sets that contain another set as a subset.)

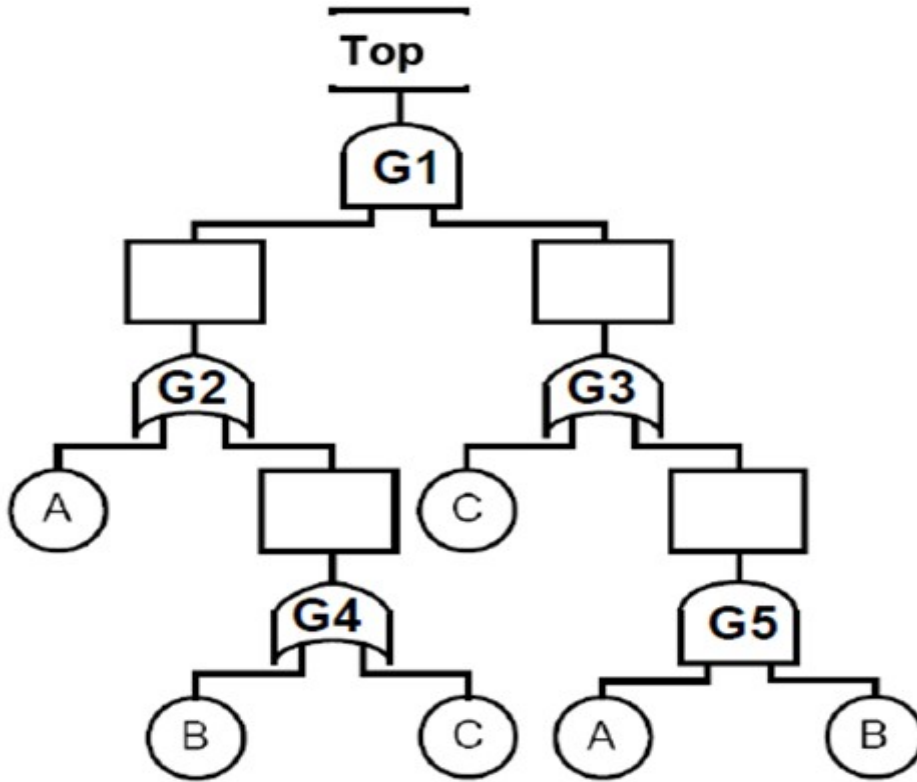


Figure 2.5 - A standard fault tree.

Table 2.5 – The top-down approach to identify the cutsets

G1	Top-gate
G2,G3	"AND" is replaced by vertical arrangement
A,G3 G4,G3	Gates are replaced with input events
A,C A,G5 B, G3 C, G3	"OR" is replaced by vertical arrangement
A,C A,B B,C B,G5 C,C C,E4	According to Boolean algebra $A \times A \equiv A$
A,C A,B B,C A,B C C,A,B	

The identified minimal cut sets for the tree are:

{C}, {A, B}, {A, C}, {B, C}

2.1.1.2 The procedure for bottom-up approach to identify the cutsets

This approach is similar, except it starts with gates containing only basic events. The procedure is executed in five steps:

1. Generate two columns, one is for gates and other for the other for cut sets.
2. Start with gates that have only basic events as inputs.
3. Generate cut sets for each of these gates in the table.
4. For "OR" gate If gate use union rule and represent the basic events separately. Example: A "OR" B= (A), (B).
5. For "AND" gate uses intersection rule and put the events into the same
Example: using the same fault on above for bottom-up approach

Table 2.6 – Results of the bottom-up approach

G5	(A,B)
G4	(B),(C)
G2	(A),(G4)
G2	(A),(B),(C)
G3	(C),(G5)
G3	(C),(A,B)
G1	(G2,G3)
G1	(A,C),(B,C),(C),(A,B),(A,B),(A,B,C)

The identified minimal cut sets for the tree are similar to the ones obtained by the previous method:

{C}, {A, B}, {A, C}, {B, C}

2.1.1.3 Importance factor estimation

- **Basic-events (Components) importance (BI_i):** It is calculated by “the sum of the probability of occurrence of all cutsets containing the basic-event (component)” divided by the total probability of occurrence for the system.

$$BI_i = \frac{\sum_{i \text{ in } j} C_j}{P_{Top}} \tag{2.1}$$

The symbol “Σ” in the equation denote a “sum of all those probability of cutsets containing basic-event i as one of its basic-events”.

- **Cutsets importance (CI_j):** It is the ratio of **cutsets characteristic** over the system characteristic.

$$CI_j = \frac{C_j}{P_{TOP}} \quad (2.2)$$

The classic fault tree, as a static modelling tool, represents the probabilities of the random events by constant values. This leads certainly to a misjudgment of top event probability. On the other hand, FT is based on basic events' independency, which is not suited for majority of complex systems where some elements' dynamic behaviours are significant factors (i.e automatic start and stop pumps and backup units) and/or interdependencies are strong or critical for the system analysis (i.e intrinsic dependency or cascading dependency). In these circumstances, the need for formalisms, able to handle the limitations of conventional FT, becomes evident. Extensive discussion on limitations of the FT is provided by (Siu, 1994).

2.1.2 Advance fault trees

In the past few years, FTs have experienced a lot of improvements to overcome their weaknesses (Baig et al., 2013). In the literature, some work has successfully used hybridized fault trees to assess, reliability, availability, maintainability and safety of complex systems (RAMS). Volkanovski (2009) successfully applied improved FTA using algorithms to assess power system reliability. In safety assessment, Khakzad (2013) used the bow-tie (BT) structure and mapped a Bayesian network based on it, while proposing a procedure for mapping and dealing with dependencies and data updating, with the help of BN properties. Other work dealt with the comparison of different techniques used in accident modelling contexts. Sunanda (2015) compared FT, FMEA and PNs for hazard analysis of a safety critical system, with a railroad crossing junction as a case study, and conclude that generalized stochastic Petri nets (GSPN) have the ability to identify the failure occurrences more specifically than the other formalisms. Nivolianitou (2004), compared FT, ET and PN for accident scenario analysis of an ammonia release from an ammonia storage plant and come out with a conclusion that PNs offer better time/duration depiction of an accident development, while FTs present better the primary events that may affect them.

Some advance Fault trees are presented below:

2.1.2.1 Dynamic fault tree

In process systems, usually the order in which the events occur affects the outcome modelling results. In these cases, the conventional fault tree cannot provide an accurate model for those systems. Dynamic fault tree, by introducing two special fault tree gates can make it easier to model those systems. These two special gates are part of the Dynamic Fault Tree (DFT) methodology that has been developed specifically for the purpose to overcome the order issue. A relevant example is the systems with back-up unit. Where, the failure of the primary unit will lead to the activation of the back-up unit. In this case the operational order is important for the system.

2.1.2.2 Fault tree driven Markov process

Fault Tree Driven Markov Processes (FTDMP) formalism is developed to enable the analysts to combine conventional fault trees and Markov models in a new way (Cacheux et al., 2013). Markov process, as a stochastic process time dependent, integrates the dynamism property in the static model of the conventional FT and makes it possible to model and study distinctive elements as the case of repairable components where the component passes by different phases (i.e operational, failed and under repair phase). Some applications of this formalism as the case (Talebberrouane et al., 2016) shows the modelling capacity improvement of the FT due to Markov process implementation. In FTDMP, each basic event is associated to a Markov process given the behaviour and phases during which the component is operational, failing, experiencing a diagnostic review or a repair and so on. It also provides information on component's availability in each phase of its life cycle. FTDMP and multi-phases Markov process approaches are described in annexes B4 and B5 of the IEC 61508-6 (2010). Cacheux (2013) assessed the availability using FTDMP formalism included in the software GRIF, without presenting the Markov models behind it. It was illustrated that a lack of relevant models usually leads to an overestimation of reliability performances. Srinivasa (2016) applied the FTDMP

method to estimate the probability of failure on demand (PFD) of the Indian tsunami early warning system then assesses and analyzes its reliability based on Safety integrity level (SIL) classification. (Signoret, 2007) explained the principal of FTDMP formalism and illustrated it by a multi-phases Markov model. For more details about the use of FTDMP method.

2.1.2.3 Fault tree coupled with Binary Decision Diagrams

Some works have implemented the exponential distribution to the basic events. Dutuit and Rauzy (1997) successfully used the exponential distribution on basic events coupled with binary decision diagrams (BDD) to perform the Monte-Carlo simulation and study the uncertainty propagation through the tree.

2.1.2.4 Dynamic fault tree coupled with Markov process

Bucci (2008) implemented Markov models in specific parts (sub-systems) of dynamic fault tree (DFT) and dynamic event tree (DET) to enhance their dynamic modelling capacities. The approach was illustrated by using a water level control system.

2.1.2.5 Boolean Logic Driven Markov Process (BLDMP)

Bouissou (2002) presented formalism similar to the main principle of FTDMP, called Boolean logic driven Markov process (BDMP). This formalism uses the concept of “triggered Markov process” time dependant commanding the state of targeted logic gates via dotted arrows on the FT. In this way, the FT becomes dynamic without the introduction of new gates as it is the case of the well-known dynamic FT.

2.1.3 Event tree

Event tree is an inductive procedure which maps the all possible outcomes resulting from an initiating event (any accidental release or occurrence), e.g. gas leakage, equipment failure or human error. It consist of the determination of the

probability of various outcomes (i.e final consequences) resulting from the initiating event.

2.1.3.1 The steps of ETA

The event tree analysis as a study is began by the identification of initiating event. After that, the identification of safety functions, that can be an automatic shutdown, alarms which alert the operator, or operator actions in response to alarms. The safety functions can have at least two states, usually, operational state and failure state. Depending on which state the safety barriers are, a diagram is traced to conduct at the end to the final consequences of the predefined initiating event.

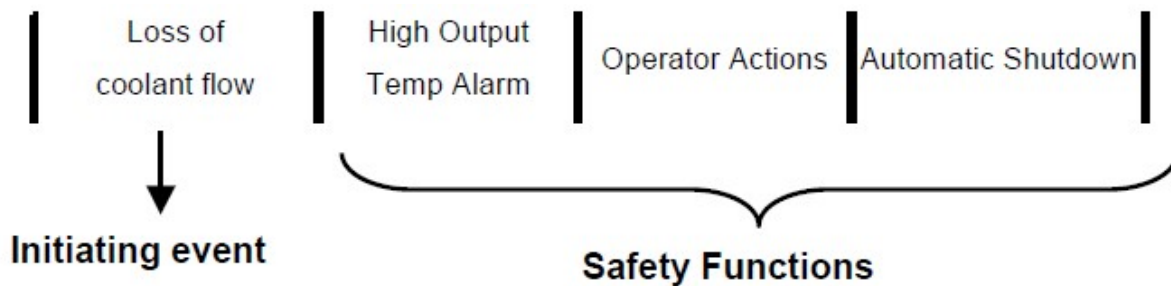


Figure. 2.6. Example of an initiating event and related safety functions.

2.14 Reliability Block Diagrams

Any reliability study is based on the knowledge of operational relationships of the various elements constituting a system. The reliability of a system cannot be improved or even evaluated unless there is a thorough understanding of how each of its elements function and how these functions affect system operation. The accurate representation of these relationships is an integral part of this understanding and is particularly important for meaningful predictions, apportionments and assessments. A Reliability Block Diagram (RBD) provides a method of representing this information in a form, which is easy to comprehend because it is simple and has visual impact.

It should be noted that a system or equipment might require more than one RBD to describe it. This is particularly true of equipment, which is capable of performing several functions, or experiences several different operating states during a deployment. An RBD may be required for each particular condition. In fact, the approach should be to produce a RBD for a function in a particular operating state, rather than for a piece of hardware.

2.1.4.1 Definition and basic concept

A Reliability Block Diagram (RBD) is a graphical representation of the components of the system and how they are reliability-wise related (Bistouni and Jahanshahi., 2014). The diagram represents the functioning state (i.e, success or failure or any other states) of the system in terms of the functioning states of its components. Thus, the reliability of the whole system is derived from knowledge of the reliability of its components (Bourouni., 2013).

The rational course of a RBD stems from an input node located at the left side of the diagram. The input node flows to arrangements of series or parallel blocks connected by arcs reflecting the relationships between different components concluding to the output node at the right side of the diagram. The RBD is a graph without circuit should only contain one input and one output node. Successful operational system requires at least one maintained path between the system input and the system output, otherwise it may fail. A RBD can always be constructed as connected groups of three types:

- Elements in series;
- Elements in active redundancy;
- Elements in standby redundancy.

a) A series connection: (joined by one continuous link from the Start Node to the End Node). The simplest form of a system for reliability analysis is one where the elements are connected in series. In this type of system, if one or more of the elements are down then the whole system is down. For example, consider the power train of a motor car, comprising engine (e), gearbox and drive links (g), and two

wheels (w1, w2). A failure of any element results in failure of the system. The RBD of the system is:

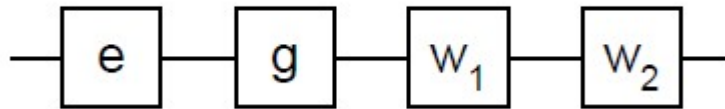


Figure. 2.7 Example of a series RBD

b) Elements in Redundancy:

There is redundancy in a system if not all of its constituent elements are required to be up for successful operation of the system. A ‘m/n redundant group’ is a group of n items where only (any) m of them has to be up for the group to be considered up. This chapter considers two forms of redundancy, namely active and standby redundancy

b.1) Active Redundancy:

A group of elements are said to be in active redundancy if all elements in the group are active when the system is operating, but it is not necessary for all elements to be up for the group to be up. Redundancy appears in an RBD as parallel routes. For example, consider the rear suspension of a lorry comprising four wheels on either side. Suppose the load can be supported by three out of four wheels on each side. Then the RBD for the off-side wheels is as shown in Fig. 2.7:

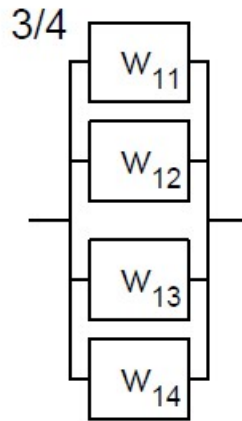


Figure. 2.8 Example of RBD for Active Redundancy

For all eight wheels considered as a system the RBD is a series combination of active redundancy groups, as shown in Figure. 2.9:

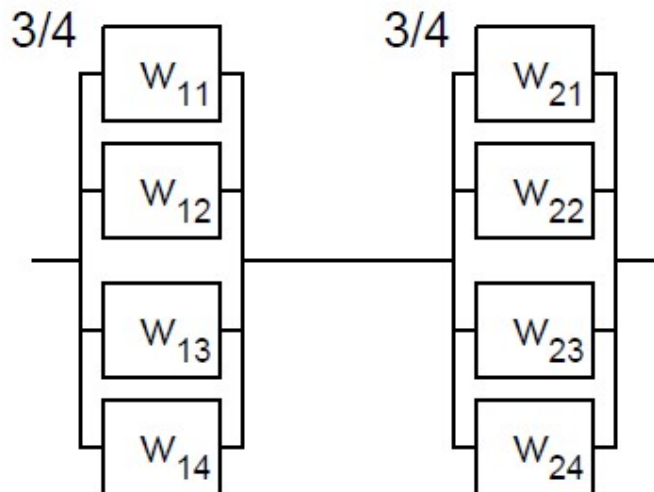


Figure. 2.9 Example of RBD for a Series Combination of Active Redundancy Groups (series-parallel).

b.2) Standby Redundancy:

Elements are said to be in an ‘m/n standby redundant group’ when only m of the elements are required to be in an active state and the remainder are in a passive state. When an active element fails then one of the passive elements is switched on in its

place. The failure time distribution of the elements depend on whether they are in an active or passive state (the failure rate of an element in an active state is generally much larger than its failure rate when it is in a passive state). An example of a standby redundancy group is a car with a spare wheel (assuming that the car with a burst tyre is not regarded as a system failure when there is a working spare). The RBD of this system is shown in Figure. 2.10.

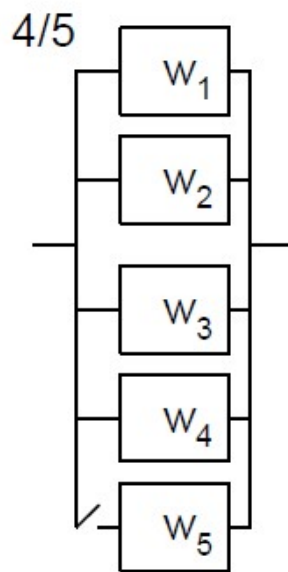


Figure. 2.10 Example of RBD for Standby Redundancy.

An important feature of most standby redundancy groups is that failures of elements in the passive state will not be detected until the passive element is required to replace a failed active element. Thus, even elements with a low failure rate in the passive state can have a critical effect on system reliability unless the 'spare' is regularly and comprehensively tested. In addition, if an automatic switching mechanism is used to bring in the passive elements, the mechanism itself may have its own failure time distribution.

2.1.4.2 Construction of a reliability block diagram

a) Method

A system can have a single function, such as in the examples described above, it is generally a straightforward matter to construct the system RBD. Normally such systems will comprise a group of elements in series or, at the most, a number of groups with redundancy themselves connected in series, (e.g. Figure 3). However, where a system has to perform more than one function or where the same function may be performed by more than one set of elements, the construction of the RBD may become much more complex. In these situations, it is advisable to follow a set procedure when drawing the RBD.

- The first step is to define the functions that the system is to perform, and the operating states (e.g. standby, full power, etc.)
- The next step is to decide which of these functions is the minimum required for successful operation of the system. If it is decided that all functions are required, then the functions should be represented as shown in Figure 4.



Figure. 2.11. Representation of Series Function with n elements.

If any one of these functions is sufficient for the operation of the system, then the system should be represented as shown in Figure. 2.12.

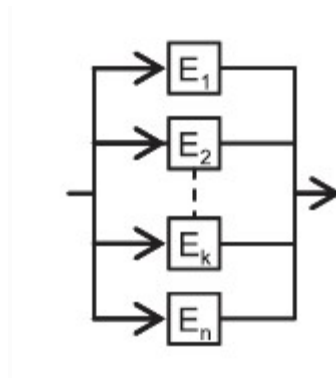


Figure. 2.12 Representation of Redundant Functions with n elements.

- Intermediate configurations are also possible of course. When one function is the prime requirement and any one of the other functions were sufficient for system operation, then the initial RBD would be as shown in Figure. 2.13. The components in an active redundancy might be connected in a parallel structure Figure 2, or a combination of series and parallel structures as shown in Figure3 and figure 8.

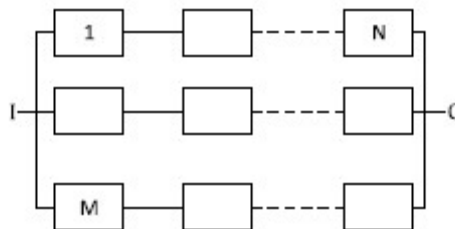


Figure. 2.13. Parallel combination of active redundancy groups (parallel-series).

- The next step is to associate with each function those elements that are required to perform the function. It may be that there are some elements which are common to all functions and they should be separated out first.

2.1.4.3 RBD simplification

Not all the systems are straightforward, they can be more complicated particularly if some elements are required for more than one function but not all. In these cases, a rigorous procedure based on a Boolean algebra should be followed when constructing RBDs.

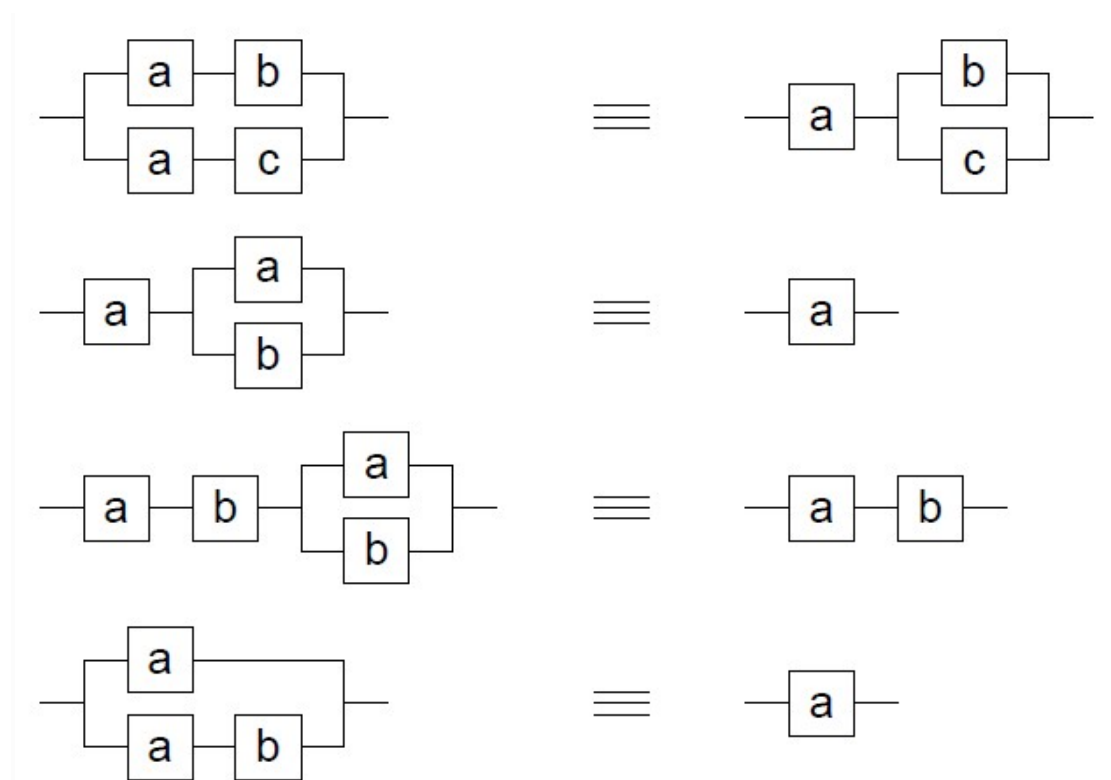


Figure 2.14. Equivalent structures in RBD.

2.4 Conclusion

The applications of logical diagrams as fault trees and event trees in the safety and risk assessment studies show a good capabilities to provide a good qualitative results as a graphical structure describing the relationship between the system's components. And the second most important aspect is the identification of the most probable sequence (MPS). Identifying this sequence is useful to make an improvement to the system based on systematic and comparative analysis. On the other hand some modelling performances are still need to be improved as the

interdependency and the time dependency aspect. These two criteria that are usually an integrated part in failure mechanisms of the complex systems make the challenge of the logical diagrams to be used with large confidence and accuracy as it required in such studies. However, the absence of reliable tools for safety analysis are due to the fact that some methods are based more on the descriptive aspect rather than the mathematical and the computerized aspects and the way of dealing with the uncertainty and the complexity of data. In fact, the conventional risk analysis techniques such as, Failure Mode Effects Analysis (FMEA), fault tree analysis (FTA) (IEC 61025., 2006), the event tree analysis (ETA) (IEC 62502., 2010) and reliability block diagrams (RBD) (IEC 61078., 2006) are dissociate from each other, which has bad impact on the risk assessment process of the global system. Another case of dissociation exists between the qualitative and the quantitative methods; where the industrialist tries to avoid the subjective assessment and prefers the risk matrix and other kind of quantification charts.

References

- Baig, A.A., Ruzli, R., Buang, A.B., 2013. Reliability analysis using fault tree analysis: a review. *Int. J. Chem. Eng. Appl.* 4, 169e173.
<http://dx.doi.org/10.7763/IJCEA.2013.V4.287>.
- Bistouni, F. and Jahanshahi, M., 2014. Analyzing the reliability of shuffle-exchange networks using reliability block diagrams. *Reliability Engineering & System Safety*, 132, pp.97-106.
- Bouissou, M., June 2002. Boolean logic driven Markov processes: a powerful new formalism for specifying and solving very large Markov models. *PSAM* 6, 8.
[http://dx.doi.org/10.1016/S0951-8320\(03\)00143-1](http://dx.doi.org/10.1016/S0951-8320(03)00143-1).
- Bourouni, K., 2013. Availability assessment of a reverse osmosis plant: comparison between reliability block diagram and fault tree analysis methods. *Desalination*, 313, pp.66-76.
- Bucci, P., Kirschenbaum, J., Mangan, L.A., Aldemir, T., Smith, C., Wood, T., 2008. Construction of event-tree/fault-tree models from a Markov approach to dynamic system reliability. *Reliab. Eng. Syst. Saf.* 93, 1616e1627.
<http://dx.doi.org/10.1016/j.ress.2008.01.008>.
- Cacheux, P.J., Collas, S., Dutuit, Y., Folleau, C., Signoret, J.P., Thomas, P., 2013. Assessment of the expected number and frequency of failures of periodically tested systems. *Reliab. Eng. Syst. Saf.* 118, 61e70.
<http://dx.doi.org/10.1016/j.ress.2013.04.014>.
- Dutuit, Y., Rauzy, A., 1997. Monte-Carlo simulation to propagate uncertainties in fault trees encoded by means of binary decision diagrams. In: 1st Int. Conf. Math. Methods Reliab. MMR'97, pp. 1-8.
- IEC 61025., Fault Tree Analysis (FTA). Technical report. International Electrotechnical Commission; 2006.

- IEC 61508-6, 2010. Functional Safety of Electrical/electronic/programmable Electronic Safety Related Systems. International Electrotechnical Commission, Switzerland.
- IEC 62502., Analysis techniques for dependability — event tree analysis. Technical report. International Electrotechnical Commission; 2010.
- IEC 61078., Analysis techniques for dependability — Reliability block diagram and Boolean methods. International Electrotechnical Commission; 2006.
- Khakzad, N., Khan, F., Amyotte, P., 2013. Dynamic safety analysis of process systems by mapping bow-tie into Bayesian network. *Process Saf. Environ. Prot* 91, 46-53. <http://dx.doi.org/10.1016/j.psep.2012.01.005>.
- Nivolianitou, Z.S., Leopoulos, V.N., Konstantinidou, M., 2004. Comparison of techniques for accident scenario analysis in hazardous systems. *J. Loss Prev. Process Ind* 17, 467e475. <http://dx.doi.org/10.1016/j.jlp.2004.08.001>.
- Signoret, J.-P., 2007. High-integrity protection systems (HIPS): methods and tools for efficient safety integrity levels analysis and calculations. In: *Proc. Offshore Technol. Conf*, pp. 1e6. <http://dx.doi.org/10.2118/117173-ms>.
- Siu, N.O., 1994. Dynamic approaches e issues and methods: an overview. In: Aldemir, T., Siu, N.O., Mosleh, A., Cacciabue, P.C., Goktepe, B.G. (Eds.), *Reliability and Safety Assessment of Dynamic Process Systems*. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 3-7. http://dx.doi.org/10.1007/978-3-662-03041-7_1.
- Srinivasa Kumar, T., Venkatesan, R., Vedachalam, N., Padmanabham, J., Sundar, R., 2016. Assessment of the reliability of the Indian Tsunami early warning system. *Mar. Technol. S. J.* 50 (3), 92-108.
- Stamatelatos, M., Vesely, W., 2002. *Fault Tree Handbook with Aerospace Applications*. NASA Office of Safety and Mission Assurance. Washington, DC.
- Talebberrouane, M., Khan, F., Lounis, Z., 2016. Availability analysis of safety critical systems using advanced fault tree and stochastic Petri net formalisms. *Journal of Loss Prevention in the Process Industries* 44: 193-203. <http://dx.doi.org/10.1016/j.jlp.2016.09.007>

Taleb-berrouane, M., Lounis, Z., 2016. Safety assessment of flare system by fault tree analysis. *Journal of Chemical Technology and Metallurgy*. 51-2: 229-234.

Volkanovski, A., Cepin, M., Mavko, B., 2009. Application of the fault tree analysis for assessment of power system reliability. *Reliab. Eng. Syst. Saf* 94, 1116e1127. <http://dx.doi.org/10.1016/j.res.2009.01.004>.

Chapter 3

Risk Assessment of Gas Flare Systems by Fault Tree Analysis “LNG Flares”

3.1 Abstract

Flaring is a combustion process of waste gases from the oil and gas industry. The escapement of these gases from the flare stack without being burned is known as Flameout. These released gases can present human and environment toxicity, it can also lead to a vapor cloud explosion (V.C.E), if the conditions are united. Flares flameouts have not received significant attention compared to other types of flare incidents, this is probably due to the fact that they may usually pass unnoticed if they are detected and successfully reignited in the early hours. Flameout event can occur by environmental, equipment and human factors. In this work we define some performance indicators extrapolated from a prepared fault tree. These indicators will be subsequently assessed through probabilistic methods in order to evaluate our system safety. An investigation about this flare incident has been done in order to better understand its occurrence mechanisms.

3.2 Introduction

Flare systems in oil and gas plants play critical roles in the safe operation of plants. Flare systems are designed to dispose of waste gases and discharged liquids from process units safely. It is generally used to handle materials vented during normal operations, start-up, and emergency conditions. There are three main kinds of flare systems in oil and gas industry: elevated flares, ground flares and low pressure flares. Elevated flares are used as normal feature of a refinery or a petrochemical plant and are handled in both normal and emergency circumstances (Zadakbar et al., 2011; 2015).

The hazards associated with flare systems are very various. Among most frequently met, we will quote: embrittlement or corrosion due to low temperature causing failure of the collection system pipe work in the flare system, explosion in the flare system, heat radiation, liquid carryover from the flare, flameout (emission of toxic materials from the flare).

In the context of safety and environment preserving about flares systems, some authors have investigated the flaring reduction (Anejionu et al., 2015) or recovering (Fisher

and Brennan., 2002; Abdulrahman et al., 2015). In this paper we focus on flare hazards, exactly the flare flameout hazard conditions using Fault tree analysis.

Fault tree analysis has been widely used to calculate reliability of the complex system. It is a logical and diagrammatic approach for evaluating the possibility of an accident resulting from sequences and combinations of failure events (Yuhua and Datao., 2005).

In literature, limited works have been done on the flare flameout, the research works of Zadakbar et al., (2011) were focused on the consequences of flare flame-out on environmental and humans.

The paper is organized as follows: In section 2, we definite our case study and we give descriptive figure of the system. Section 3 introduces some formal definitions of fault tree analysis and shows the developed fault trees with the failure rate of the elementary events. Section 4 presents the obtained results. Finally, we conclude our work and discuss some future research.

3.3 Experimental

3.3.1 Case study

The case study is taken from a LNG complex, the GL1/Z-SONATRACH – Algeria, complex that contains three flare systems. The Cold flare system for gases colder than 0° C, the Hot flare for gases warmer than 0° C, and the Tank flare system for excess vapors from the LNG storage tanks. Hydrocarbon gases entering the Hot/Cold flare systems in each Unit flow to a main header, into knockout drums where any hydrocarbon liquids are removed and sent to the flare stack to be burned at a distance from the complex (SONATRACH., 2010).

According to the feedback experiences on (SONATRACH., 1999), we noted that the cold flare is the most exposed to the risk of flameout, it is for that we will be directed our research on this flare. A descriptive figure of steam assisted flare system is given below.

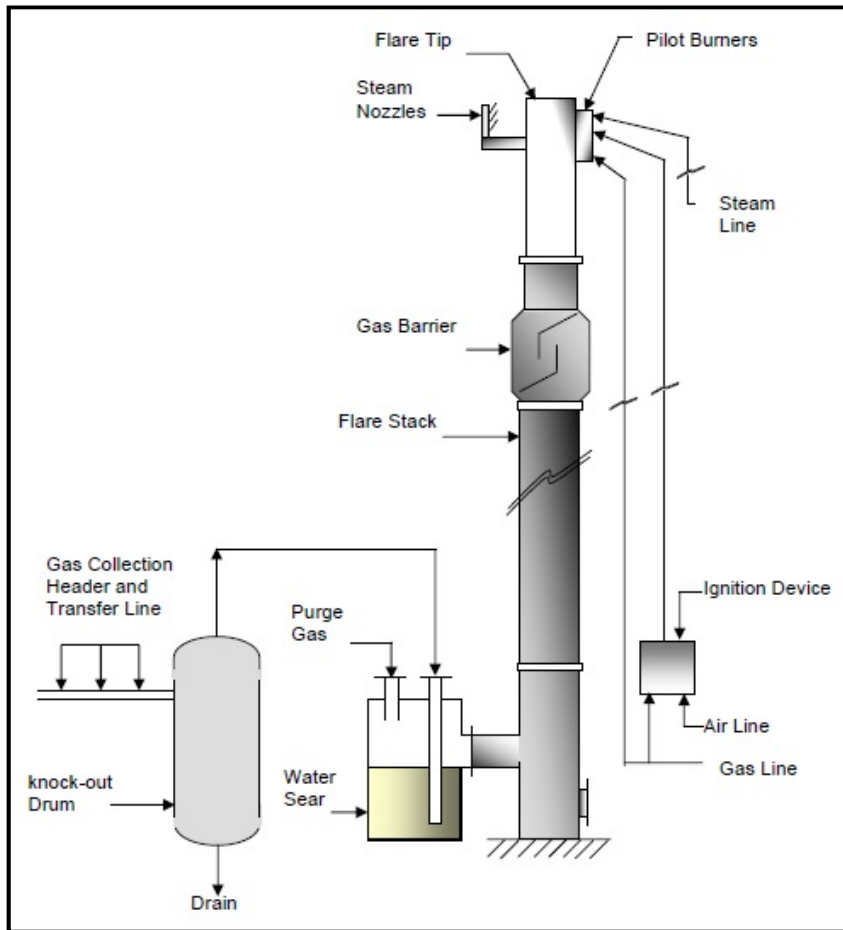


Figure 3.1 - Steam assisted flare system (Ling., 2007).

3.3.2 Analysis of flameout incident

In order to identify the sequences of the probable causes of this incident, a fault tree analysis was made from the experience feedback of the complex (GL1 / Z - Sonatrach) (SONATRACH., 1999), and other complex (SONATRACH., 2013), as well as technical knowledge about the flares systems.

The analysis by fault tree known in the literature as "FTA" for (fault tree analysis) is a deductive method, starting from elementary events leading to a undesirable event (top event) the latter is obtained by a hazard study for a given system. FTA is usually used to predict reliability of complex systems in many engineering fields, such as nuclear, space

and aeronautics, Oil, gas and petrochemical industry... etc. In conventional fault tree analysis, the failure probabilities of components were considered as exact values. However, it is often difficult to estimate precise failure probability of the components due to insufficient data or vague characteristic of the events.

Definition of events:

- a) The principal event (Flare flameout): is the undesirable event that we are studying.
- b) The intermediates events (flame detachment, defect on ignition pilot system...), Those are causes for other events. For example it is the combination of intermediate events that led to the feared event.
- c) The elementary events: they are corresponding events at the most detailed level of analysis of the system.

Table 3.1 Occurrences probabilities (λ) of elementary events.

Elementary event	Occurrence probability (λ)
Failure on ignition device	1.14×10^{-4}
Ignition pipes clogged	5.7×10^{-5}
Mechanical failure	1.38×10^{-6}
Instrumentation failure	0.1×10^{-6}
Manual valve blocked close*	0.29×10^{-6}
Operator fault	2.85×10^{-5}
Condensate presence in the FG	1.14×10^{-4}
Pipe not drained	3.8×10^{-5}
Nitrogen valve opened	3.8×10^{-5}
FG supply interrupted at source	3.8×10^{-5}
Isolation of the FG line for works	1.14×10^{-4}
Wind Speed > 120 km / h	5.7×10^{-5}
Pumping phenomenon	2.28×10^{-4}
Relief PCVs closed	1×10^{-3}
Switching to another flare	5.7×10^{-5}

FG: Fuel gas.

PCVs: Pressure control valves.

*: Probability from OREDA database (OREDA., 2002).

- The others probabilities are made by a voting system from a group of qualified plant staff (production – technical – safety) taking into account information feedbacks and some statistics.

Figures 3.2, 3.3, 3.4, depict the fault trees of our system.

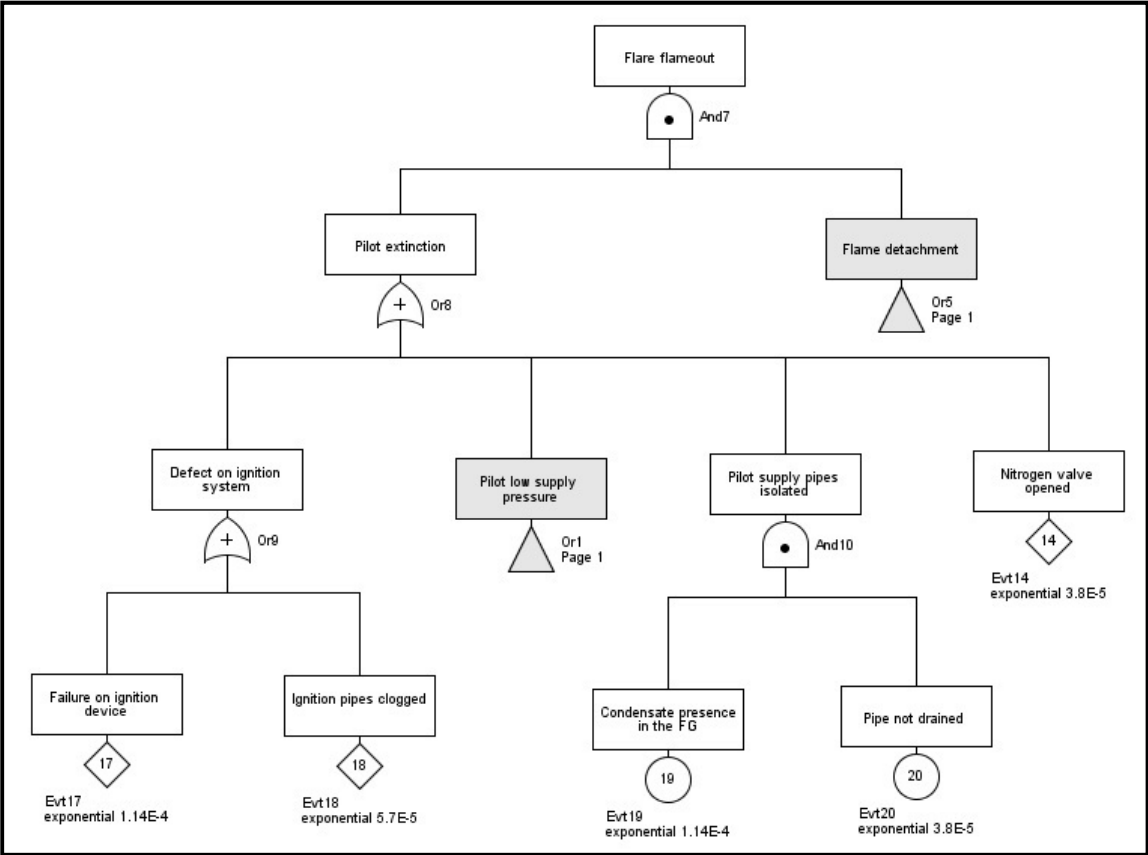


Figure 3.2 - Flameout fault tree.

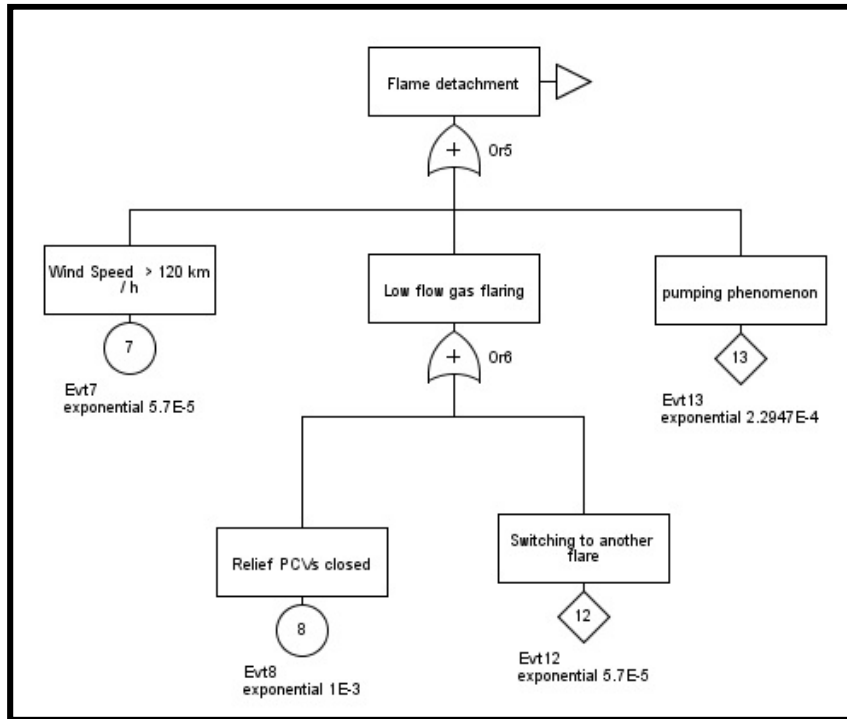


Figure 3.3 - Flame detachment fault tree.

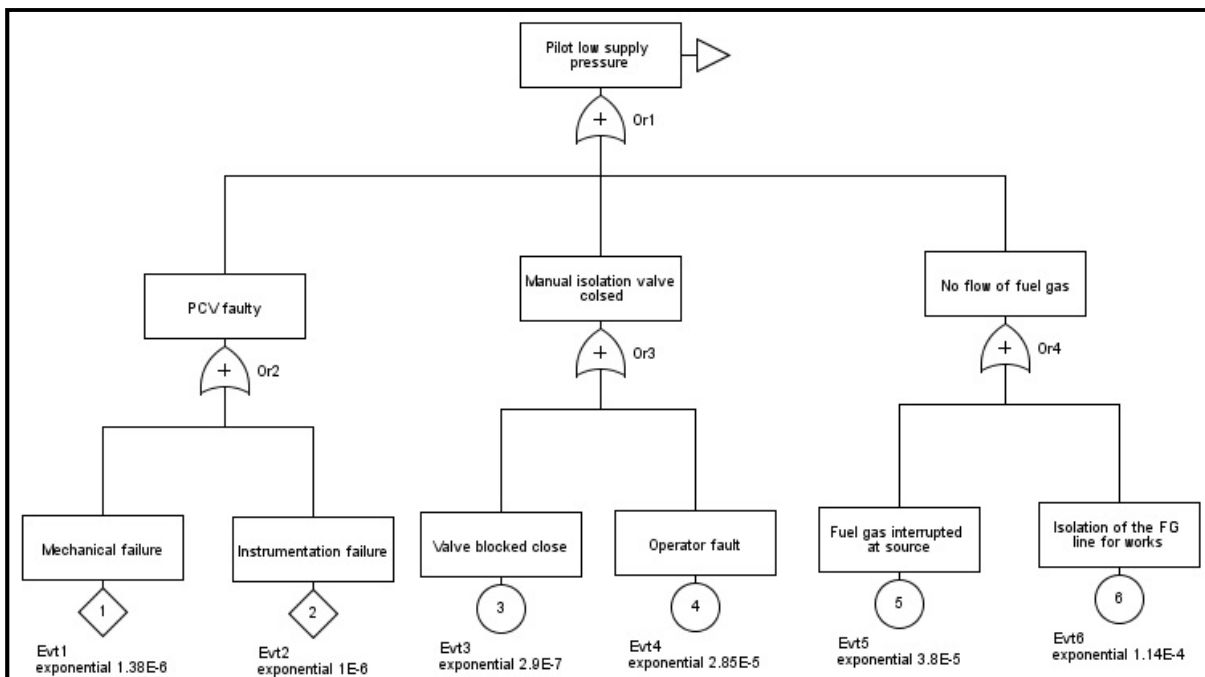


Figure 3.4 - Pilot pressure fault tree.

3.4 Results and discussion

The Fault Tree module of GRIF (graphical interface for reliability) software developed by SATODEF & TOTAL (GRIF-Workshop., 2015) was used to calculate the probabilities our system from the elementary failure rates given in (Table I).

The probabilities (λ_{eq}) generated are the following:

- F1: Probability of flame detachment.
- F2: Probability of low supply pressure of pilot.
- F3: Probability of flare flameout.

The performances set for our system are:

- P1: the ability to avoid flame detachment.
- P2: the ability to avoid pilot low supply pressure.
- P3: the ability to avoid a flameout.

The failure rates (F1, F2, and F3) are considered to be unreliability so:

$$P = 1 - F \quad (3.1)$$

Table 3.2 Results of the FTA study.

Event	F	P
Flame detachment	$1.34 \cdot 10^{-3}$	99.87%
Low SP* of pilot	$1.83 \cdot 10^{-4}$	99.98%
Flare flameout	$4.28 \cdot 10^{-4}$	99.96%

*: Supply pressure.

The calculations show that the performances indicators of our system can reach more than 99%. This is due to implementation of the adequate protection and prevention barriers set up in our case study.

3.5 Conclusions

Even though flare flameout is not a frequent risk like others flare incidents (explosion – heat radiation - liquid carryover from the flare), but it can be very dangerous because of

the further accidents that it can be generated if it remain sufficient duration with risk of toxic emission or ignition and causes vapor cloud explosion. By evaluating the performances indicators of a LNG flare, we can conclude that the safety level of our system for the flameout incident is acceptable.

We propose this developed method for safety assessment of systems for a specific incident which difficult to be predicted. Although a significant research effort has been made to improve the knowledge on this phenomenon, and as future work we will use an advanced methods to evaluate the performances of complex system in the field of safety.

REFERENCES

- Zadakbar, O., Abbassi, R., Khan, F., Karimpour, F., Golshani, M. and Vatani, A., 2011. Risk Analysis of Flare Flame-out Condition in a Gas Process Facility, *Oil Gas Sci. Technol. Rev. IFP Energies nouvelles*, 66-3, pp 521-530.
- Zadakbar, O., Khan, F., and Imtiaz, S., 2015. Development of Economic Consequence Methodology for Process Risk Analysis, *Society for Risk Analysis*, 35-4, 713-731.
- Anejionu, O. C. D., Blackburn, G. A., Whyatt, J. D., 2015. Detecting gas flares and estimating flaring volumes at individual flow stations using MODIS data, *Remote Sensing of Environment*, 158, 81–94.
- Fisher, P. W., and Brennan, D., 2002. Minimize flaring with gas flare recovery, *Hydrocarbon process*, 83-85.
- Abdulrahman, A. O., Huisingh, D., Hafkamp, W., Cleaner, J., *Prod*, 98, July 2015, 116–122.
- Yuhua, D., Datao, Y., 2005. Estimation of failure probability of oil and gas transmission pipelines by fuzzy fault tree analysis, *J. Loss Prev. Process Ind.*, 18-2, 83–88.
- SONATRACH GL1/Z Complex, Sonatrach Process Operating Manual « Flare Systems », Section 11.4, 2010.
- SONATRACH - GL1/Z Complex, Internal Communication -Incident Report of cold flare, 19 Sept. 1999, (French).
- SONATRACH - GL1/Z Complex, Internal Communication -Incident Report of cold flare, 29 Nov. 2000, (French).
- SONATRACH - GL1/Z Complex, Internal Communication -Incident Report of cold flare, 01 Oct. 1999, (French).
- Ling, A. L., 2007. flare selection and sizing (engineering design guideline), KLM technology group, Malaysia.
- SONATRACH - GP2/Z Complex, Extinction Report of HP flare, 17 March 2013, (French).
- OREDA Offshore Reliability –data handbook 4th edition, DNV, 2002, 567-573.
- GRIF-Workshop, <http://grif-workshop.fr/tag/total>, page accessed (20. 02. 2015).

Chapter 4

Risk Based Modelling Using Advanced techniques

Part 1: Bayesian Networks

4.0 Introduction

Many potential accidents scenarios either have not been noticed or ignored in current conventional safety and risk analysis, because of the static nature and other limitations of the methods used to capture these potential sequences (i.e fault trees and events trees). To overcome the independency limitation of the FT and ET, many researchers prefer to use the Bayesian networks (BN) as a good alternative of those conventional methods. Bayesian networks (Weber et al., 2012), as modelling tools, have been more and more discussed topic during the last years. They are widely used in safety analysis as a powerful data mining technique for handling uncertainty and incomplete data information. Bayesian Networks appear to be a practical solution to model systems with strong interdependency because they perform the factorization of variables joint distribution based on the conditional dependencies. The main objective of BN is to compute the distribution probabilities in a set of variables according to the observation and belief (i.e evidence of a state) of some variables and the prior knowledge of the others. The principles of this modeling tool are explained in Jensen (1996) and Pearl (1988).

4.1 Definitions and basic concept

Bayesian Networks also called belief networks and Bayesian belief networks. From a graphical point of view, Bayesian networks are directed acyclic graphs (DAGs). It consists of nodes interconnected with arcs. Nodes represent events, safety barriers and/or consequences, and arcs represent the causal relationships between them. If the event (a) cause (b), the connection will be from (a) to (b), the node (a) is called the parent node and node (b) is the child node. If node (b) has a child node called (c), then the nodes (b) and (c) are the descendants of (a).

From a mathematical point of view, the Bayesian networks are one of the compact representations of the joint probability table. Where, other formalisms provide different kinds of the joint probability table representations. From a knowledge engineering point of view, a Bayesian network is a type of graphical model. The structure of the network is formulated in a unidirectional graphical communication language based on the probability and the causality. Furthermore, the graphical specification also specifies the requirements for the quantitative part of the model (the conditional probabilities).

4.1.1 The conditional probability

The concept of conditional probability is the statement of the probability of an event given conditions on other known events. For example, a statement such as “the probability of the die turning up 6 is 1/6” usually has the unsaid prerequisite that it is a fair die, or rather, as long as I know nothing further, I assume it to be a fair die. This means that the statement should be “given that it is a fair die, the probability” (Nielsen and Jensen., 2009). That will conduct us to the perception that, without predefined assumptions or conditions, we cannot predict any probability. So, all the probabilities are actually conditional probabilities. The difference between them is nothing but the level or the conditions. The general statement of the conditional probability is given by the following expression:

“Given the event B, the probability of the event A is p ”

Where, B can be a qualitative or Boolean expression (true or false) or a quantitative representation. The notation of this statement is $P(A|B) = p$. Even with this statement the conditional probability is completely described. And it state that whenever B is true or satisfied, then the probability of A is p without considering any predefined conditions. In this way, the complete statement is that “if B is true, and everything else is irrelevant for A or considered irrelevant by the previous assumptions, then the probability of A is p ”. Otherwise, we take in consideration other factors before give the statement of the probability. For example, $P(A|B,C,D) = p$. In this case, the factors C and D are relevant for A. Using the terminology of the Bayesian Networks, we will say. The state of A is depending on the state of B, C and D.

4.1.2 The Bayes' rule

$$P(A|B) = \frac{P(B|A) \times P(A)}{P(B)} \quad (1)$$

$P(A|B)$: the conditional probability for A given B

- ❖ The Bayes' rule allows an information's updating, so we can call $P(A)$ the prior probability of A, $P(A|B)$ is the posterior probability of A given B and the probability $P(B|A)$, the likelihood of A given B.
- ❖ Using the conditional independence assumptions of BNs, the joint probability distribution of a set of random variables $\{X_1, X_2, X_3, \dots, X_{(n-1)}, X_n\}$, can be determined using a chain rule as:

$$P(X_1, X_2, X_3, \dots, X_{n-1}, X_n) = \prod_{i=1}^n P(X_i | Parents(X_i)) \quad (2)$$

- ❖ For two events A and B, with $P(B) > 0$, the conditional probability for A given B is :

$$P(A|B) = \frac{P(A, B)}{P(B)} \quad (3)$$

So: $P(A, B) = P(A | B) \times P(B)$

N.B: The notation $P(A, B)$ is the same as $P(A \cap B)$ and it represent the joint probability of the events A and B that means the probability of occurrence of the both events.

If we have another event (c), we will get the conditional probability generalizes as:

$$P(A|B, C) = P(A, B, C) \times P(B, C)$$

If the variable B has states (b_1, b_2, \dots, b_m) , then $P(A|B)$ contains $n \times m$ conditional probabilities $P(a_i | b_j)$ that specify the probability of seeing a_i given b_j . That is, the conditional probability for a variable given another variable is a set of probabilities (usually organized in an $n \times m$ table) with one probability for each configuration of the states of the variables involved. Moreover, since $P(A|B)$ specifies a probability distribution for each event $B = b_j$, we know from Axiom 1 that the probabilities over A should sum to 1 for each state of B:

$$\sum_{i=1}^n P(A = a_i | B = b_j) = 1 \text{ for each } b_j \quad (4)$$

Table 4.1 Probabilities tables in BN modelling.

Table	Corresponding nodes	Symbol
marginal probability table (MPT)	Nodes doesn't have parents	P(A)
Conditional probability table (CPT)	Nodes have parents	P(A Pai)
Joint probability table (JPT)	All Nodes	P(A,B)

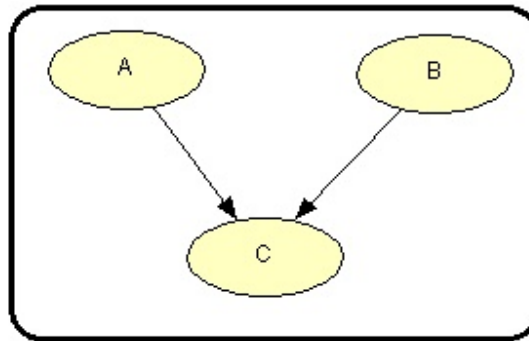


Figure 4.1 - Simple example of a Bayesian network.

In the Figure 3.1, the event or variable A is depending on the events or variables B and C. That means that, we cannot give any probability of the variable C without considering the variables B and C. In other words, the conditional probability or the conditional dependency from B and C to A. Using the Bayes theorem, we can write:

$$P(A|D) = \frac{P(A, D)}{P(D)} = \frac{P(D|A) \times P(A)}{P(D)} \quad (5)$$

$$P(B|D) = \frac{P(B, D)}{P(D)} = \frac{P(D|B) \times P(B)}{P(D)} \quad (6)$$

Where,

$$P(C) = \sum_{i=1}^n P(C, A_i, B_i) \quad (7)$$

If the variable A has two states, state A and Ac. And B has two states B and Bc, then:

$$P(C) = P(C, A, B) + P(C, A_c, B) + P(C, A, B_c) + P(C, A_c, B_c) \quad (8)$$

And

$$P(D|A) = [P(D,A,B) + P(D,A,Bc)] / P(A) \quad (9)$$

$$P(D|B) = [P(D,A,B) + P(D,Ac,B)] / P(B) \quad (10)$$

The nodes A and B are independents, so:

$$P(D,A,B) = P(D|A,B) \times P(A) \times P(B) \quad (11)$$

$$P(D,Ac,B) = P(D|Ac,B) \times P(Ac) \times P(B) \quad (12)$$

$$P(D,A,Bc) = P(D|A,Bc) \times P(A) \times P(Bc) \quad (13)$$

The BN's representation:

- The BN's qualitative representation is given by a representation of the nodes interconnected by their corresponding arcs.
- The BN's quantitative representation is given by the MPTs and CPTs and JPTs.

4.1.3 The conditional independence

We said that event A and event B are independent, if any change happen on the event B will not influence the event A.

Theorem of independence: A and B are independents if:

$$P(A|B) = P(A) \quad \text{Then} \quad P(B|A) = P(B), \text{ a symmetric relationship.}$$

$$\text{Also we can write: } P(A,B) = P(A|B) \cdot P(B|A) = P(A) \cdot P(B)$$

The events A and B are conditionally independent given the event C, so:

$$P(A|B,C) = P(A|C),$$

$$\text{And: } P(A,B|C) = P(A|C) \cdot P(B|C),$$

- ❖ For a conditional probability table (CPT), $P(A|B)$ for each state of B the probabilities of A sum up to 1.
- ❖ For a joint probability table (JPT), $P(A,B)$ the sum of all entries up to 1.

$$P(a_i, b_j) = P(a_i | b_j)P(b_j) \quad (14)$$

$$P(a_i) = \sum_{j=1} P(a_i, b_j) \quad (15)$$

- For another variable C we have:

$$P(A,B | C) = P(A | B,C)P(B | C) \quad (16)$$

4.1.4 Evidence and data updating

Bayesian networks are used for calculating new probabilities when new information is provided (Nielsen and Jensen., 2009). Each variable represented by a node has the probabilities to be at one the predefined states; the sum of the probabilities of being in each state is equal to 1. The evidence on this node is that we know the state of the node so the probability of this state will be 1 and 0 for the others states. This evidence makes change on the descendents nodes, this change called data updating and it represents a prediction of the future.

4.2 Types of Bayesian Network

Discrete Bayesian networks are probabilistic models that combine probability theory and graph theory (Pearl, 1988). The simple probabilities and the conditional probabilities are represented by absolute values between 0 to 1.

4.2.1 Static Bayesian Networks

Static Bayesian networks model just the actual situation of the study system without informations on the past or prediction of future situation. The conditional probabilities are stationary and don't change from a situation to another one.

4.2.2 Dynamic Bayesian Networks

In contrary to the SBNs, Dynamic Bayesian networks is a way to extend Bayes nets to model probability distributions over semi-infinite collections of random variables (Murphy., 2002). It contain temporal sequences to predict the future situation.

- To convert a SBN to a DBN, we need to add nodes representing multiples instances and link them with the precedents nodes.

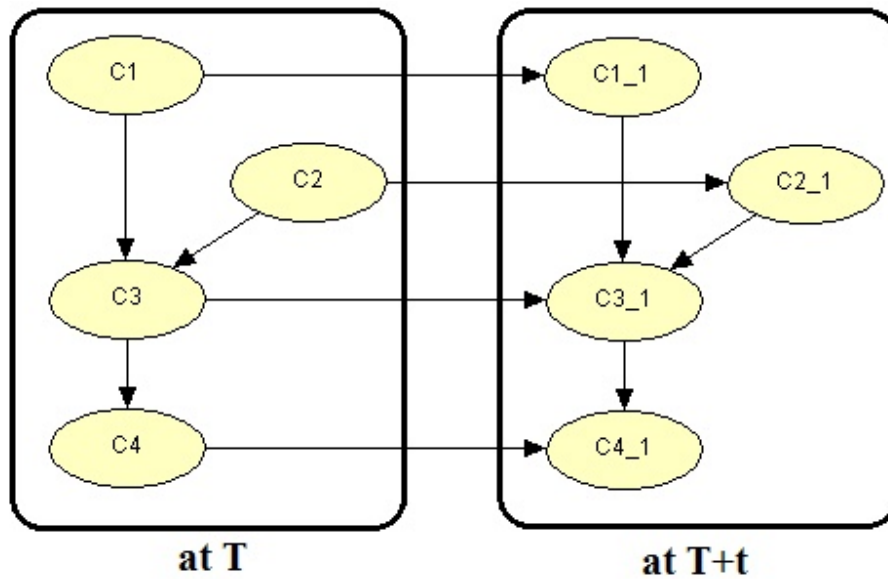


Figure 4.2 - Example of a dynamic BN.

4.2.3 Influence Diagram

The Influence diagram (ID) called also Limited Memory Influence Diagram (LIMID) or Object Oriented Bayesian Network is widely used in the field of investment, business and so on. It represents a BN with decision nodes also called action nodes to model the several possible decisions taken by user and utility nodes model the utilities. The others nodes are called the chance nodes.

- The utilities nodes are representing by utility tables but the decision nodes don't have tables.
- The utility function is defined by the arcs (links) from chance nodes or decision nodes to a utility node (the utility nodes never have children), the global utility function is the sum of all the local utility functions.
- The information available to the decision maker are defined by the arcs (called informational links) from chance nodes or decision nodes to a decision node.

4.3 Advantages of the Bayesian networks

Bayesian networks have plentiful advantages as a probabilistic modelling tool. First, they allow the use of the domain expert knowledge on their conditional probability tables (CPTs) with

give more access to the model input. Second, their graphical structure limited to a set of nodes and arrows provides an ease of understanding and tractability than many of the other techniques. Where the dependencies are simply represented by an unidirectional arrow from one node to another. Third, the modelling outcomes are simply absolute probabilities in a range from 0 to 1 inclusive. Fourth, the BNs are less influenced by small sample size (Eisenstein, 1996) because of the incorporation of the expert knowledge into the statistical data.

Bayesian networks are also superior in capturing interactions among input variables and they are flexible in regards to missing information. Even with missing data, the Bayesian networks show the ability to produce relatively accurate predictions (Lee and Abbott, 2003).

4.4 Disadvantage of the Bayesian networks

The Bayesian networks present few disadvantages such as their acyclic aspect making them unable to model some systems involving looping or information feedback. The domain expert knowledge is subjective and difficult to be standardized or technically assess.

4.5 Applications

4.5.1 Application on offshore drilling operations

The Bayesian network modelling has been applied to investigate the possible accidental scenarios causing the control well failure. The safety barriers and the emergency plan were assessed as well in the model to provide a complete understanding of these hazardous offshore operations.

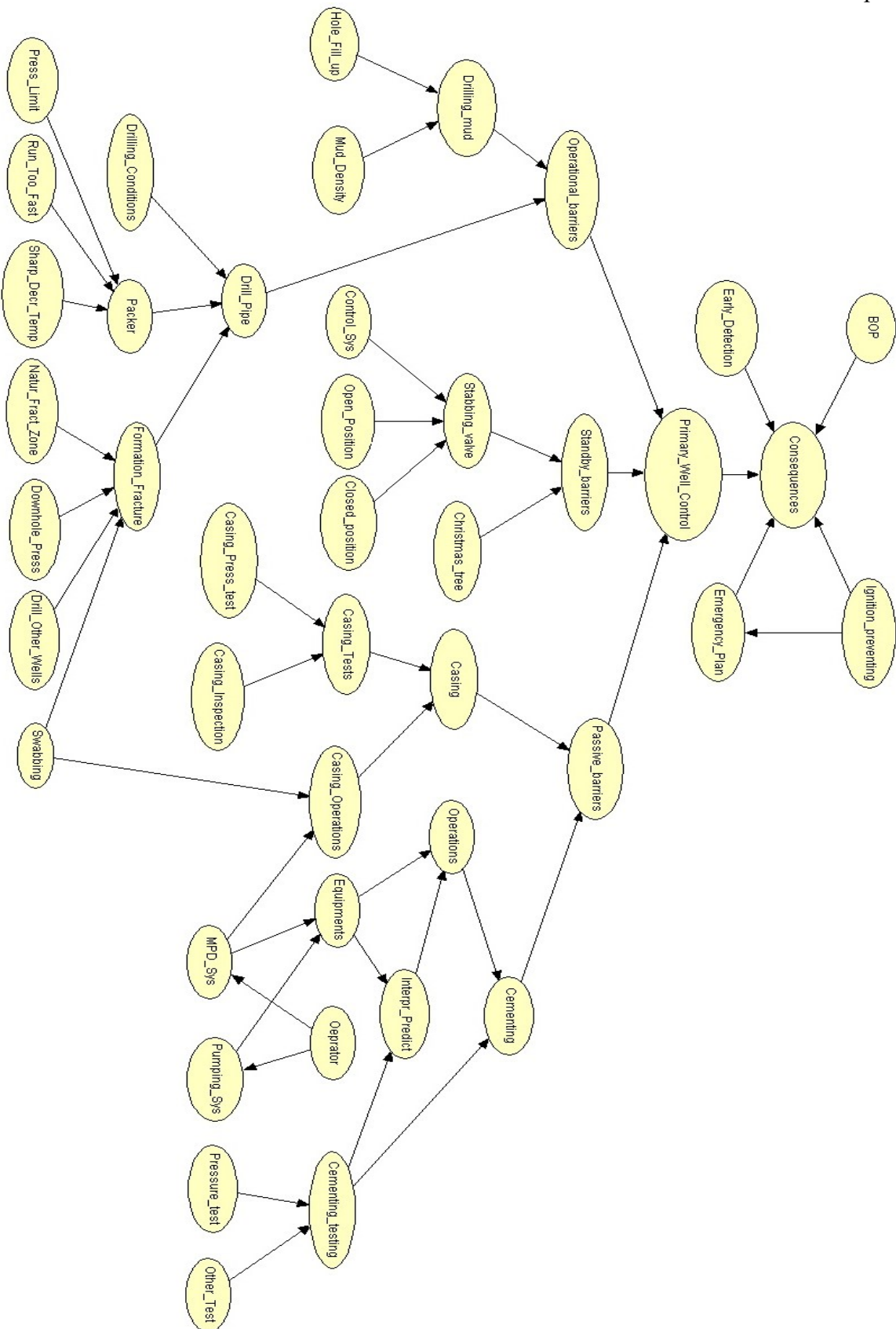


Figure 4.3 – BN application on well control failure scenarios and consequences.

SIMULATION OF INDUSTRIAL ACCIDENTS DUE TO UNCONTROLLED PRESSURES

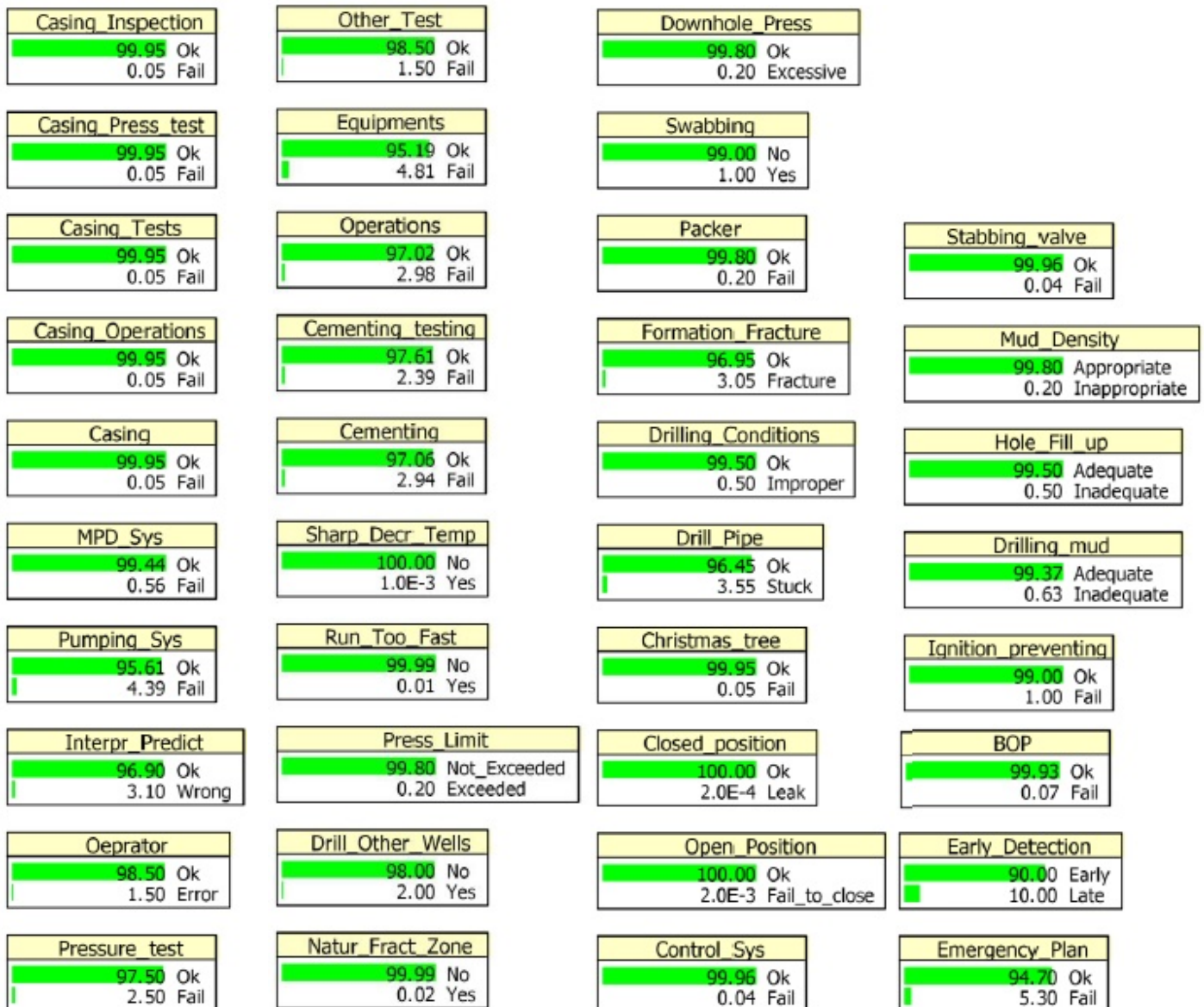


Figure 4.4 – Data from the BN model of offshore drilling operations.

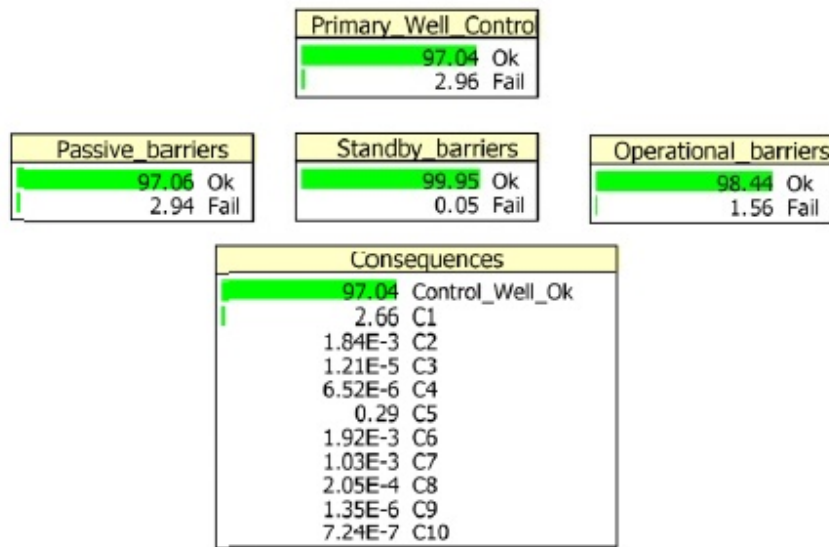


Figure 4.5 – Results from the BN model of offshore drilling operations.

4.5.2 Application on dynamic safety barriers assessment

This model aims to provide an understanding of the post-accidental situation following a flammable vapour release. In this hazardous situation, there are three safety barriers. The first safety barrier is the ignition preventing, it consist of all preventive acts to remove the ignition sources, as the use of ATEX certified equipment, lighting rod and so on. Figure 3.6 below show the static Bayesian network for these safety barriers responses.

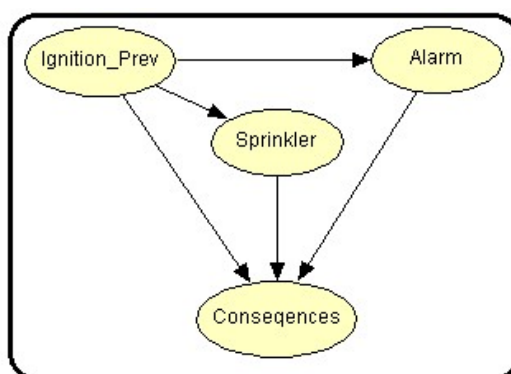


Figure 4.6 - Static Bayesian network for safety barriers response.

The ignition preventing barrier has a failure probability of 0.1. The failure probability of the alarm system is depending on the ignition preventing barrier success or failure. In case of success of the ignition preventing barrier, the alarm will be detecting the flammable vapour with a failure probability of 0.225. Otherwise, it will detect the fire with a failure probability of 0.0013. For the automatic fire sprinkler, it detects only the fire. So it doesn't have any response against the flammable vapour. In case of fire, the automatic fire sprinkler will detect and rain the water with a failure probability of 0.04. The conditional probabilities are represented in the following conditional probabilities tables.

Table 4.2 - conditional probabilities tables.

Ignition_Prev	IP	IPc
A	0.775	0.9987
Ac	0.225	0.0013

Ignition_Prev	IP	IPc
S	0	0.96
Sc	1	0.04

Ignition_Prev	IP				IPc			
	S		Sc		S		Sc	
Alarm	A	Ac	A	Ac	A	Ac	A	Ac
C0	1	0.4	1	0.4	0	0	0	0
C1	0	0.6	0	0.6	0	0	0	0
C2	0	0	0	0	0.8	0.6	0.2	0.05
C3	0	0	0	0	0.15	0.35	0.7	0.15
C4	0	0	0	0	0.05	0.05	0.1	0.8

Using Hugin software (Hugin., 2017) based on the Bayes theorem, we introduce the failure probabilities as described above and the dependencies given on the previous CPTs. The Hugin software give the consequences probabilities as follow:

Table 4.3 The UVC consequences and their probabilities.

Consequences	Probability (%)
C0	79.74%
C1	12.15%
C2	7.76%
C3	1.72%
C4	0.52%

In real cases from process industries, this risk of ignition is not the same at any moment after the release. Actually, it is proportional to the vapour cloud dispersion. That makes the safety barrier response a dynamic function. The static model of the BN cannot deal with this dynamic behaviour of the ignition preventing barrier. The same situation is applied for the fire/vapour alarm and the automatic fire sprinkler. In this case, the dynamic Bayesian network comes to solve and model this dynamic behaviour. Figure 3.6 below show the static Bayesian network for these safety barriers responses.

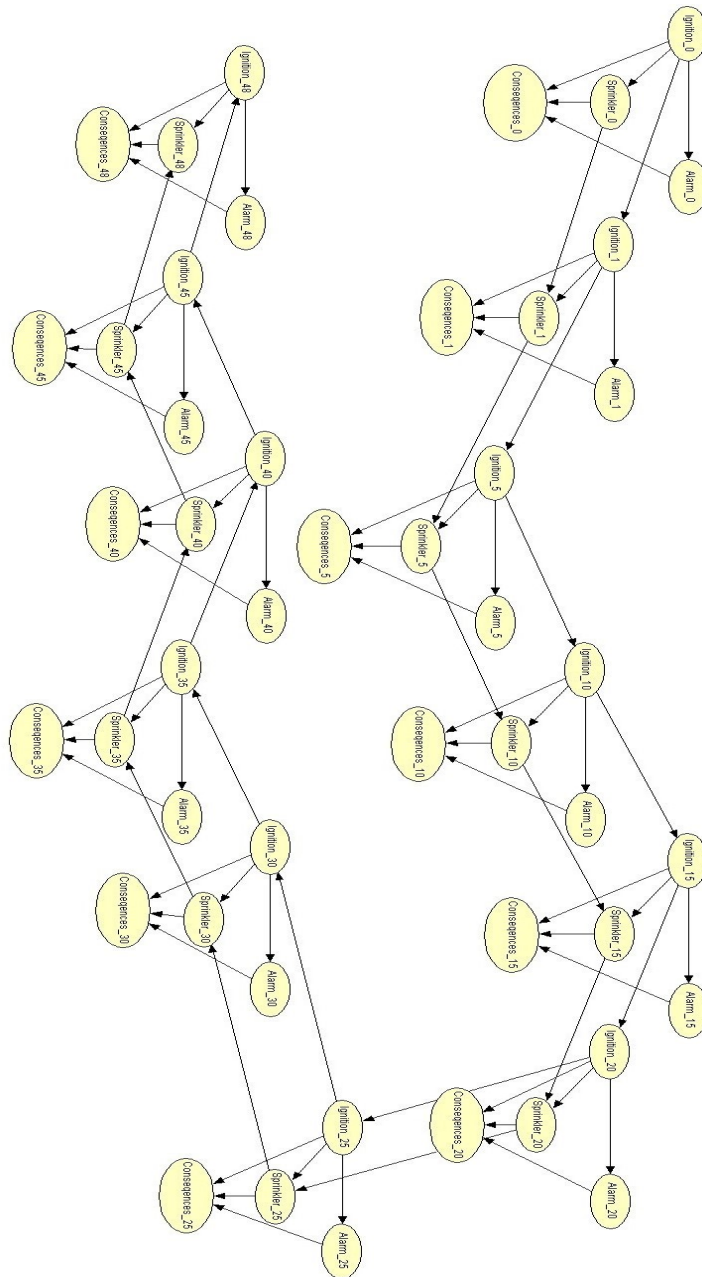


Figure 4.7 – Dynamic Bayesian network for the safety barriers.

4.6 Conclusion

The increase trend of use of the Bayesian networks in safety analysis studies is due to the benefits and the ease of use that provide these formalisms for the user and the input data accuracy that are originally subjective by nature, based on domain expert knowledge making them less exposed to the critics of accuracy and validation. Many researchers have used the

different varieties of Bayesian Networks (i.e. discrete time, dynamic, continuous and fuzzy BN) to express the causal relationships among the different system's elements. Experience from past accidents demonstrate the evidence that major industrial accidents never result from one single cause, but in all registered cases accidents involve multiple, interdependent causal factors. All actors or decision-makers influencing the normal work process might also influence accident scenarios, either directly or indirectly. This complexity should be reflected in the accident investigation process, and there may be need for analytical techniques to support the investigators to structure information and focus on the most important features. That can be provided in acceptable way by the various forms of Bayesian networks.

Part 2: Petri Nets

4.7 Introduction

Petri nets are graphical and mathematical modelling tool applicable to a large variety of systems. They are a promising tool for analysing and studying information processing systems that are characterized as being concurrent, asynchronous, distributed, parallel, and/or stochastic. As a mathematical tool, a Petri net model can be described by a set of algebraic equations, or other mathematical models reflecting the system's behaviour. This opens possibility for formal analysis of the model. It will allow, first to perform a formal check of the properties related to the behaviour of the underlying system, e.g., concurrent operations. Second, appropriate synchronization, freedom from deadlock, repetitive activities, and mutual exclusion of shared resources. Petri nets are particularly suited to represent in a natural way logical interactions among parts of activities in a system. This theory originated from the doctoral thesis of C. A. Petri in 1962. Since then Petri nets have been developed and used in many theoretical as well as applicative (Dutuit et al., 1997). Petri Net (PN) is a graphical paradigm for the formal description of the logical interaction among parts or of the flow of activities in complex systems. There exist many classes and various types of Petri Nets (i.e time, stochastic, fuzzy, hybrid...etc), with different features (i.e inhibitor arcs, coloured tokens, negative tokens...etc). That makes the study of their different kind difficult to accomplish. For this reason, this chapter presents a general view of these types of PN and focus on the class of Stochastic Petri Nets (SPN). In SPN formalism, the transitions' firing can be conditioned by a firing delay. If the delay is deterministic, the transition is called timed transitions. If it is stochastic, it's called stochastic timed transition. In the case of zero delay, the transition becomes instantaneous. A Time Petri Net (TPN) is a PN with at least one timed transition. But it shouldn't contain any stochastic transition, otherwise it becomes Stochastic Petri Net (SPN). In this chapter, the TPN are modelled using TINA soft (Berthomieu and Vernadat., 2006; TINA., 2017), and the SPN are modelled using GRIF-Workshop (SATODEV., 2017).

4.8 Definitions and basic concept

The Petri networks (PNs) were invented in 1962 by a German mathematician, Carl Adam Petri, as a new mathematical model to connect events and conditions. The PN's were applied first

in the fields of computer science and automatic control (David and Alla, 2010). After that, several research from 1968 consolidated the development and applications of PNs. Several early works until 1989 are listed minutely in the paper of Tadao MUTADA (Mutada, 1989).

4.8.1 Places, Transitions and Arcs

A PN is a bipartite directed graph (2types of nodes):



Places and transitions are connected by directed arcs.

Arcs exist only between a place and a transition or vice-versa.

Tokens circulate in the system between places.

➤ Example

Transition

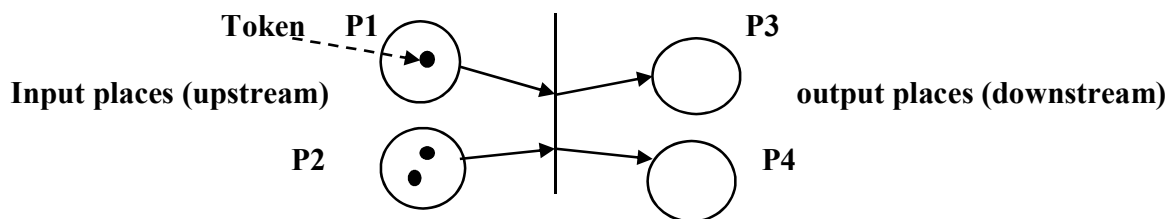


Figure 4.8 – An example of a simple structure of a Petri network.

A transition without an input place is a source transition.

A transition without an output place is a sink transition.

4.8.2 Marking

PN= (P, T, I, O)

P = set of places = {P₁, P₂, P₃, ..., P_M}.

T=set of transitions={T₁,T₂ ,T₃,....., T_N}.

Each place contains an integer number of tokens or marks.

The number of tokens contained in a place P_i will be called either m(P_i) or m_i.

The net marking, m , is defined by the vector of these markings, $m = \{m_1, m_2, \dots, m_M\}$.

4.8.3 Transition firing

A transition is fired whenever there is at least one token in all its input places. Once fired one token is removed from all its input places and one token is added to all of its output places.

Example:

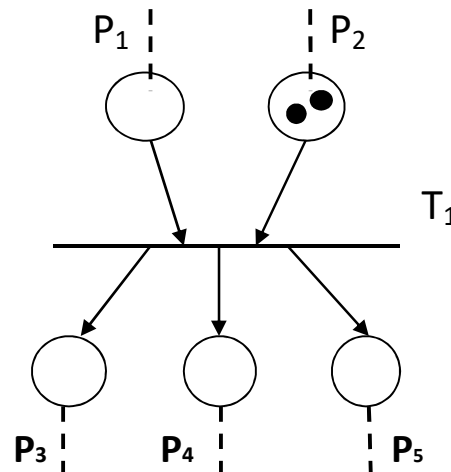


Figure 4.9 – transition firing demonstration of a simple Petri network.

Transition T₁ is not enabled, since P₁ does not contain any tokens.

4.8.4 Autonomous and non-autonomous Petri Net

Autonomous PN consist of a simple PN which the transitions don't contain any information (duration, probability...) its serve just to describe the passage between the places. This kind of PN is used to give a qualitative manner of the system. So, non-autonomous PN are all other kind of PN when we have some information on one or more transitions. We can said that the non-autonomous PNs describe functioning of systems that external events and/or time conditioned their evolutions.

Automaumous PNs have some characteristics, as follow:

- The dynamic system described by a PN is represented by the evolution of the markings.
- Deadlock occurs if no transition can be fired any longer.
- A PN for which a return to the initial marking is always possible is reversible.
- A conflict structure exists when the same place is an input of two or more transitions.

4.9 Special Petri Nets

4.9.1 Particular structures

4.9.1.1 State Graph

An unmarked PN is a state graph if and only if every transition has exactly one input and one output place.

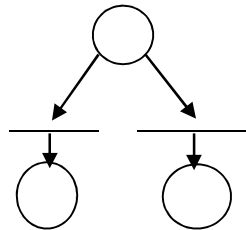


Figure 4.10 – Example of unmarked Petri network.

4.9.1.2 Event graph

A PN is an event graph if and only if every place has exactly one input and one output transition. An event graph is also called a transition graph or marked graph. An event graph is thus the dual of a state graph.

4.9.1.3 Conflict free PN

A structural conflict will be noted by the pair formed by one place and one set of output transitions of this place: $[P_1, \{T_1, T_2, \dots\}]$.

Example

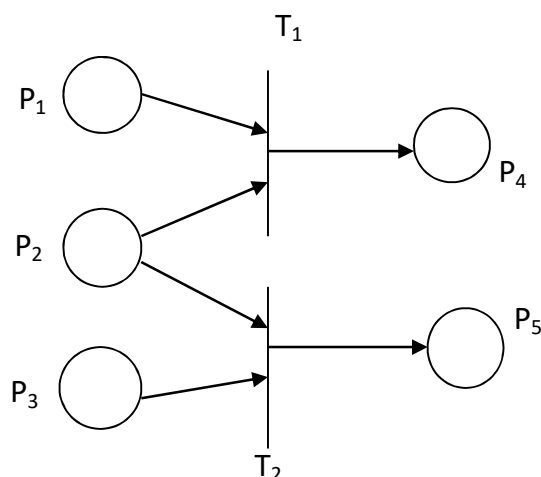


Figure 4.11 – An example of a conflict situation in a Petri network.

- If P_1 and P_2 have tokens but not P_3 : T_1 is fired.
- If P_2 and P_3 have tokens but P_1 : T_2 is fired.
- If both these transitions are enabled and there is only one token in P_2 , only one of these transitions can be fired. There is thus a conflict between these transitions. This concept relates to a decision to be taken between two firings.

4.9.1.4 Free choice Petri Net

Two definitions exist: free choice and extended free choice.

A free choice PN is a PN in which for every conflict $[P_1, \{T_1, T_2, \dots\}]$ none of the transitions T_1, T_2, \dots possesses another input place than P_1 .

An extended free choice PN is such that for every conflict $[P_1, \{T_1, T_2, \dots\}]$ all the transitions T_1, T_2, \dots have the same set of input places. That is to say if T_1 has P_1 and P_2 for input places, then T_2 has P_1 and P_2 for input places, etc.

In such a PN, if a transition involved in a conflict is enabled, all the transitions involved in the same conflict are also enabled.

4.10 Simple Petri Net

This is a PN in which each transition can only be concerned by one conflict at the most.

Example:

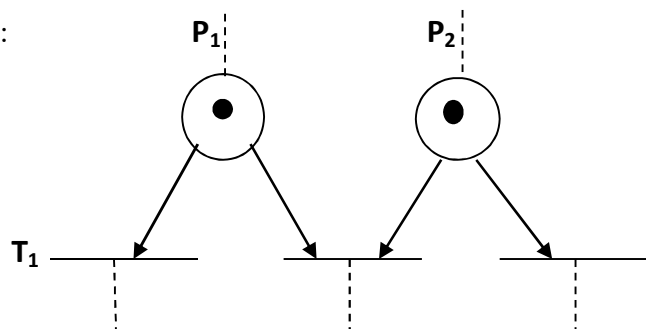


Figure 4.12 – An example of a simple Petri network.

This is not a simple PN because transition T_2 is involved in two conflicts $[P_1, \{T_1, T_2\}]$ and $[P_2, \{T_1, T_3\}]$.

4.11 Pure Petri Net

A pair consisting of a place P_i and transition T_j is called a self-loop if P_i is both an input and output place of T_j . A PN is pure if it has no self-loop.

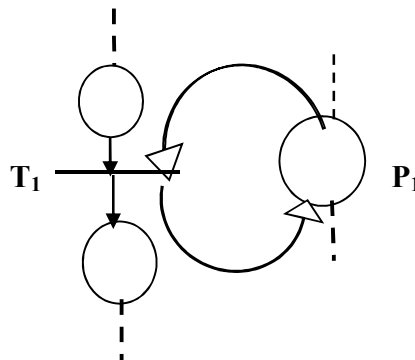


Figure 4.13 – Example of an impure net.

Place P_1 is both the input and the output of T_1 .

T_1 is said to be self-loop transition or impure transition, place P_1 is said to be self-loop place or impure place.

All impure PNs can be converted into pure PNs.

4.12 Generalized Petri Nets

A generalized PN is a PN in which weights (strictly positive integers) are associated with the arcs. When an arc $P_i \rightarrow T_j$ has a weight p , this means that transition T_j will be only enabled if place P_i contains at least p tokens. When this transition is fired, p tokens will be removed from place P_i . When an arc $T_j \rightarrow P_i$ has a weight p , this means that when T_j is fired, p tokens will be added to place P_i .

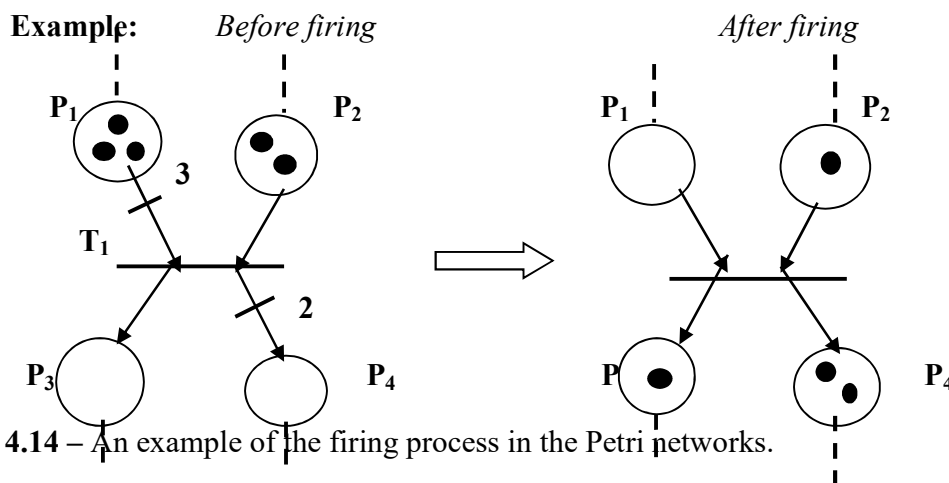


Figure 4.14 – An example of the firing process in the Petri networks.

All generalized PNs can be converted into ordinary PNs.

4.13 Finite Capacity PNs

Finite capacity PN is a PN in which capacities (strictly positive integer) are associates with places. Firing of an input transition of a place P_i , whose capacity is $Cap(P_i)$, is only possible if firing of this transition does not result in a number of tokens in P_i which exceeds this capacity.

All finite capacity PNs can be converted into ordinary PNs.

Example:

Transformation is simple in the case of Pure PNs, a complimentary place is added P_2 , known as P'_2 , $m(P'_2)=Cap(P_2)-m(P_2)$. thus when $m(P_2)= Cap(P_2)$, we have $m(P'_2)=0$ and transition T_1 is no longer enabled

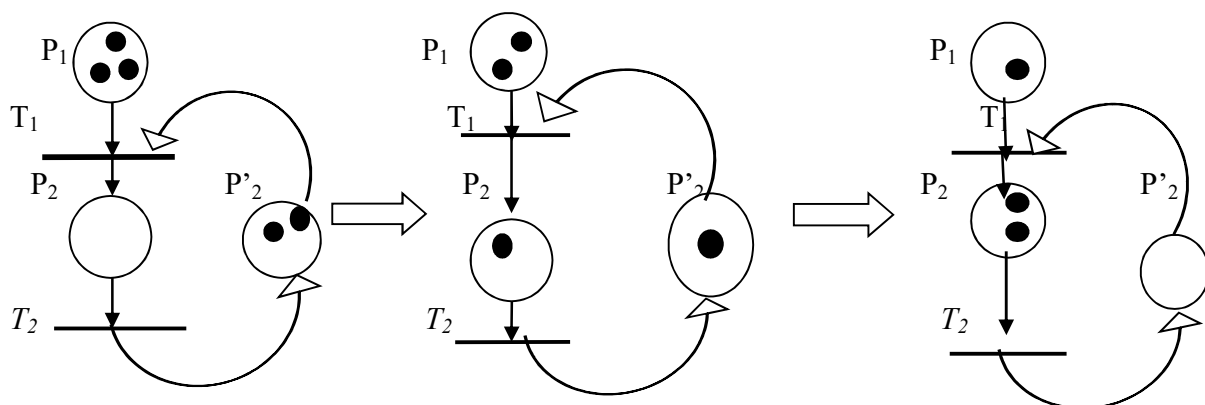


Figure 4.15 – An example of the firing process in a looping network.

4.14 Extended Petri Nets

An extended Petri Net contains special arc qualified as inhibitor and represented with a circle headed arc. An inhibitor arc between P_i and T_j means that transition T_j is only enabled if place P_i does not contain any tokens.

Example: *Transition with an inhibitor arc*

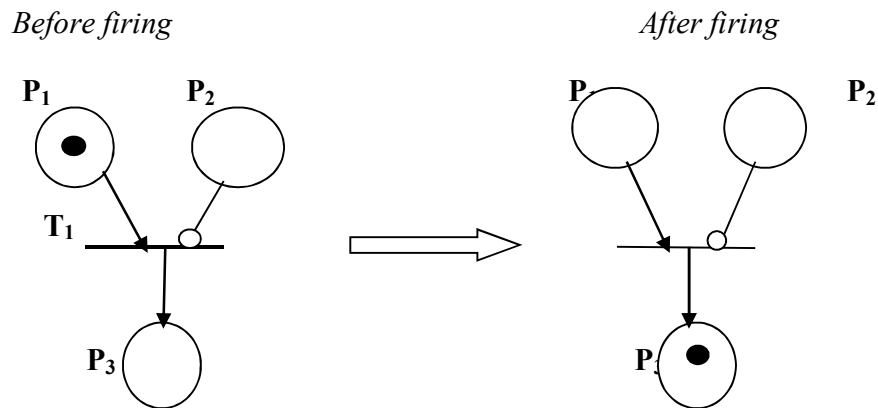


Figure 4.16 – An example of the firing process with inhibition arcs.

If the weight of an inhibitor arc $P_i \rightarrow T_j$ is s , then transition T_j is enabled only if $m(P_i) < s$, this is a threshold test .

A particular case called zero test when $s=1$ means that T_j is enabled only if $m(P)=0$.

4.15 Priority Petri Nets

This type of net is used to choose between a number of enabled transitions. The relation $T_j < T_k$ means that T_j has priority over T_k if both are enabled.

Priority PNs cannot be converted into ordinary PNs.

Example

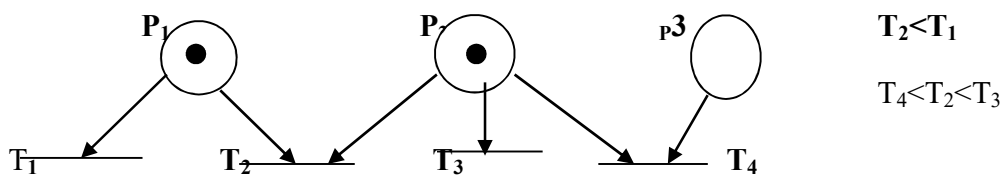


Figure 4.17 – An example of the priority in Petri networks.

T_1, T_2 and T_3 are enabled. Since $T_2 < T_1$ and $T_2 < T_3$, transition T_2 will be fired .

The core of PNs modelling is the concept of marking and firing. The marking of places represent the token's numbers of each place. Firing a transition represents the dynamic behaviour of PN, it consist of tokens migration from the input places to the output places...

An example of PN modelling is given in figure 5-11.

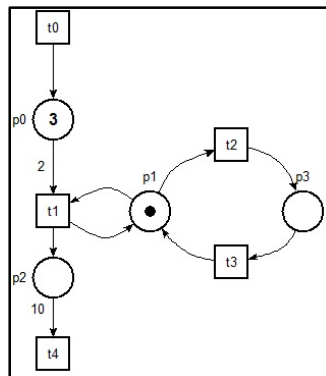


Figure 4.18 - Qualitative modelling using Petri Nets.

Figure 4-18 presents a part of production line, where the store (t0) fed the cage (p0) by items (tokens), a machine_on (p1) process two items from (p0) to one finished component on (p2), ten finished components (token) from (p2) will be moved to the store (t4). Through (t2), the (p1) can fail and become machine_off (p3). Then through (t3), the machine_off (p3) will be repaired and returns to machine_on (p1).

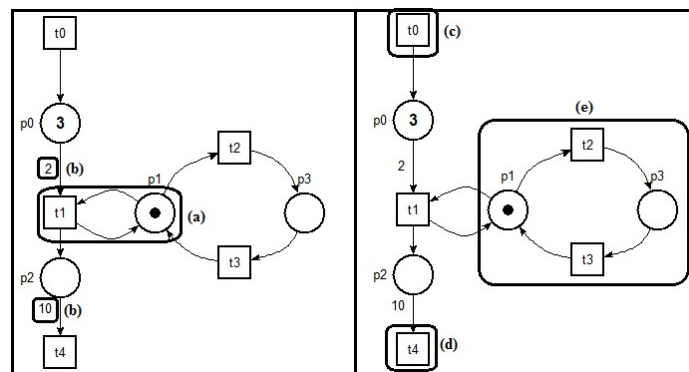


Figure 4.19 - Pointing the strong points of PN modelling.

The figure 4.12 points the some strong point of the PN modelling, there are explain on table2 below.

Table 4.4 - The pointing parts and their descriptions.

Part	Name	Description
(a)	Reading	This self-loop, mean that (t1) read the content or the state of (p1) without modifying
(b)	Arc	If it is on the arc from place to transition, it represents the required number

	weight	of tokens in the input place to enable the transition.
(c)	Source transition	(Transition without input places) uses to model the arrival of sources or events
(d)	Sink transition	(Transition without output places) uses to model the exit of sources or disappearance of events
(e)	“on-off loop”	This loop is largely uses to model a reversible alternation as (operational-failure) or other pair states.

The PN of the figure 5.3 is an autonomous PN, where just a qualitative description is given to understand the system functioning. For a quantitative modelling, figure 4 is given with time Petri Nets (TPN).

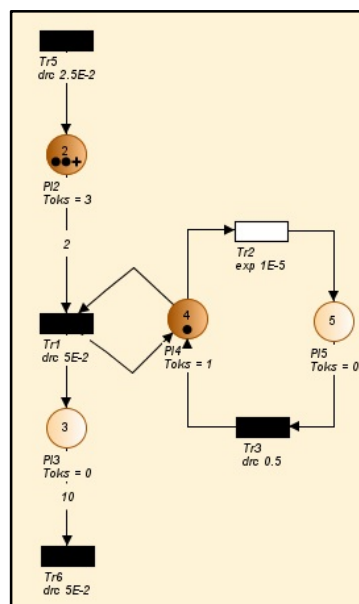


Figure 4.20 - Quantitative modelling using Time PN.

Figure 4 illustrate the quantitative modelling of the time PN with the new data given below:

- The interval between each input item is 0.025h (1min 30 sec)
- The required duration of transformation process is 0.05h (3min)
- The failure probability of the machine is 1E-5
- The machine’s repair duration is 0.5h
- Ten finished components (if available) will be moved to the store each 0.05h (3min)

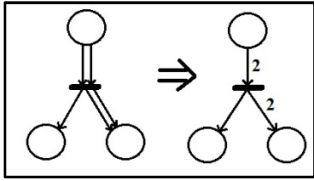
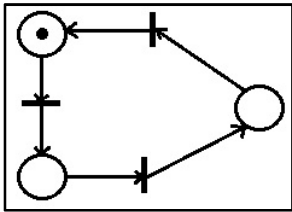

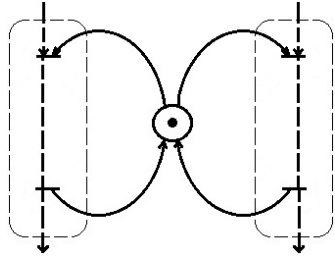
These data will allow us to quantify some parameters in table 4.2.

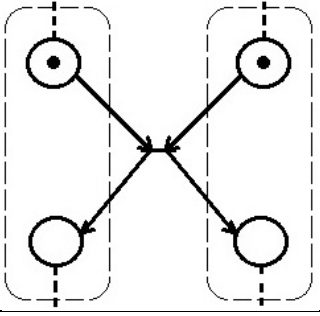
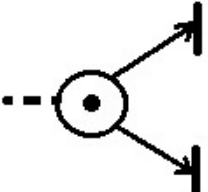
Table 4.5 - Quantitative results using Time Petri network.

	Name	Mean time in a place		Mean number of tokens at end of the history	
		mean time	Standard deviation	Mean mark	Standard deviation
1	PI2	1.00 E+004	0.00 E+000	5.02 E+000	4.56 E+000
2	PI3	0.99 E+003	1.05 E-001	5.50 E+000	7.95 E-005
3	PI4	9.99 E+003	1.74 E-001	9.99 E-001	1.74 E-005
4	PI5	6.99 E-002	1.74 E-001	6.99 E-006	1.74 E-005

Table 4.6 - Comparative analysis.

Characteristics	Techniques		
	Petri Nets	Bayesian Network	Fault tree
Composition	2 types : places and transitions	2 types : nodes and arcs	2 types : events and gates
Arcs direction	Non-sequential, can be cyclic or acyclic	Non-sequential but Acyclic	Sequential: from basic or elementary to intermediate events, from intermediate to intermediate events and from intermediates to top event
Connections	Between one or more places to one or more transitions or vice versa	All, except arcs from utility nodes.	Through logic gates (Or, And, Inhibition gate, KoutofN)
Types of arcs	Regular, with weight, Inhibitor, inhibitor with weight	Simple link	Simple link or inhibitor
Weight of arc	Integral number, positive or negative (Bartoletti et al., 2015)	No weight	No weight

			
Relationship	From a simple firing to a complex dependency	Conditional dependency	Binary mode
Graph forms	Cyclic or acyclic graph	Acyclic graph	Acyclic graph
Tables	Marking graph, coverability graph,...	CPT, JPT and utility tables	Probability table-minimal cut sets
Static/Dynamic modelling	Can be static or dynamic	Can be static or dynamic	Static only
Evidence	Can use evidences	Can use evidences	Can use evidences
Data updating	No developed	Can use data updating	Limited data updating
Good proprieties for a graph	Live, reversible and bounded 	Clear, readable and without overlapping	Clear and readable
Tokens/marks	A positive integral number (or negative[1])	No	No
Time dependency	Possible	Possible in continuous form	Possible in some advance forms
Parallelism	Possible 	Limited	Possible
Resources share	Possible 	No	No
Basic concept	Marking and firing (Réné)	Conditional	Logical dependency in

	et Alla.,2010)	dependency	vertical only
Synchronism	Possible 	No	No
Qualitative analysis	Possible	Possible	Possible
Graphical aspect	Low	Medium	High
Use for discrete, continue and hybrids system's evolution	Possible	Possible	Only for discrete
Conflict	Possible structural conflict 	No conflict	No conflict

4.16 Petri Nets modelling power

Petri Nets are particularly suited to model the concurrency and conflicts behaviours, the event's synchronization, resources sharing as the case of spare parts or maintenance team or any other resources that are not dedicate to be used in one place or by one user. PNs are also good in modeling sequencing and conditional branching and looping.

Stochastic Petri nets with Predicates and Assertions (Hamzi et al., 2013) have a great strength in their ability to model the dysfunctional state of a system and the functional or the operational state as well. SPN can be used for any kind of systems. Strong dependences among components can be modeled with reconfigurations over time, using deterministic or stochastic transitions: exponential, Weibull, triangular, uniform or any other law you may have programmed.

Tokens are used in PNs to simulate the dynamic and concurrent activities of systems, and it is possible to set up state equations, algebraic equations, and other mathematical models governing the behavior of systems (Murata, 1989)

Petri nets present two interesting characteristics. Firstly, they make it possible to model and visualize behaviours with parallelism, concurrency, synchronization and resource sharing. Secondly, the theoretical results concerning them are plentiful; the properties of these nets have been and still are extensively (David and Alla, 2010).

4.17 Limitations of Petri Nets

The limitations of the Petri Nets are:

- 1- In the application of Petri Nets, some difficulties arise making the modelling more complicate and intractable, or subject to many assumptions leading to a misrepresentation of the system’s real behaviour.
- 2- Petri nets need the support of other methods as the Monte Carlo simulation to enhance the modelling accuracy.

4.18 GSPN with predicates and assertions

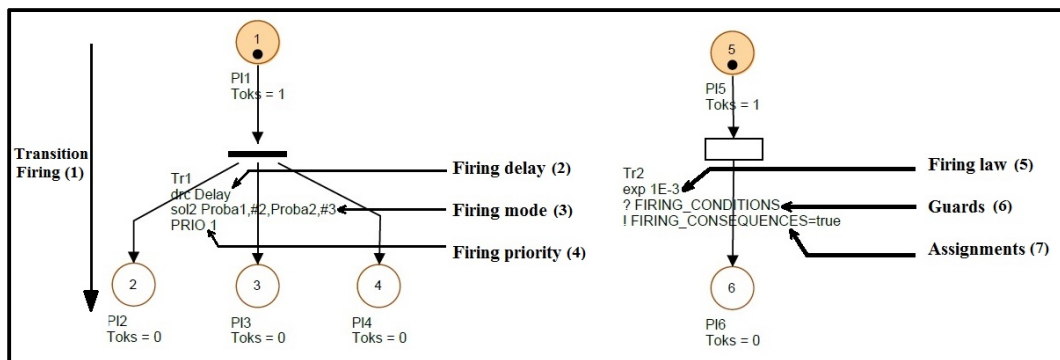


Figure 4.21 - Pointing the characteristics of the Stochastic PN with predicates and assertions.

In Petri nets modelling, tokens’ moving from a place to another must pass through a transition; this movement is called transition firing represented by (1) in Figure 4.14. This follows a firing law (5) permits to define the transition distribution (i.e exponential, weibull, normal or log normal distribution and so on) or timing through determination of firing delay (3).

The firing mode (4), can concern all downstream places equitably or on demand, where each downstream place has its specific probability law. Guards (6) are Boolean expressions conditioning transition firing. Assignments (7) are mathematical variables that receive predefined changes (i.e incrementation, turn to true or false) as firing consequence (M. Taleb Berrouane, al, 2016).

4.19 Conclusion

Petri Nets, as a modelling formalism, is combining a well-defined mathematical theory with a graphical presentation for dynamic systems' behaviours. Petri Nets have experienced several extensions enhancing their modelling power as techniques for RAMS analysis. GSPN with predicates and assertions is one of these PN extended forms, recently developed. The main advantages of this formalism are the use of variables for transitions' firing and virtual links between the different sub-systems modelled on separated networks. This allows a less complicated structure. However, their graphical presentation and their tractability are still subject of many critics and development initiatives. The new developed formalism developed in our current project may bring a contribution de this side of the modelling. The chapter also denotes advantages of using the PNs for reliability and risk analysis.

References

- Berthomieu, B. and Vernadat, F., 2006, September. Time petri nets analysis with tina. In Quantitative Evaluation of Systems, 2006. QEST 2006. Third International Conference on (pp. 123-124). IEEE.
- David, R. and Alla, H., 2010. Discrete, Continuous, and Hybrid Petri Nets. Springer Science & Business Media, New York, NY 10013, USA.
- Dutuit, Y., Châtelet, E., Signoret, J.P. and Thomas, P., 1997. Dependability modelling and evaluation by using stochastic Petri nets: application to two test cases. Reliability Engineering & System Safety, 55(2), pp.117-124.
- Eisenstein EL, Alemi F. A comparison of three techniques for rapid model development: an application in patient risk-stratification. Proc/AMIA Annu Fall Symp 1996:443–7.
- Hamzi, R., Innal, F., Bouda, M. A., Chati, M., 2013, Performance Assessment of an Emergency Plan Using Petri Nets, Chemical Engineering Transactions, 32-2013. ISBN 978-88-95608-23-5; ISSN 1974-9791
- Hugin, <http://www.hugin.com/index.php/hugin-developerhugin-researcher> page accessed (14.01.2017).
- Lee, S, M., Abbott, P, A., 2003. Bayesian networks for knowledge discovery in large datasets: basics for nurse researchers. *Journal of Biomedical Informatics* 36, Issues 4–5: 389–399 <http://dx.doi.org/10.1016/j.jbi.2003.09.022>
- Murata, T., 1989. Petri nets: Properties, analysis and applications. Proceedings of the IEEE, 77(4), pp.541-580. <http://dx.doi.org/10.1109/5.24143>
- Murphy, K.P., 2002. Dynamic bayesian networks: representation, inference and learning (Doctoral dissertation, University of California, Berkeley).
- Nielsen, T.D. and Jensen, F.V., 2009. Bayesian networks and decision graphs. Springer Science & Business Media. ISBN 978-0-387-68282-2
- Jensen, F.V., 1996. An Introduction to Bayesian Networks. Editions UCL Press, London, UK.
- Pearl, J., 1988. Probabilistic reasoning in intelligent systems: networks of plausible inference. Morgan Kaufmann Publishers Inc, San Francisco, USA.

SATODEV, 2017. GRIF-Workshop. <http://www.satodev.com/category/grif> (accessed 03.19.17).

Talebberrouane, M., Khan, F. and Lounis, Z., 2016. Availability analysis of safety critical systems using advanced fault tree and stochastic Petri net formalisms. *Journal of Loss Prevention in the Process Industries*, 44, pp.193-203.

TINA, <http://projects.laas.fr/tina/> page accessed (05.12.2016)

Weber, P., Medina-Oliva, G., Simon, C. and Iung, B., 2012. Overview on Bayesian networks applications for dependability, risk analysis and maintenance areas. *Engineering Applications of Artificial Intelligence*, 25(4), pp.671-682. <http://dx.doi.org/10.1016/j.engappai.2010.06.002>

Chapter 5

Applications of Risk Based Assessment Using Petri Nets Formalisms

Part 1: Risk Based Assessment of Gas Flares Systems by using Time Petri Nets

5.0 Introduction

Systems in oil and gas plants play critical roles in the safe operation of plants. They are designed to dispose of waste gases and discharged liquids from process units safely. It is generally used to handle materials vented during normal operations, start-up, and emergency conditions. There are three main kinds of flare systems in oil and gas industry: elevated flares, ground flares and low pressure flares. Elevated flares are used as abnormal feature of a refinery or a petrochemical plant and are handled in both normal and emergency circumstances. Contrary to the discharges composed of vapor or mist, elevated flares rapidly disperse when they are vented in the atmosphere at high velocity, liquid discharges settle to ground. If volatile components are present, then a flammable atmosphere can result. The risk of fire or explosion can be high if appreciable quantities of hydrocarbons liquid are released to the atmosphere when the ambient temperature is at or above the liquid flash point. Theoretically, liquids of a flash point above the maximum anticipated ambient temperature do not vaporize enough to create a flammable atmosphere. However, widespread spraying of oil droplets can create concern in an emergency and constitute a serious nuisance (Zadakbar et al., 2011; 2014).

Liquid overflowing from the flare stack may result in a more smoky flame, in dispersion of burning drops of flammable material or dispersion of drops of toxic material. Liquid drops as small as 15 μm can negate the devices used for smokeless operation and give a smoky flame (Charles and Baukal., 2014) The main means used to prevent liquid drops from reaching the flame is a knockout drum at the stack base. However, it is sometimes difficult to eliminate completely spray and condensation.

The need to develop formal methods enabling to know nominal and degraded behavior of complex systems in order to evaluate their abilities to provide services without causing damages to environments, persons, etc. is very important (Benani et al., 2014). Many formal methods using different approaches for specification and validation systems exist in literature. These works represent a current field which concerns researchers of the automatic control community and the computer science community. Among existing models in literature we can give bond

graph model (Boon et al., 2011), timed automaton for the supervisory control (Gouin and Ferrier., 1999) and Petri nets (Sekhri and Slimane., 2014).

Petri nets are a mathematical tool well suited to model and to analyze systems exhibiting behaviors such as concurrency, conflict, and causal dependency between events. They have been proposed as a promising tool for modeling and analyzing Discrete Event Systems (DES). They are notably used to model concurrent-software systems, communication protocols and monitoring of automated production systems (Sekhri et al., 2004).

In the context of reactive and safety related applications, some authors have investigated the use of Petri nets and some extensions for these applications. A review of some developed works from 1992 to 2000 is given in (Vernez et al., 2003). Some authors have investigated the graph transformation into Petri nets (Raiteri., 2005) while others deal with performance evaluation and reliability assessment (Keyner and Volovoin., 2010; Hamzi et al., 2013). In literature, limited works have been cited on the overflowing of flammable liquid from flare stack. In (Kalantarnia., 2010) a modeling of the BP Texas city refinery accident is given using dynamic risk assessment approach (Kalantarnia., 2010).

This part is organized as follows: in section 2, the removal liquid system is presented, section 3 introduces some formal definitions of Petri nets (PN) and time Petri nets (TPN); section 4 offers a case study which consists of a flaring system modeled by a time Petri net, in this section some scenarios are studied where some failures are introduced in the model. In section 5, the validation of the results is performed using TiNA tool. Finally, we conclude our work and discuss some future research.

5.1 Removal Liquid System

5.1.1 Knockout Drum

All flares, vent and relief systems must include a liquid knockout drum. Knockout drums or knockout vessels are used to slow down gasses and allow liquids to essentially fall out of the gas stream. Knock-out drums can be installed either in the waste gas header or in the flare stack base itself. Knockout drums can be configured in either a horizontal or vertical arrangement. Horizontal knockout drum is generally build with one gas stream inlet, and two outlets, which

can then be joined with a manifold. Another configuration that can be used is one inlet with a much larger outlet. Automatic drain controls can be included to prevent fluids accumulation in the seal. Flanged drain connections are included for draining and cleaning the vessel. Figure 5.1 depicts knockout drum components (Cheremisinoff., 2013).

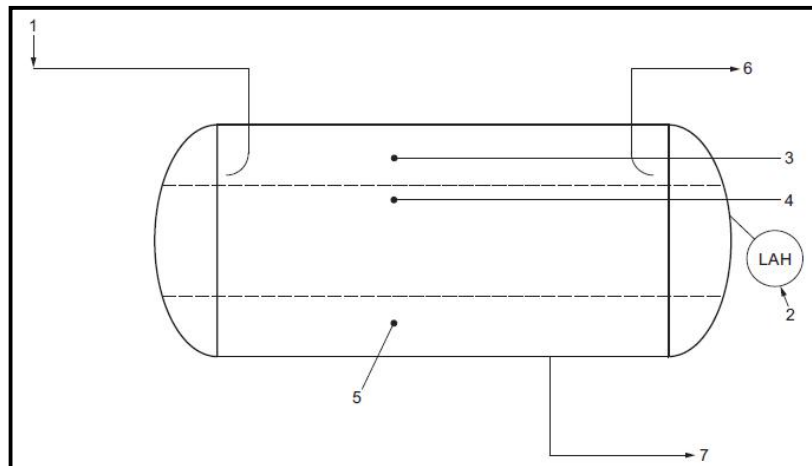


Figure 5.1 - Flare Knockout Drum.

1. Vapor and liquid pressure relief valve releases.
2. Level instrument to indicate when stipulated slop and drain volume becomes liquid full.
3. Minimum vapor space for dropout velocity.
4. Liquid holdup from pressure relief valves and other emergency releases.
5. Slop and drain liquid.
6. Flare.
7. Pump-out.

5.1.2 Liquid overflowing occurrence

In flare systems, the potential of either liquid introduction or the formation of hydrocarbon or water vapor condensate in the flare header. Allowing this liquid phase to overflow the knockout drum, this can obstruct gas flow to the flare, resulting in overpressure to upstream systems (Raiteri., 2005). If a failure occurs on discharge system, then the liquid phase reaches the combustion zone where small hydrocarbon droplets are led by waste gas and carried into the flame to be usually burnt incompletely forming soot. So, the smokeless capacity of the flare is

reduced. If the droplets become larger, then they may be able to fall out of the main flame envelope.

An example of the spectacular flammable liquid overflowing from flare stack in an offshore installation is given by Figure 5.2.a, Figure 5.2.b and Figure 5.2.c. Events have been reported where a mostly-liquid stream has been discharged from the flare (Charles and Baukal., 2014).



Figure 5.2.a Start of the flaring event.



Figure 5.2.b Liquid fall out and flaming rain from flare flame.



Figure 5.2.c Flaming liquid engulfs flare stack.

Figure 5.2.c illustrates a photo taken only a few minutes after the photo illustrated by Figure 5.2.b showing how rapidly the situation can be deteriorated. Another case is the non-flammable liquids (generally water) and able to extinguish the flame, which may result in environmental or safety hazards. During carry over, burning efficiency may be reduced and

possible hazardous (flammable, toxic, or corrosive) fluid may spray from the stack. Flammable or toxic vapor cloud or other adverse safety consequences can occur. This situation can be composed by a release from another part of facility of flammable or heavier-than-air vapor likely to cause an explosion.

5.2 Petri Nets Modeling

5.2.1 Petri nets

In this model, we follow the terminology and the notations of Petri nets as defined in (Barkaoui and Peyre., 1996; Hanžic et al., 2013).

➤ 5.2.1.1 Definition 1

A Petri net N is a 4-tuple $G = (P, T, F, V)$ where:

$G = (P, T, F, V)$ is a weighted bipartite digraph.

P is a finite set of state places and T is a finite set of transitions with $P \cup T \neq \emptyset$ and $P \cap T = \emptyset$

F is a set of directed arcs connecting state places to transitions and vice-versa.

V is the weight application (valuation): $V \in [F \rightarrow \mathbb{N}^+]$

➤ 5.2.1.2 Definition 2

A marking M of a Petri net $G = (P, T, F, V)$ is a mapping from P to \mathbb{N} (set of integer) where $M(p)$ denotes the number of tokens contained in place p .

A marked Petri net is a couple (G, M_0) where G is a Petri net and M_0 a marking of G called the initial marking.

We denote for a node $s \in P \cup T$, $\bullet s$ (resp. $s \bullet$) the set of nodes such that $(s', s) \in F$ (resp. $(s, s') \in F$).

The valuation V of a Petri net can be extended to the application W from $(P \times T) \cup (T \times P) \rightarrow \mathbb{N}$ defined by: $u \in (P \times T) \cup (T \times P)$, $W(u) = V(u)$ if $u \in F$ and $W(u) = 0$ otherwise. The matrix C indexed by $P \times T$ and defined by $C(p, t) = W(t, p) - W(p, t)$ is called the incidence matrix of the net.

➤ **Definition 3**

Let (G, M_0) be a marked Petri net. A transition $t \in T$ is enabled by a marking M if and only if $\forall p \in \bullet t, M(p) \geq W(p, t)$. The marking M' reached by firing t at M is defined by $\forall p \in P, M'(p) = M(p) - W(p, t) + W(t, p)$ denoted by $M[t > M']$.

By extension, a marking M' is said to be reachable from a marking M if there exists a sequence of transitions $s = t_0 . t_1 \dots t_n$ and a series of marking M_1, \dots, M_n such that $M[t_0 > M_1, M_1[t_1 > M_2, \dots M_n[t_n > M']$ (denoted $M[s > M']$). The set of the markings of N reachable from a marking M is denoted by $R(G, M)$.

➤ **Definition 4**

Let (G, M_0) be a marked Petri net. A transition t of G is live if and only if $\forall M \in R(G, M_0), \forall M' \in R(G, M)$ such that $M'[t > (G, M_0)$ is quasi-live if and only if $\forall t \in T, \forall M \in R(G, M_0)$ such that $M[t > (G, M_0)$ is weakly-live (deadlock-free) if and only if $\forall M \in R(G, M_0), \forall t \in T$ such that $M[t > (G, M_0)$ is called bounded if and only if $\exists k \in \mathbb{N} / \forall M \in R(G, M_0), \forall p \in P, M(p) \leq k$. (G, M_0) is live if and only if all transitions of G are live.

5.2.2 Time Petri nets

In order to formally prove the correct operation of our system, it is important to model it in a convenient mathematical model according to its specifications. Petri nets are mathematical modeling language for use on huge complex systems (Berthomieu and Vernadat.,2006), the introduction of time Petri nets is motivated by their ability to model easily temporal constraints and the existence of a TiNA (Time Net Analyzer) software tool for properties verification. TPN extend Petri nets by associating two values (min, max) value min (min = 0), is the minimal time that must elapse, starting from the time at which transition t is enabled until this transition can fire and max (0 = max = 8), of time (temporal interval) to each transition. They denotes the maximum time during which transition t can be enabled without being fired. Times min and max, for transition t , are relative to the moment at which t is enabled.

If transition t has been enabled at time a , then t cannot fire before $a + \min$ and must fire before or at time $a + \max$, unless it is disabled before its firing by the firing of another transition.

5.2.3 TiNA tool

TiNA functionalities allow a temporal study of a TPN model based on the reachability analysis method for usual Petri nets (Hamzi., 2013). TiNA allows us to validate properties of our liquid overflowing model as:

- a. Boundedness property: this property relates to the finite number of tokens in each place of a TPN for any marking reachable from an initial marking. The not bounded property is characterized by an infinite number of tokens in at least one place among other places of the TPN. In this case, we notice that the model diverges or the implemented system will require an abnormally high quantity of resources (memory, CPU time, etc).
- b. Liveness property: this property allows the detection of portions of died code. The absence of liveness makes it possible to highlight portions of code which are never performed (thus to detect the modelling errors) and situations where the system modelled is likely to be blocked.
- c. Reversibility property: the re-initialisation of the system supposes that the system finds its initial state (initial marking) on the basis of any other state during its operation. This property is fundamental to validate automata based systems which present a cyclic operation.

5.3 Case Study

5.3.1 Liquefaction Natural Gas (LNG) cold flare

Our case study is taken from LNG complex, the GL1/Z-SONATRACH – Algeria, containing three flare systems. The cold flare system for gases colder than 0° C, the hot flare for gases warmer than 0° C, and the tank flare system for excess vapors from the LNG storage tanks. Hydrocarbon gases entering the Hot/Cold flare systems in each unit flow to a main header, into knockout drums where any hydrocarbon liquids are removed and sent to the flare stack to be burned at a distance from the complex (Sekhri et al., 2004).

According to the feedback experiences with the testimony by the personal (team) of gas complex, we noted that the cold flare is the most exposed to the risk of liquid overflowing, it is

for that we will be directed our research on this flare. A detailed description of the LNG cold flare is given in (Sekhri et al., 2004).

5.3.2 Liquid overflowing modeling

Figure 5.3 depicts the time Petri net model of our system in abnormal situation, where the risk that the liquid fall out to the flare stack occurs if the LSH is failed (p7 place) followed by poorly monitoring of the field operator (p10 place), failure of either LSH and the level indicator (LI) (p8 place) or failure of the pump (p9 place) followed by poorly monitoring of the field operator. So the rise of liquid continues in the knockout drum (p11) and after in the flare stack until it's overflowing (p12). Hypotheses on incident occurrence are as follows:

- The duration of knockout drum filing from the low to the high level equal one time unit.
- The duration for the pump to drain the knockout drum from the high to the low level is negligible compared to the duration of knockout drum filing.
- The duration is between four to five time units to arrive to the summit of the flare stack, it varies according to quantity of liquids in the flaring gas.
- The end of overflowing took between three to four time units.
- The duration for the end of overflowing is between two to three times unites.
- The switching-on of the LSH, the pump startup and the draining of the knockout drum with stopping pump are instantaneous.
- The durations and the occurrences probabilities of the initiators events of the incident are given in Table1.

Table 5.1 Occurrences probabilities and durations of initiators events.

Transitions	Characteristics		
	Meanings	Occurrence Probabilities	Durations
t ₅	Failure of the LSH	0.083-0.01	100-120
t ₆	Poorly monitoring	0.033-0.04	25-30
t ₇	Failure of the pump	0.019-0.02	50-60
t ₈	Failure of either LSH and LI	$(5.5-6.6) \times 10^{-3}$	150-180

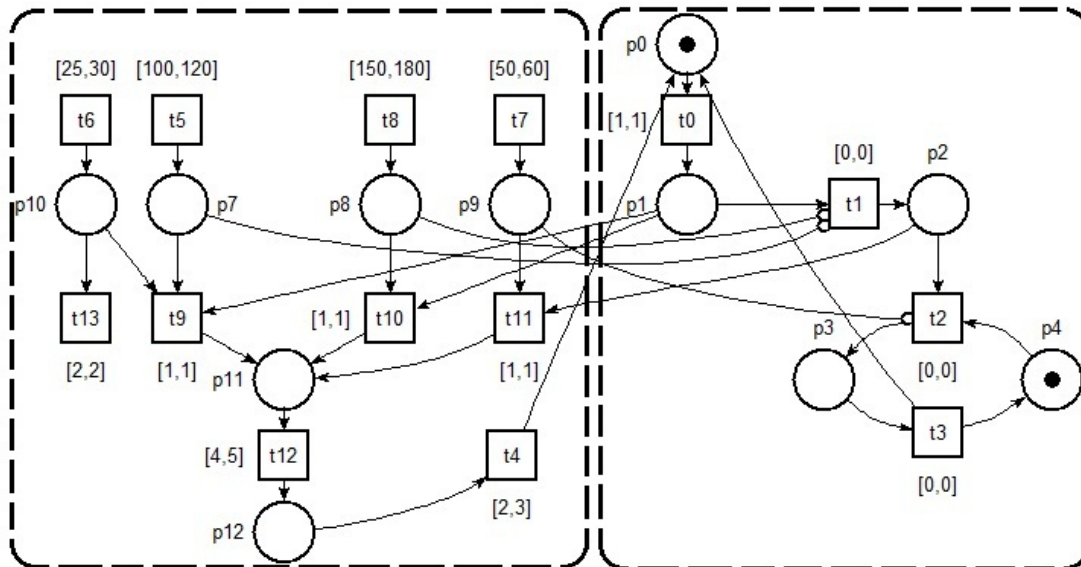


Figure 5.3 - Time Petri net model for the liquid overflowing incident.

- (a) : Sub-system of normal operating.
- (b) : Sub-system of failure mechanism.

The meaning of the places and transitions are given respectively in Table 2 and Table 3.

Table 5.2 Places and their meanings.

Places	Meanings
P ₀	LSL [switched on]
P ₁	Knockout drum at high level
P ₂	LSH [switched on]
P ₃	Pump [on]
P ₄	Pump [off]
P ₇	LSH [Failed]
P ₈	LSH and LI [Failed]
P ₉	Pump [Fail to start on demand]
P ₁₀	Poorly monitoring by the field operator
P ₁₁	Knockout drum [Overflowed]
P ₁₂	Overflowing of flammable liquid

Table 5.3 Transitions and their meanings.

Transitions	Meanings
t ₀	Level elevation of the knockout drum
t ₁	Switching on the LSH
t ₂	Pump startup
t ₃	End of the overflowing
t ₄	Draining of the knockout drum and Stop pump
t ₅	LSH failure (failure to be activate)
t ₆	Poorly monitoring
t ₇	Pump failure (failure to start on demand)
t ₈	LSH and LI failure (failure to be activate)
t ₉	Overflowing of the knockout drum
t ₁₀	Overflowing of the knockout drum
t ₁₁	Overflowing of the knockout drum
t ₁₂	Overflowing of liquid in the flare stack
t ₁₃	Monitoring resumption

On the sub-system of failure mechanism of Fig.3, three scenarios conducting to the incident on (P12) are representing by the firing of the transitions (t₉, t₁₀, t₁₁) is shown in table 4.

Table 5.4 Scenarios and their causes.

Transitions	Scenarios	Causes
t ₉	First scenario	LSH failure with poorly monitoring
t ₁₀	Second scenario	Failure of either LSH and LI
t ₁₁	Third scenario	Failure of the pump with poorly monitoring.

5.3.3 Removal liquid system modeling

5.3.3.1 Normal operating modeling

Figure 5.4 depicts the time Petri net model of the sub-system (a) representing the normal functioning of the flare draining system.

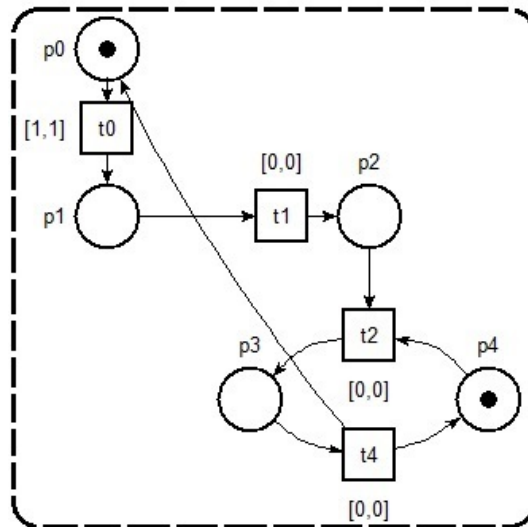


Figure 5.4 Time Petri net model of normal operating.

The values in the intervals associated to transitions refer to relative time for execution, one time unit is the necessary duration to the rise of liquid from the LSL to the LSH level (p1 place). In the flaring system, the knockout drum is provided by a centrifugal pump. The pump star-up is controlled automatically by switching the level security high (LSH) at high level of the knockout drum (p2 place) and stopped by switching the level security low (LSL) at low level of the knockout drum level (p0 place).

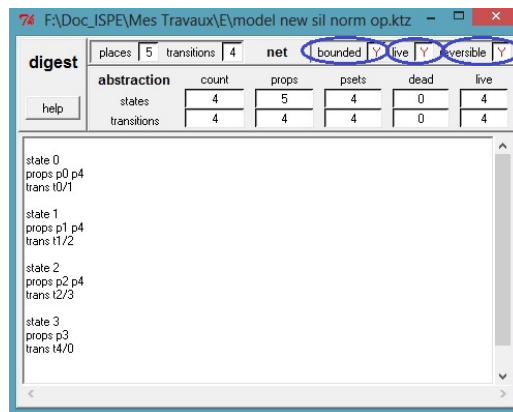


Figure 5.5 State classes of normal operating.

Figure 5.5 depicts the state classes of the sub-system of normal operating. the following classes (C0 to C3) are generated by TiNA tool during the analysis phase:

- Class 0: p0, p4, $1 \leq t0 \leq 1$
- Class 1: p1, p4, $0 \leq t1 \leq 0$
- Class 2: p2, p4, $0 \leq t2 \leq 0$
- Class 3: p3, $0 \leq t4 \leq 0$

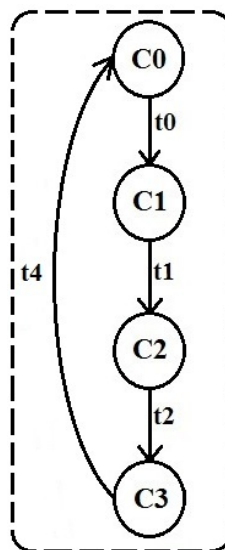


Figure 5.6 State classes graph of normal operating system.

Figure 5.6 depicting the state classes graph reveals that our model has effectively the good properties previously mentioned:

- a. Liveness: the net is deadlock freeness and each transition is always able to be fire infinitely.
- b. 1-Boundedness: the number of tokens in every place is limited to one token.
- c. Reversibility: the return of the system to its initial state shows that the normal operating model is reversible (able to be reinitialized).

5.3.3.2 LSH failure with poorly monitoring

If the LSH fails, the level indicator of the knockout (KO) drum continues to indicate the level in real time. If the indication exceeds the high level, theoretically the field operator checks the LI and doubt about a possible failure on the KO drum draining system. Otherwise, if the field operator doesn't check the LI (poorly monitoring) the rising of the liquid continues and passes unobserved.

5.3.3.3 Failure of LSH and LI

This case can take place if a failure of the LI occurs with one of the following scenarios: failure not detected, detected failure but the procedure to repair it doesn't being executed correctly or unavailability of spare part. Otherwise, the flare system can function without indication of the KO drum level, what can make ignorance on its failure. Afterward, it is enough that the LSH fail and the failure doesn't being detected in early time.

5.3.3.4 Pump failure with poorly monitoring

The level indicator of the knockout (KO) drum indicates the level in real time, if the pump fails; theoretically the field operator checks the LI and doubt about a possible failure on the KO drum draining system. Otherwise, if the field operator doesn't check the LI (poorly monitoring) the rising of the liquid continues and passes unobserved.

5.4 Results And Interpretations

5.4.1 Results

Using TiNA simulation tool, the obtained results are given in table 5 and illustrated by Fig. 7.

Table 5.5 Occurrences times of the different scenarios.

Order of occurrences	Scenarios	Occurrences times
1	Third scenario	55.76
2	First scenario	105.8
3	Third scenario	114.47
4	Second scenario	155.74
5	Third scenario	164.96
6	First scenario	215.14
7	Third scenario	224.5

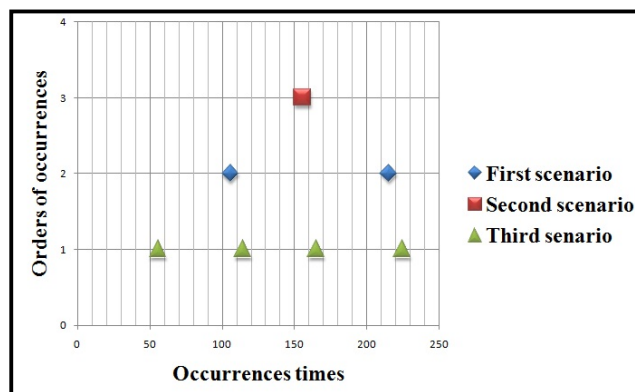


Figure 5.7 Graph of occurrences times.

5.4.2 Results interpretation and recommendations

Results interpretation and recommendations given from the system analysis are illustrated by Table 5.6 and Table 5.7.

Table 5.6 Scenarios and their implicated elements.

Order of occurrences	Scenarios	Implicated elements
1	Third scenario	KOD pump – Field operator
2	First scenario	LSH – Field operator
3	Second scenario	LSH – LI

Table 5.7 Preventive maintenance planning.

Order of maintenance	Element	Time for preventive maintenance
1	KOD pump	50
2	LSH	100
3	LI	100

5.5 Conclusion And Future Works

In dependability, Petri nets have been applied for performances assessment of emergency plan, reliability of shutdown procedures, etc. In this paper, we have successfully introduced for the first time the time Petri nets model for study and analyzing the occurrence sequence of an industrial incident with a case study on flaring system.

The system modeling allowed us to propose a way to present the occurrence probability of a failure using time Petri nets. Also, this model helps us to handle the human imperfection problem in monitoring industrial measurements. By using a time model having good properties as boundedness, reversibility and liveness, we were able to establish a preventive maintenance plan based on occurrences times of the studied incident scenarios. A recommendation to modernize

the knockout drum level indication was suggested by setting up a LT (level transmitter) connected to the control room with alarm if the indication exceeds the high level while keeping the LI (level indicator) on site. This modernization ensures a double redundancy for level indication, between LI and LT and between LT and LSH. And a redundancy for human surveillance with the involvement of the control room operator in the monitoring of the KOD level.

Although a significant research effort has been made to improve the knowledge about this phenomenon, more research may be required. The focus of this work was qualitative rather than quantitative, and as a future work we will use a quantitative model using stochastic Petri nets.

Part 2: Risk Based Availability Analysis of Gas Flares Systems Using Advanced Fault Tree and Stochastic Petri Net Formalisms

5.6 Introduction

Risk analysis has scored significant progress in the last two decades; however, accidents continue to happen in facilities at different risk levels. This leads to defining a concept of safety critical systems. A system could be classified as a safety critical system if its failures can cause injury/fatalities, significant damage to properties or the environment, and/or an important financial loss (Knight, 2002). Process systems in the oil and gas industry often witness accidents of significant losses. This justifies the importance allocated to study, supervise and measure the parameters of safety critical systems. Devastating accidents in process facilities such as the BP Texas city refinery explosion in 2005 (Ferdous et al., 2013; US Chemical Safety Board, 2007) and the Macondo well accident in 2010 (US Chemical Safety Board, 2014a, 2014b) prove that the era of safe production and processing is still distant and that the current methods of safety assessment require improvements. In this context, much research has been done to mend some methods widely used in the risk analysis field. Fault tree (Geffroy and Motet, 2002) is indeed one of these methods due to its capacity to translate a physical system to a clearly presented logical diagram.

FT models are the easiest and most used technique in dependability assessment (Bouissou et al., 2004; Talebberrouane and Lounis, 2016). It is well-suited in many engineering problems to identify the logic behind the undesired event, or at least conservative relationship between top event successes and failures, and plant damage states (Siu, 1994). FT has been emerged by Bell Telephone Laboratories in the early sixties; later many engineering disciplines adopted it, including aviation, medicine, nuclear and safety. FT is a deductive top-down method that aims to compute the occurrence's probability (P) of the top event as function of basic events' probabilities (X_i). The latter represent likelihood of components' failures and/or occurrence of random incidents (i.e natural catastrophe or power outage). Representing the probability of these random events by a constant value will lead certainly to a misjudgment of top event probability. On the other hand, FT is based on basic events' independency, which is not suited for majority of complex systems where some elements' dynamic behaviours are significant factors (i.e automatic start and stop pumps and backup units) and/or interdependencies are strong or critical

for the system analysis (i.e. intrinsic dependency or cascading dependency). In these circumstances, the need for formalisms, able to handle the limitations of conventional FT, becomes evident. Extensive discussion on limitations of the FT is provided by (Siu, 1994).

In the past few years, FTs have experienced a lot of improvements to overcome their weaknesses (Baig et al., 2013). In the literature, some work has successfully used hybridized fault trees to assess, reliability, availability, and safety of complex systems. Volkanovski (2009) successfully applied improved FTA using algorithms to assess power system reliability. In safety assessment, Khakzad (2013) used the bow-tie (BT) structure and mapped a Bayesian network based on it, while proposing a procedure for mapping and dealing with dependencies and data updating, with the help of BN properties. Other work dealt with the comparison of different techniques used in accident modelling contexts. Sunanda (2015) compared FT, FMEA and PNs for hazard analysis of a safety critical system, with a railroad crossing junction as a case study, and conclude that generalized stochastic Petri nets (GSPN) have the ability to identify the failure occurrences more specifically than the other formalisms. Nivolianitou (2004), compared FT, ET and PN for accident scenario analysis of an ammonia release from an ammonia storage plant and come out with a conclusion that PNs offer better time/duration depiction of an accident development, while FTs present better the primary events that may affect them.

GSPN have been widely used to study workflow systems. Workflow systems, by their nature, are dynamic and complex systems subject to timing constraints. They deal with; external events, simultaneous actions, sequential relationship and concurrency (Chuang et al., 2002). GSPN brought a significant improvement to this engineering area over existing techniques such as Markov process. The latter was one of the main performance analysis techniques for workflow systems (Chuang et al., 2002), but the state space explosion of Markov process limited its ability to analyze complex and big-scale systems. Van Der Aalst (1998) proclaimed that there are at least three good reasons for selecting a Petri-net-based workflow management system, which are: formal semantics despite the graphical nature, state-based instead of event-based and abundance of analysis techniques. Petri nets, as a mathematic tool, allow deterministic and stochastic performance measures (i.e. production rate or bottleneck workstations estimation in production systems). In process automation, Petri nets are known as an effective tool for modelling, control, and performance analysis of manufacturing systems. They can handle situations that cannot be adequately modeled by queuing theory (i.e. deadlock, conflict, and

boundedness), and they avoid the trial and error approach of simulation (DiCesare and Desrochers, 2012). Petri nets, and more specifically GSPN, proved that they can be used for system requirement specifications (SRS) through programmable logic controllers (PLCs). Compared to the Ladder logic, which is known to be very difficult to debug and modify, Petri nets based sequence controllers are easy to design, implement and maintain (Zhou and Zurawski, 1995). In process systems, resources sharing (i.e spare parts or repairers sharing) are important dynamic characteristic that GSPN can clearly model even with different priority levels. It represents one of the powerful points making this formalism suitable for systems with complex behaviour (i.e workflow systems or safety instrumented systems) compared to FTDMP or other formalisms. According to IEC 61508, GSPN with predicates have been proven to be a very efficient way of modelling dynamic systems for the following reasons (IEC 61508-6, 2010):

- They are easy to handle graphically;
- The size of the models increases linearly according to the number of components to be modelled;
- They are very flexible and allow modelling almost all types of constraints;
- They are a perfect support for Monte-Carlo simulation (for more details see section B6 of IEC 61508-7).

In this part, we used a hybrid formalism, called the Fault Tree Driven Markov Process (FTDMP), to examine its capacities and compare them to stochastic Petri nets modelling. The present research intends to reveal the limitations of FTDMP and demonstrates how the latter can influence the availability analysis results. A methodology, step by step, to solve these limitations using GSPN is provided in details.

A brief description of the FTDMP is presented in section 2. An overview of Petri Nets, Generalised Stochastic Petri Nets (GSPN) and Monte Carlo Simulation, a description of the mapping process from the FT structure to PN modelling is presented in Section 3. The accident scenario is described in section 4 along with the step by step modelling approach applied to the case study using both methods. Results and discussions are presented in section 5 with additional data supplied by PN modelling that provides another perspective to the availability modelling. Section 6 is devoted to the conclusions and potential ways to improve the present work.

5.7 Brief description of FTDMP

Fault Tree Driven Markov Processes (FTDMP) formalism was partially introduced by Signoret (1986), when he presented his approach as a “directed graphs approach”. This idea was subsequently developed to enable the analyst to combine conventional fault trees and Markov models in a new way (Cacheux et al., 2013). Markov process, as a stochastic process time dependent, integrates the dynamism property in the static model of the conventional FT and makes it possible to model and study distinctive elements as the case of repairable components where the component passes by three phases; operational, failed and under repair phase, taking in consideration the complete/partial shutdown as a consequence of the failure or requirement of the repair procedure. Another example of distinctive elements is the component periodically tested, more details about this category of components are given in section 2 where it shows the modelling capacity improvement of the FT due to Markov process introduction.

Trying to model a complex system using only the Markov process will lead to a huge model with combinational problems (de Souza e Silva and Mejia Ochoa, 1992; IEC 61508-6, 2010). This explains the reason for directly using regression for Markov process. In FTDMP, each basic event is associated to a Markov process given the behaviour and phases during which the component is operational, failing, experiencing a diagnostic review or a repair and so on. It also provides information on component’s availability in each phase of its life cycle. FTDMP and multi-phases Markov process approaches are described in annexes B4 and B5 of the IEC 61508-6 (2010).

In FTDMP, the Markov models generate the behaviour of basic events as function of time which results in real time FT in a mechanized manner. While preserving the use of the deductive logic to clearly identify the events’ sequence leading to the specific top event, and offers interesting mathematical properties. An application of the FTDMP formalism for unavailability calculations is provided in clause 8 of the standard ISO/TR 12489 (2013) and details about the multi-phases Markov process are also provided on the clause 9 of the same standard.

In the literature, some work has implemented the exponential distribution to the basic events. Dutuit and Rauzy (1997) successfully used the exponential distribution on basic events coupled with binary decision diagrams (BDD) to perform the Monte-Carlo simulation and study the uncertainty propagation through the tree. Bucci (2008) implemented Markov models in

specific parts (sub-systems) of dynamic fault tree (DFT) and dynamic event tree (DET) to enhance their dynamic modelling capacities. The approach was illustrated by using a water level control system. Bouissou (2002) presented formalism similar to the main principle of FTDMP, called Boolean logic driven Markov process (BDMP). This formalism uses the concept of “triggered Markov process” time dependant commanding the state of targeted logic gates via dotted arrows on the FT. In this way, the FT becomes dynamic without the introduction of new gates as it is the case of the well-known dynamic FT. Cacheux (2013) assessed the availability using FTDMP formalism included in the software GRIF, without presenting the Markov models behind it. It was illustrated that a lack of relevant models usually leads to an overestimation of reliability performances. Srinivasa (2016) applied the FTDMP method to estimate the probability of failure on demand (PFD) of the Indian tsunami early warning system then assesses and analyzes its reliability based on Safety integrity level (SIL) classification. (Signoret, 2007) explained the principal of FTDMP formalism and illustrated it by a multi-phases Markov model. For more details about use of FTDMP method, readers can refer to this last cited paper.

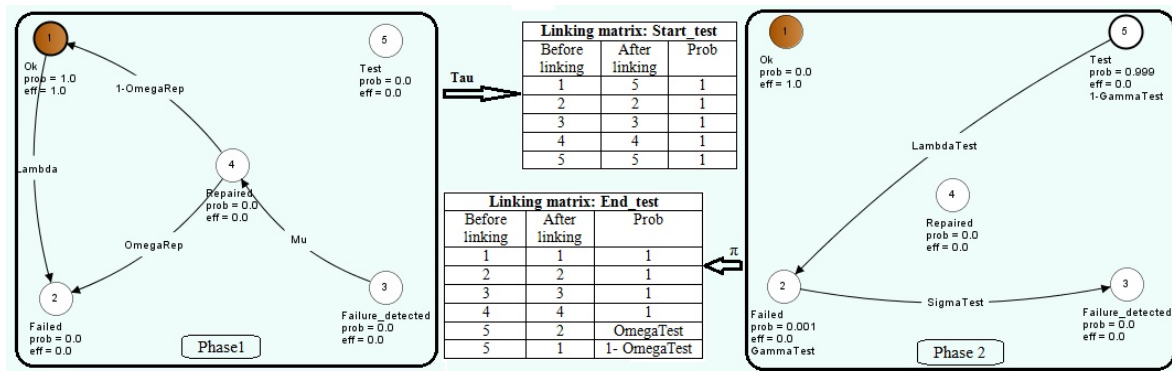


Figure 5.8 Markov model of periodically tested component.

To illustrate the power of this method, Figure 5.8 provides an example of multi-phase Markov modelling developed for a repairable component periodically tested (i.e. periodic maintenance). The parameters lambda, lambda-Test and Mu represent failure, failure during PM and repair rates successively. Omega and sigma represent probabilities of maintenance error and the probability of failure detection respectively. States in brown represent the situation when a component is available and parameter “prob” represents the initial probability to be in the corresponding state (i.e. gamma-test which represents failure due to starting PM). Phase 1 represents the functional phase and phase 2 represents the PM phase. This Markov model can be

embedded in a basic event using a dedicated tool, the Boolean package of Grif software. More details about this software package are given in (TOTAL GRIF-Workshop, 2016).

5.8 Overview of PNs and GSPN

Petri networks (PNs) were developed in 1962 by Carl Adam Petri, as a new mathematical model to connect events and conditions (David and Alla, 2010). The PNs were applied first in the fields of computer science and automatic control, work on PN modelling up until 1989 are listed in detail in the work of Murata (1989).

Definition1 (Ordinary Petri net). A Petri net is a quintuple,

$N = \langle P, T, Pre, Post, M_0 \rangle$ where:

$P = \{p_1, p_2, \dots, p_m\}$ is a finite set of places,

$T = \{t_1, t_2, \dots, t_m\}$ is a finite set of transitions,

$Pre: P \times T$ is the “receding places” application,

$Post: P \times T$ is the “following places” application,

$M_0 : P \rightarrow \{0, 1, 2, \dots\}$ is the initial marking.

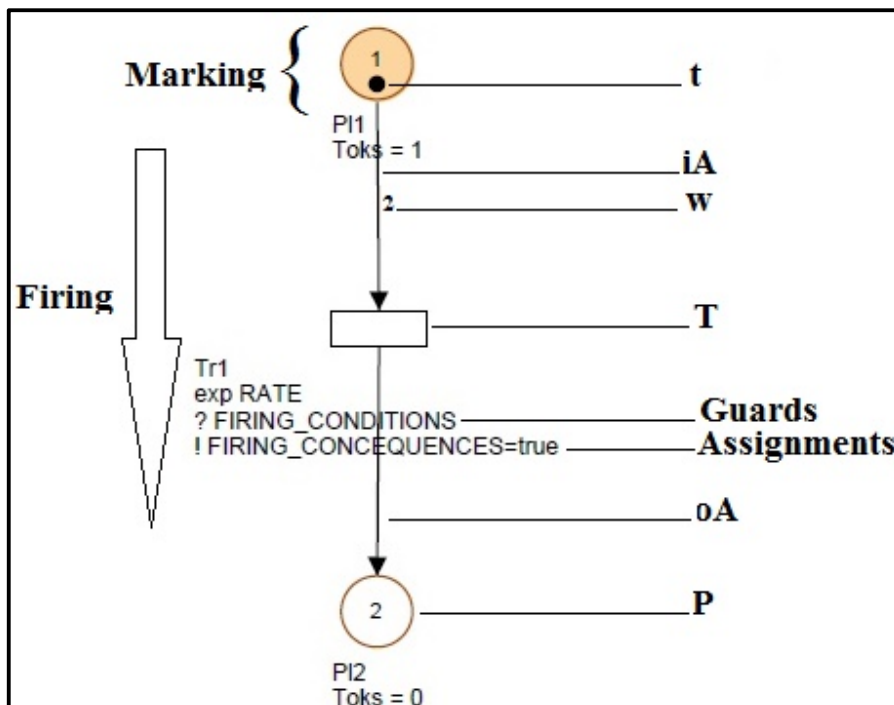


Figure 5.9 Glossary of PN notations.

A Petri Net is a weighted bipartite graph (P, T, A, w) (Cassandras and Lafortune, 2009) with two functional parts. Figure 2 shows the static part represented by places (P), transitions (T) and oriented arcs that connect places to transitions (input arcs, iA) and transitions to places (output arcs, oA). w represents the weight function on the arcs. The dynamic part is represented by movements of tokens (t) following firing transitions (tokens' migration from input places to output places). The marking represents the tokens' number in a place. A stochastic Petri Net (SPN) (Dutuit et al., 1997) also has non-deterministic firing delays associated with transitions.

Definition2 (Stochastic Petri net). A Stochastic Petri net Z is defined as a six-tuple (P, T, I, O, m, f) , where

$P = \{p_1, p_2, \dots, p_n\}$, $n > 0$, and is a finite set of places;

$T = \{t_1, t_2, \dots, t_s\}$, $s > 0$, and is a finite set of transitions.

$I: P \times T \rightarrow \mathbb{N}$ and is an input function that defines the set of directed arcs from P to T;

$O: P \times T \rightarrow \mathbb{N}$ and is an output function that define the set of directed arcs from T to P;

$m: P \rightarrow \mathbb{N}$ and is a marking whose i th component represents the number of tokens in the i th place. An initial marking is denoted by m_0 . $\mathbb{N} = \{0, 1, 2, \dots\}$.

$f: T \rightarrow \mathbb{R}^+$ and is a firing rate whose i th component represents the firing rate of the i^* transition, where \mathbb{R}^+ is the set of all positive real number.

In a stochastic Petri net, when a transition is enabled at marking m , the tokens remain in input places during the firing time delay. At the end of the firing time, the tokens are moved from input places to output places, the number of tokens in the flow depends on the input and output functions (Zhou et al., 1990).

Later, this was developed and extended to include generalised Stochastic Petri Nets (GSPN), In fact it keeps the same meaning of SPN; in addition two notations are introduced (Sunanda and Seetharamaiah, 2015), immediate transitions (no delay required for firing transition) and inhibitor arcs (the absence of tokens enables transition, unlike the conventional arcs). PNs are considered as formalism for the description of concurrency and synchronisation (Bause, 2002). Observing the graphical presentation of a simple SPN model, it looks like the data flow diagram (DFD). Moreover, SPN goes further due to tokens' movements which simulate dynamic and concurrent activities (Nivolianitou et al., 2004). In this article, the authors used GSPN with predicates and assertions. The predicates or guards as defined by IEC 61508-6 (2010) are any formula which may be true or false, validating transitions, as is shown in Figure

2. Assignments are the mathematical variables that receive predefined changes (i.e. incrementation, turns to true or false, and so on) as firing consequences. The behaviour of these mathematical variables can be traced and used as outcomes of PN modelling by using instantaneous, average by time interval, transition firing frequencies or mean sojourn time in a place.

To deal efficiently with systems involving stochastic and deterministic events a simulation approach is used here. Monte Carlo simulation is considered an effective tool dedicated to these situations. It is based on the use of random numbers to animate system behaviour. According to the standard IEC 61508-6 (2010), PN formalism provides a very efficient support for performing Monte Carlo simulation. The latter produces a large statistical sample from which statistical results are obtained. We provided below some basic statistics, which allowed the calculation of the average (\bar{X}), variance (σ^2) and confidence interval of the sample (X_i) which has been simulated:

$$\bar{X} = \sum_i^n X_i / n \quad (1)$$

$$\sigma^2 = \sum_i^n (X_i - \bar{X})^2 / n \quad (2)$$

$$\text{Confidence interval} = [\bar{X} - E. (\sigma / \sqrt{n}), \bar{X} + E. (\sigma / \sqrt{n})] \quad (3)$$

where $E = 1.6449$ for confidence = 90%

The PN modelling approach consists of mapping a FT to a PN model, where a basic event can be modeled as sub-systems structurally separated (i.e as shown in figure 8 and 9 of the application). The logic gates were substituted by Boolean variables that can be used as guards for the transitions.

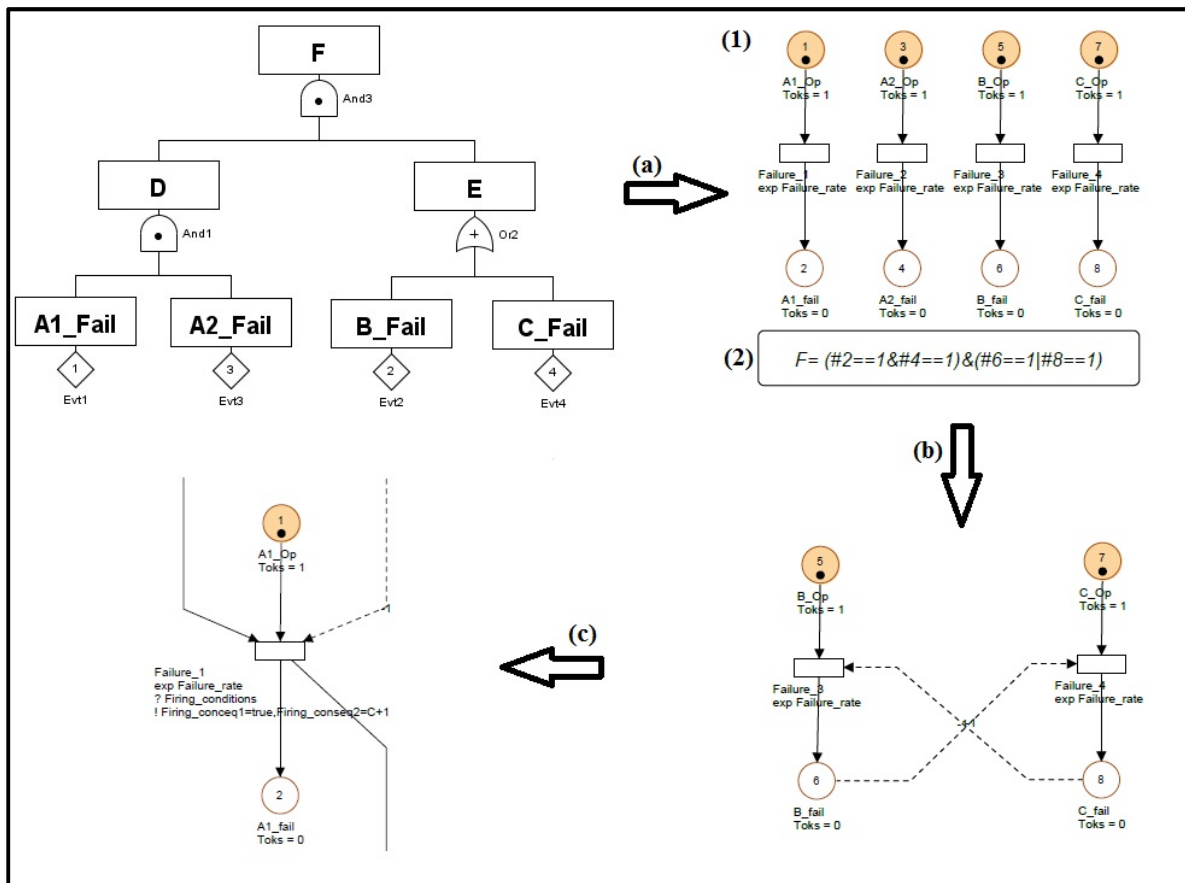


Figure 5.10 Mapping approach from FT to GSPN with predicates.

Figure 5.10 presents the mapping approach using three steps. The first step (a) is a direct mapping of the FT structure to (1) simple models for components' failure and generation of (2) the Boolean variables representing gates' sequence as shown on FT. At (b), the second step, consideration begins of simple dependencies among components as concomitance, mutually exclusive and so on using simple and inhibitor arcs or even networks. At (c), the third step, there is an integration of guards and assignments for complex dependencies or complex behaviour. After the modelling stage, the validation stage starts using step by step simulation and model adjustments.

5.9 Application Of The Formalisms

5.9.1 Problem statement

The chosen study is of a flare system incident reported in The John Zink Hamworthy Combustion Handbook (Baukal Jr, 2012). The filling of a knockout-drum (KOD) resulting in

high level occurs randomly during normal operation or when an excess liquid situation causes by emergency cases on the process as emergency shutdown (ESD). After detection of the high level in the KO drum, sensors order the pumps to start. This either fails to start or run successfully. The possible accident scenarios begin due to component's failure of the flare draining system coupled with an excess introduction of liquid to the system. If the draining capacity is surpassed, the liquid phase reaches the combustion zone and falls out from the top of the flare stack. Individual failure modes differing from one element to another while influencing the whole system performance are considered. The simplified P&ID of the flare system is provided in Figure 5.11 below.

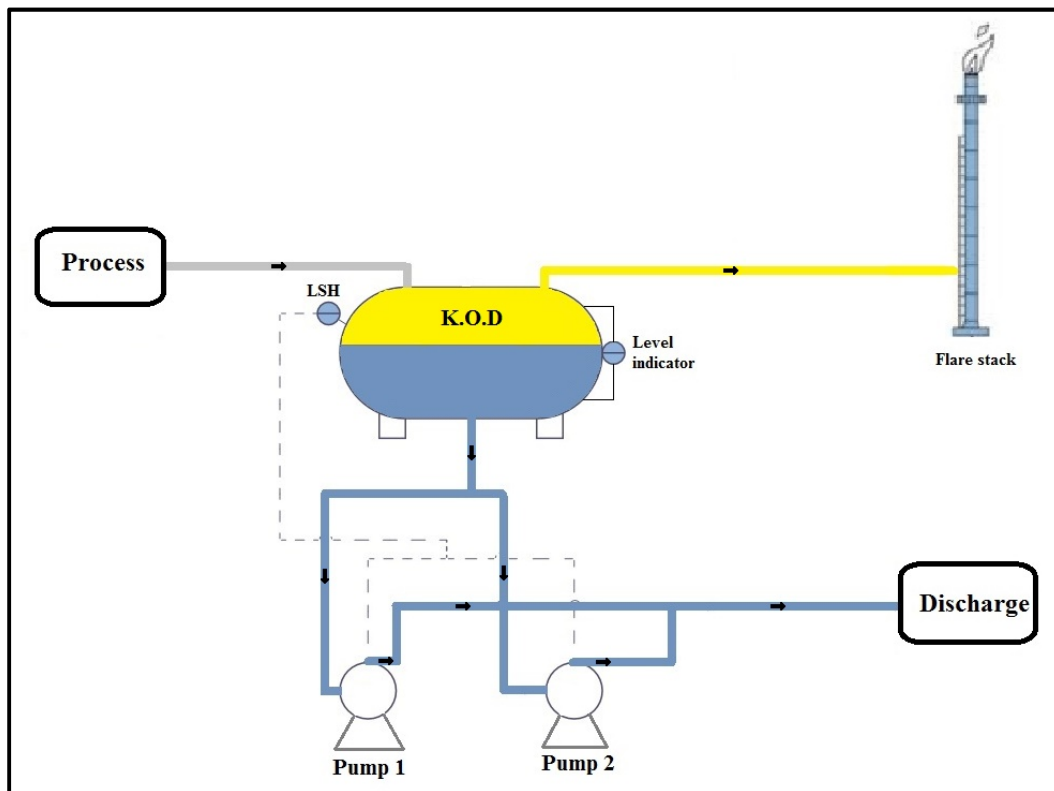


Figure 5.11 A simplified P&ID of the flare system.

5.9.2 FTDMMP Model

An investigation based on expert knowledge and experience feedback has been envisaged to determinate the possible accident scenarios leading to this overflowing and to assess the effectiveness of the various safety barriers. The investigation results are provided for the FT structure shown in Figure 5 below.

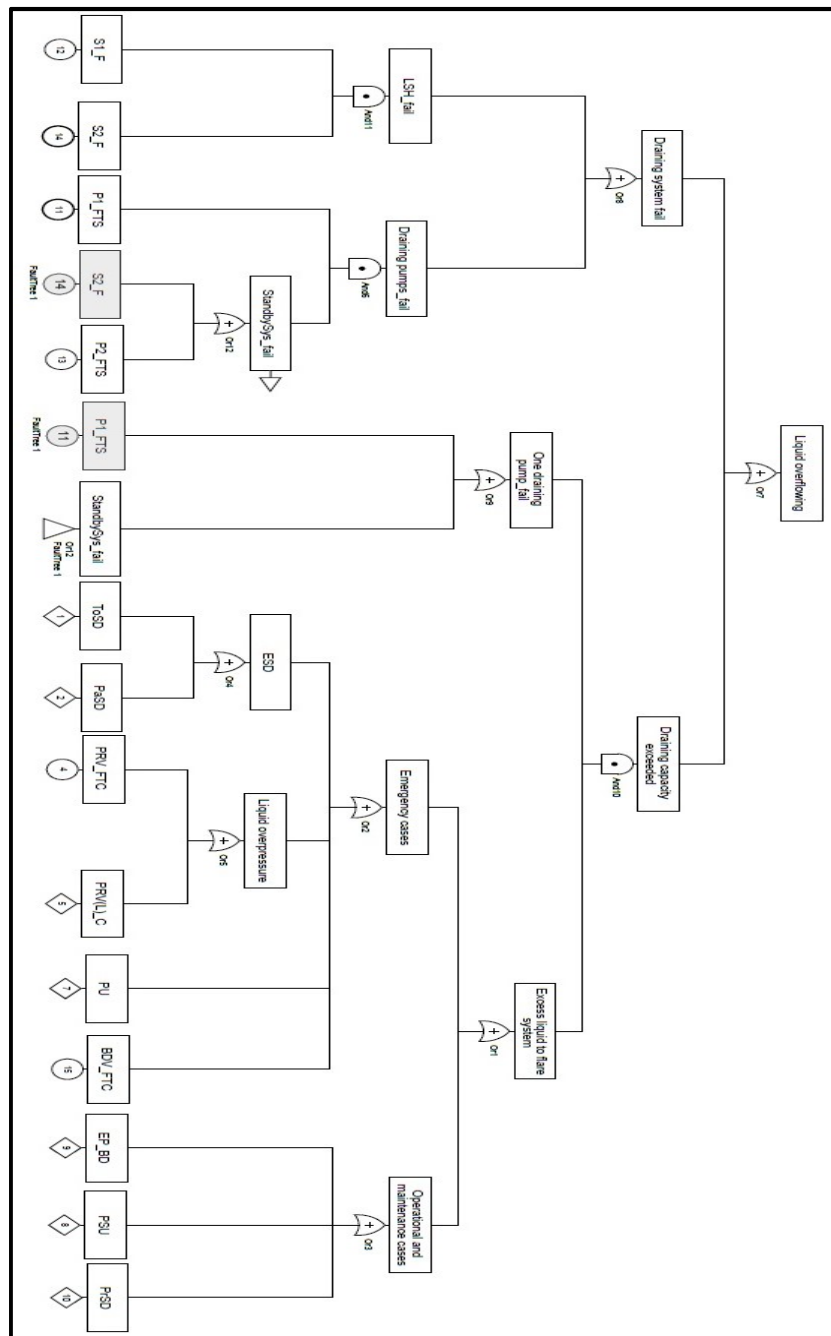


Figure 5.12 Fault tree of the flare liquid overflowing.

The accident consequences are dependent on the success or failures of the safety barriers. An event tree (ET) is provided in Figure 6 to present these consequences. In this study, we consider the KO drum level indicator (LI) as a safety barrier due to the fact that it does not

interact with the automatic drainage system. Therefore, the field operator, who should also visually inspect the flare flame, should carry out an LI reading periodically. The field operator’s inspection is also a safety barrier for this system.

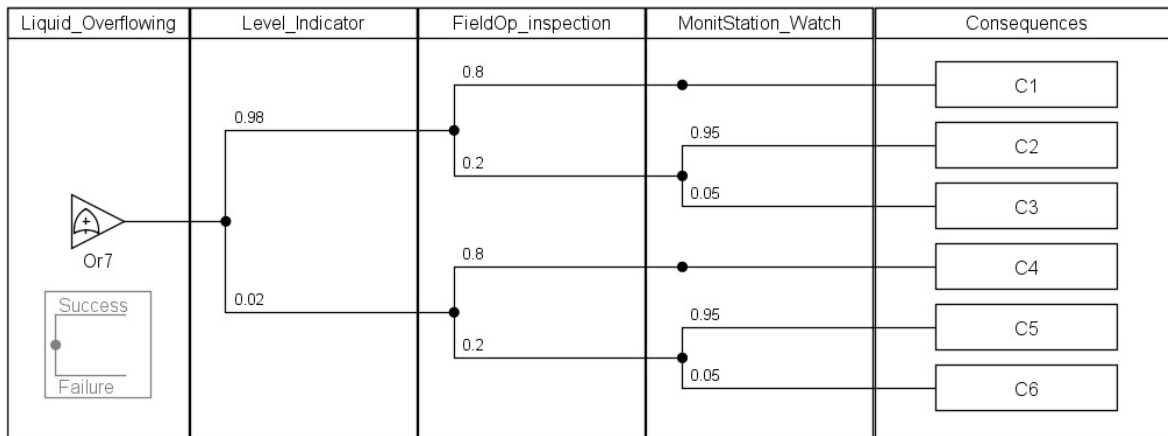


Figure 5.13 Event tree of the flare liquid overflowing.

Table 5.8 Accident consequences.

Consequences		Symbol
Severity	Description	
Minor	Controlled situation, intervention to drain the KOD	C1
Medium	Flammable liquid overflowing with low damage (C4) to moderate damage (C2, C5)	C2, C4, C5
Major	Flammable liquid overflowing, pool fire and high damage	C3, C6

The accident initiating events are organized in two categories. Basic events cover failures of simple components (i.e. sensors and valves), and are listed in table 5.9 with their symbols and failure probabilities (OREDA, 2002). Parameters shown in table 2 are defined above in section 2 and the same notation was adopted for both Markov and PN modelling.

Table 5.9 Basic events and their periodic maintenance parameters.

Basic Event	Symbol	Lambda	Mu	Lambda Test	Gamma Test	Sigma Test	Omega Test	Omega Rep
Pressure relief valve fails to close (liquid)	PRV_FTC	5.70E-07	0.1667	5.70E-07	0.001	0.8	0.001	0.001
Blow-down valve fails to close	BDV_FTC	6.90E-07	0.4348	6.90E-07	0.01	0.9	0.01	0.01
Sensor1 fails	S1_F	4.60E-07	0.1667	4.60E-07	0.001	0.99	0.001	0.01
Sensor2 fails	S2_F	4.60E-07	0.1667	4.60E-07	0.001	0.99	0.001	0.01

For all components cited in Table 5.9, the same parameters are applied concerning the periodic maintenance. It is scheduled for once every five years, with duration of four hours for each component. It is worth noting that components are considered unavailable during the preventive maintenance phase. The draining pumps are considered as repairable components including failure to start on demand ($\Gamma=0.01$), failure rate ($\lambda=2,28E-06$) and repair rate ($\mu= 0.1667$). The draining pumps' behaviour is represented by the Markov model in Figure 7. These models are embedded in the fault tree in Figure 4 using a Boolean package of Grif software.

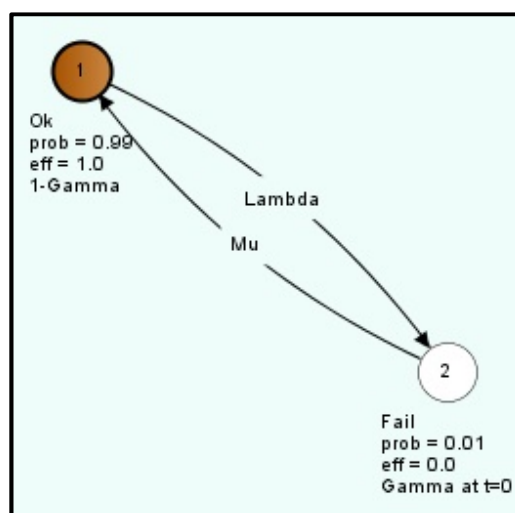


Figure 5.14 Example of Markov model to be embedded in the fault tree.

Table 5.10 Elementary events and their occurrence rates (exponential distribution).

Elementary event	Symbol	Occurrences' rates
Total plant SD	ToSD	1.9E-5
Partial Plant SD	PaSD	2.85E-5
Opening of a PRV (liquid)	PRV_C	3.8E-5
Plant upsets	PU	5.7E-5
Equipment and piping blow-down	EP_BD	2.28E-5
Plant start-up	PSU	3.26E-5
Programmable shutdown	PrSD	2.28E-5

A fault tree's elementary events cover plant upsets, shutdown (SD), start-up and so on and are listed in Table 5.10 above with their symbols and occurrence rates according to experts' knowledge. It shown that plant upsets are the most frequent event among them. After processing the FT calculations, it demonstrated that a plant upsets leading to excess liquid toward flare system coupled with dormant failure of sensor 2 present the most probable sequence (MPS) leading to the FT top event.

5.9.3 Stochastic Petri Nets modelling

The structural organisation presented by FT has been maintained for the Stochastic Petri Nets (SPN) modelling and the three steps were followed as described in section 2. Two parameters describing the system's normal operation have been taken in account, the KOD normal filling rate (0.0417 h^{-1}) and the emptying duration (4 h). To illustrate the resources sharing property, a repairers' team sharing is shown in places 3 and 6 of Figure 8. To avoid more complexity, it was assumed that the draining pumps cannot fail at standby states.

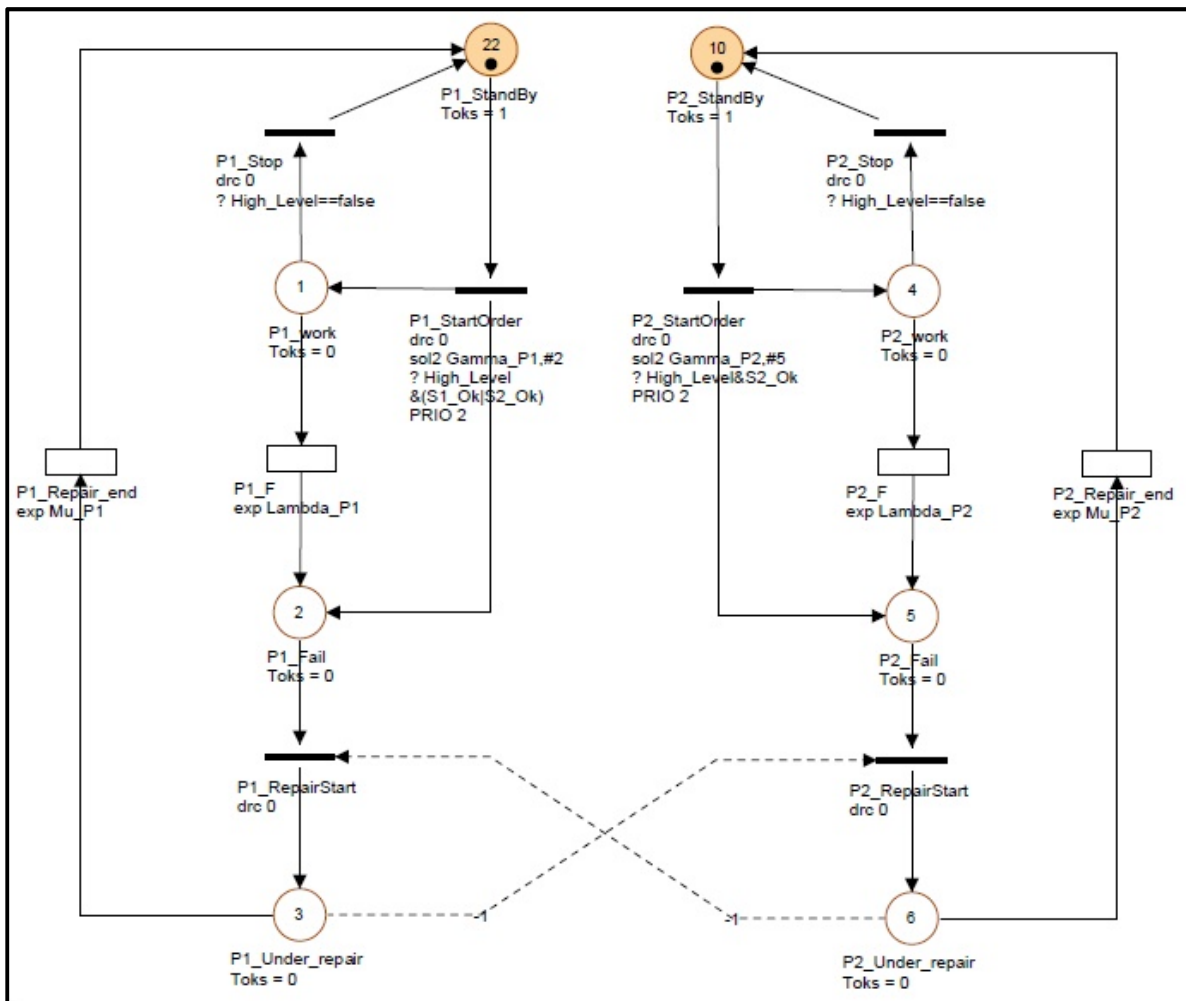


Figure 5.15 PN of Draining pumps.

Figure 5.15 below demonstrates the sensor 1 (S1) modelling using PN. The same model structure is used for modelling sensor 2 (S2), the blow-down valve (BDV) and the pressure relief valve (PRV).

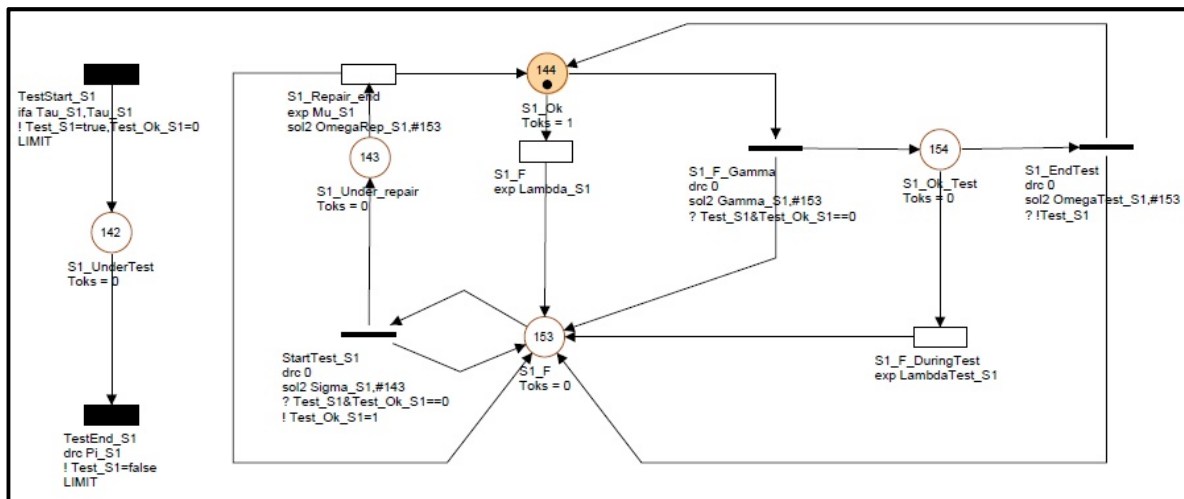


Figure 5.16 Sensor 1 behaviour modelling using PN.

In figure 5.16, the structural separation of schedule preventive maintenance modelling (on the left hand) and the component’s behaviour (on the right hand) is done while keeping the latter as one block for an easier trackability. Component’s availability is represented by a Boolean variable “S1_Avail” which is true when place 144 has one token (i.e #144==1). Component “S1” can experiences a dormant failure, so the token moves from place 144 to place 153 (#153==1) before PM. At a scheduled time, PM has the probability “Sigma” to detect this failure and correctly repair at probability “1-OmegaRep”. If it is not repaired, the component is still in its failure state until an accident occurs or until the next scheduled PM. Even if a component was operational before PM, starting PM at stage of disconnection or disassembly can causes component’s failure, or it can fails during PM. Similar to the repair phase, reconfiguration or reassembly after the PM phase can also causes failure, and this lasts until an accident occurs or until the next scheduled PM. It is worth noting that this model presents high flexibility. In an example, if a component is available during PM, a simple change can be made in the availability variable to be $S1_Avail=(\#144==1|\#154==1)$ without any changes of the model. Many other changes can be applied without any change of the model structure.

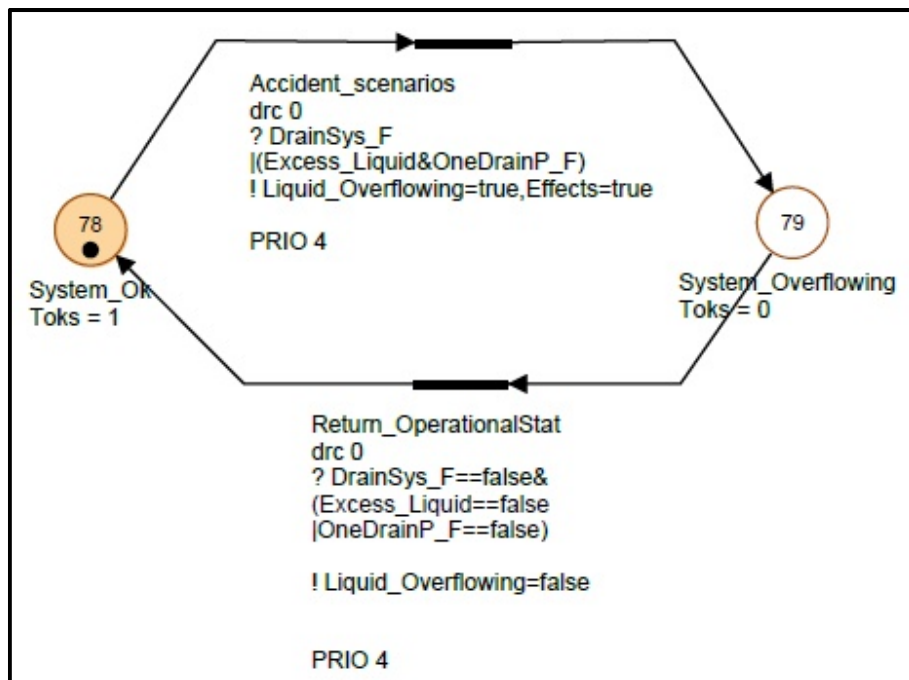


Figure 5.17 PN modelling of the top event.

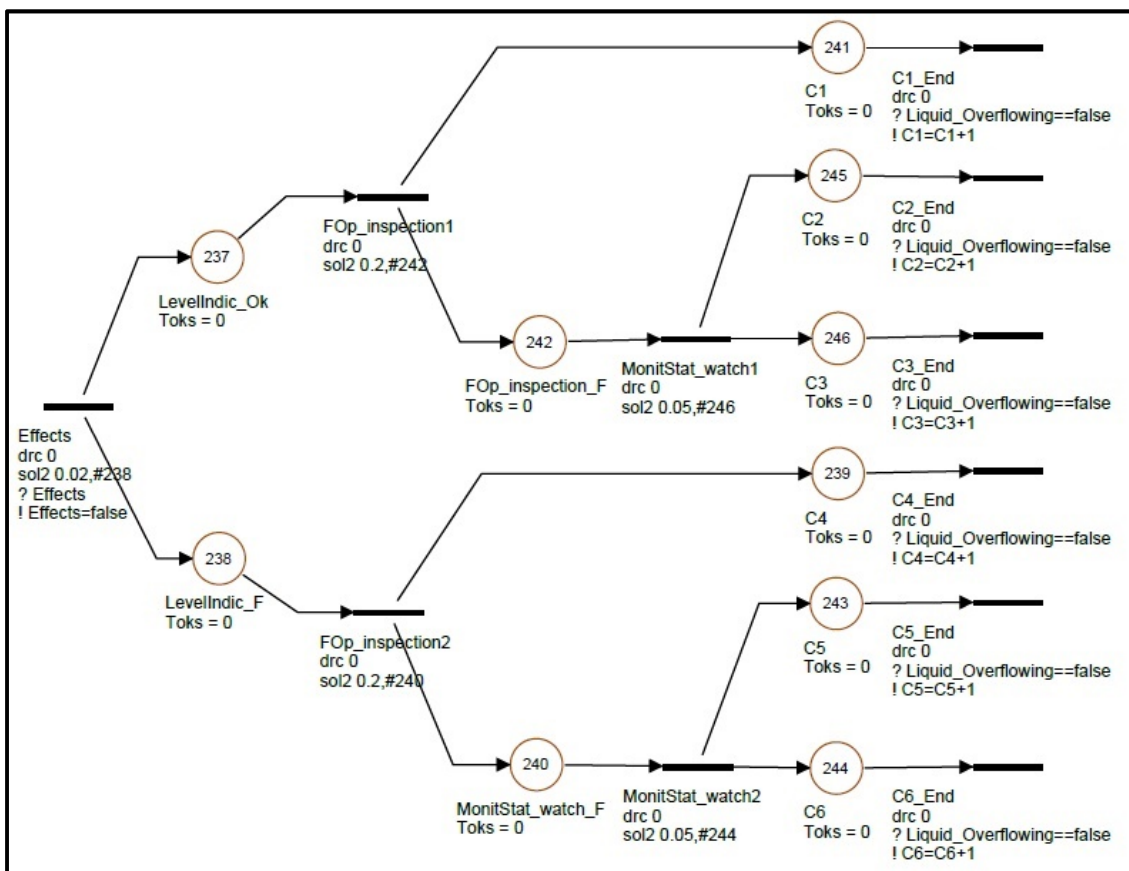


Figure 5.18 PN modelling of top event consequences.

The knockout drum filling is the critical event that initiates dynamic movement of the whole system; the filling event is modeled in normal situation and abnormal (excess liquid) situation. Both of the situations emit a start order to the draining pumps through turning on the high level Boolean variable (i.e. `!High_level==true`). After modelling the whole system's interactions, we can model the top event and its consequences a similar way to the event tree structure. Figures 5.17 and 5.18 show these two models respectively.

5.10 Results & Discussion

To facilitate comparison between the two formalisms, results are provided in tables.

Table 5.11 Average event occurrence frequency for 30 years of service.

Top event & consequences	Average frequency of occurrence (1/h)	
	FTDMP	GSPN
Top event:		
Liquid overflowing	2.54E-5	2.77E-5
Consequences:		
Minor	1.99E-5	2.13E-5
Medium	5.22E-6	5.59E-6
High	2.54E-7	2.82E-7

Results in Table 5.11 show that FTDMP modelling provides occurrence probabilities by approximately more than 90% compared to those using GSPN. These differences in frequencies are due to the limited FTDMP modelling capacities. In fact, FTDMP considers the pumps as running continuously until it fails, which does not correspond to the real case. On the other hand, GSPN modelling takes into account the intermittent and conditional sequences as mentioned in section 4. The differences in frequency are minimized thanks to the low failure rates.

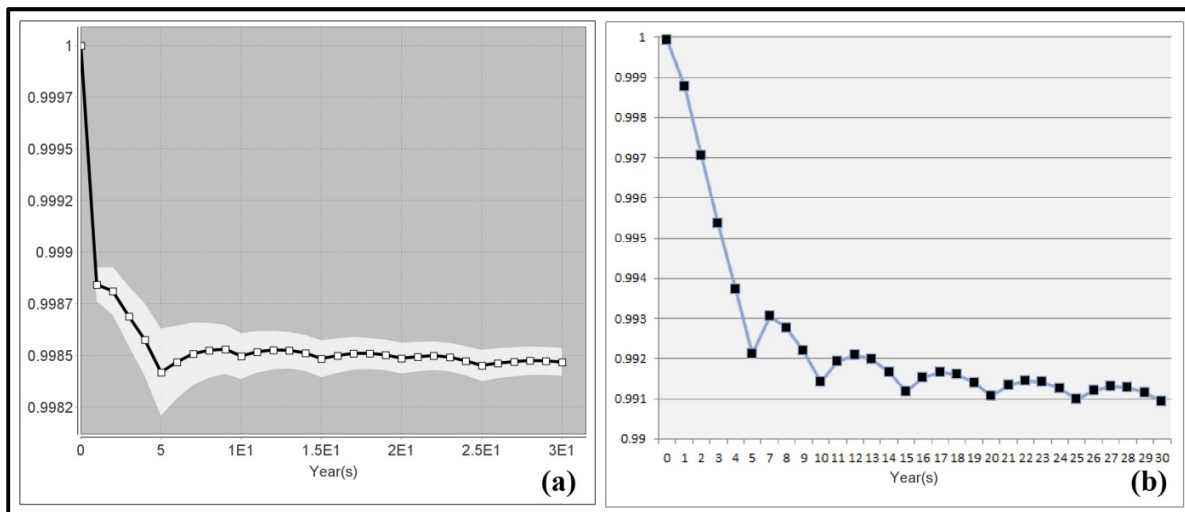


Figure 5.19 Mean availability of flare system given by (a) GSPN (b) FTDMP [30 years of service].

In Figure 5.19, both the FTDMP and GSPN modelling curves show a periodicity of five years. This periodicity corresponds to the time between periodic maintenance cycles for four components (S1, S2, BDV and PRV). In the first five years of service, the FTDMP's curve does not present any changes in the decreasing trend contrary to the PN's curve. This variance between availability curves is due to the fact that PN models the dependencies in an operating normal mode between a high level occurrence, sensor excitation and pumps starting, which FTDMP cannot model. After the first five years, these effects are hidden by the occurrence of other failures.

PN modelling shows that preventive maintenance does not bring a significant improvement in terms of availability after the second cycle. However, BDMP notes continuity of constant cyclic improvement after the third cycle, which does not correspond to the process system reality. This variance between PN and FTDMP is due to the fact that the first can model the system behaviour in its totality, including the operational and failure processes, which FTDMP cannot model. Also, FTDMP cannot model the failure on demand and standby state. Some selected additional data given by GSPN are shown in Table 5.12 below.

Table 5.12 Selected additional frequencies given by GSPN at 90% confidence interval

Outcome data	($\mu \pm \sigma$)
Frequency per 30 years:	
High level	(9396 \pm 1.4)
Normal high level	(9338 \pm 1.4)
Excess liquid high level	(58 \pm 0.1)
P1 kick off	(9140 \pm 1.4)
P1 fails to start	(92 \pm 0.02)
P1 fails (at running phase)	(0,075 \pm 0.0043)
Time (h) for 30 years' service:	
P1 duration function	(36623 \pm 6.5)
C1 first occurrence	(55267 \pm 773)
C2 first occurrence	(105710 \pm 152)

The additional information retrieved by PN modelling compared to BT is given in Table 5.12, and this provides a new perspective on event frequencies and durations. This kind of analysis can be taken into consideration at the design phase, revamping of projects or a decision to provide redundant equipments. A redundant equipment can be added to the model without any structural changes to easily provide update outcome data.

5.11 Conclusions

It is demonstrated in this research how to use FTDMP and GSPN with predicates for availability modelling of safety critical systems. This systems are dynamic, having complex behaviour involving repairable components periodically tested, failure to start, random occurrences, a standby state, and so on. It is worth noting that the FTDMP method has shown the ability to describe accident scenarios due to its ability to hide the Markov process behind FT. Beyond this capacity, it also provides interesting qualitative results showing the most probable sequence (MPS) that leads to the top event. It is also observed that this method is unable of handling complex interdependencies and resource sharing as is done using PN modelling. PN modelling provides complete dynamic system simulation; it also allows the modelling of a complex system in modular fashion into structurally separated sub-systems. Mathematical

variables through guards and assignments insure the relations between sub-systems. The modular approach enables more traceability while avoiding huge and complex models.

The GSPN with predicates is a high level modelling formalism and shows a superior modelling capacity compared to FTDMP in providing reliable results and supplementary outcomes in both operational and failure phases. Additionally, it deals with complex interdependencies of parallelism, concurrency and synchronization, which are of great significance for accident modelling.

References

- Baig, A.A., Ruzli, R., Buang, A.B., 2013. Reliability Analysis Using Fault Tree Analysis: A Review. *Int. J. Chem. Eng. Appl.* 4, 169–173. doi:10.7763/IJCEA.2013.V4.287
- Barkaoui, K. and Peyre, J.F.P. 1996. On Liveness and Controlled Siphons in Petri Nets. *Proc. of 17th International Conference on Application and Theory of Petri nets*, Osaka, Japan.
- Baukal Jr, C.E., 2012. *The John Zink Hamworthy Combustion Handbook: Volume 1- Fundamentals*. CRC Press, Boca Raton, FL 33487, USA.
- Bause, F., 2002. *Stochastic Petri nets: An introduction to the theory*, Vieweg+Teubner Verlag, ISBN 3528155353.
- Benani, F. Z., Sekhri, L and Haffaf, H. 2014. Supervision Architecture Design for Programmer Logical Controller including Crash Mode. *International Journal of Information Technology and Computer Science (IJITCS)*, Vol. 6, No. 11, pp. 10-20.
- Berthomieu, B. and Vernadat, F. 2006. Time Petri Nets Analysis with TINA. Tool paper, In *Proceedings of 3rd Int. Conf. on The Quantitative Evaluation of Systems (QEST 2006)*, IEEE Computer Society.
- Boon, L. C., Danwei, W., Shai A. and Jing-Bing Z. 2010. Causality Assignment and Model Approximation for Hybrid Bond Graph: Fault Diagnosis Perspectives' *IEEE Transactions on Automaton, Science and Engineering*, vol. 7, No. 3, July, pp. 570-580.
- Bouissou, M., 2002. Boolean Logic Driven Markov Processes: A Powerful New Formalism for Specifying and Solving Very Large Markov Models. *PSAM 6*, June 2002 8. doi:10.1016/S0951-8320(03) 00143-1
- Bouissou, M., Dutuit, Y., Maillard, S.C., 2004. Reliability Analysis of a Dynamic Phased Mission System: Comparaison of two approaches, *MMR2004 long V2*, 1–19.
- Bucci, P., Kirschenbaum, J., Mangan, L.A., Aldemir, T., Smith, C., Wood, T., 2008. Construction of event-tree/fault-tree models from a Markov approach to dynamic system reliability. *Reliab. Eng. Syst. Saf.* 93, 1616–1627. doi:10.1016/j.res.2008.01.008
- Cacheux, P.J., Collas, S., Dutuit, Y., Folleau, C., Signoret, J.P., Thomas, P., 2013. Assessment of the expected number and frequency of failures of periodically tested systems. *Reliab. Eng. Syst. Saf.* 118, 61–70. doi:10.1016/j.res.2013.04.014
- Cassandras, C.G., Lafortune, S., 2009. *Introduction to discrete event systems*. Springer Science

& Business Media, New York, NY 10013, USA.

- Charles and Baukal, Jr. 2014. The John Zink Hamworthy Combustion Handbook, Second Edition: Vol. 3, pp. 263-264.
- Cheremisinoff, P.N. 2013. "Gas Flaring Practices" Scrivener Publishing, LLC, John Wiley and Sons, pp.73-74.
- Chuang, L.I.N., Yang, Q.U., Fengyuan, R.E.N., Marinescu, D.C., 2002. Performance Equivalent Analysis of Workflow Systems Based on Stochastic Petri Net Models, in: Han, Y., Tai, S., Wikarski, D. (Eds.), Engineering and Deployment of Cooperative Information Systems: First International Conference, EDCIS 2002. China. Springer Berlin Heidelberg, pp. 64–79. doi:10.1007/3-540-45785-2_5
- David, R., Alla, H., 2010. Discrete, continuous, and hybrid Petri nets. Springer Science & Business Media, New York, NY 10013, USA.
- De Souza e Silva, E., Mejia Ochoa, P., 1992. State Space Exploration in Markov Models. Perform. Eval. Rev. 20, 152–166.
- DiCesare, F., Desrochers, A.A., 2012. Modeling, control, and performance analysis of automated manufacturing systems using Petri nets. Control Dyn. Syst. 47, 121–172.
- Dutuit, Y., Châtelet, E., Signoret, J.P., Thomas, P., 1997. Dependability modelling and evaluation by using stochastic Petri nets: application to two test cases. Reliab. Eng. {&} Syst. Saf. 55, 117–124. doi:http://dx.doi.org/10.1016/S0951-8320(96)00108-1
- Dutuit, Y., Rauzy, A., 1997. Monte-Carlo Simulation to Propagate Uncertainties in Fault Trees Encoded by Means of Binary Decision Diagrams. 1st Int. Conf. Math. Methods Reliab. MMR'97, 1–8.
- Ferdous, R., Khan, F., Sadiq, R., Amyotte, P., Veitch, B., 2013. Analyzing system safety and risks under uncertainty using a bow-tie diagram: An innovative approach. Process Saf. Environ. Prot. 91, 1–18. doi:10.1016/j.psep.2011.08.010
- Geffroy, J.-C., Motet, G., 2002. Design of Dependable Computing Systems. doi:10.1007/978-94-015-9884-2
- Gouin and Ferrier, J.L., 1999. Modeling and Supervisory Control of Timed Automata. Journal Européen des Systèmes Automatisés, Vol. 33, No. 8-9, MSR'99.
- Hamzi, R., Innal, F., Bouda, M. A, and Chati, M. 2013. Performance Assessment of an Emergency Plan Using Petri Nets, Chemical Engineering transactions, Vol. 32.

- Hanžic, F., Jezernik, K and S. Cehner. Mechatronic Control System on a Finite-State Machine. *Automatika*, 54-1, 126–138.
- IEC 61508-6, 2010. Functional safety of electrical/electronic/programmable electronic safety related systems. International Electrotechnical Commission, Switzerland.
- ISO/TR 12489, 2013. Petroleum, petrochemical and natural gas industries -- Reliability modelling and calculation of safety systems, <http://www.iso.org/iso/home.html> (last checked Sep 10, 2016).
- Kalantarnia, M., Khan, F. and Hawboldt, K. 2010. Modeling of BP Texas City refinery accident using dynamic risk assessment approach. *Process Safety and Environmental Protection*.
- Keyner, A and Volovoin, V. 2010. Application of Petri nets to reliability prediction of occupant safety systems with partial detection and repair. *Reliability Engineering and System Safety*, Vol. 95, pp. 606–613.
- Khakzad, N., Khan, F., Amyotte, P., 2013. Dynamic safety analysis of process systems by mapping bow-tie into Bayesian network. *Process Saf. Environ. Prot.* 91, 46–53. doi:10.1016/j.psep.2012.01.005
- Knight, J., 2002. Safety Critical Systems: Challenges and Directions. *Int. Conf. Softw. Eng.* 547–550. doi:10.1109/ICSE.2002.1007998
- Murata, T., 1989. Petri nets: Properties, analysis and applications. *Proc. IEEE* 77, 541–580.
- Nivolianitou, Z.S., Leopoulos, V.N., Konstantinidou, M., 2004. Comparison of techniques for accident scenario analysis in hazardous systems. *J. Loss Prev. Process Ind.* 17, 467–475. doi:10.1016/j.jlp.2004.08.001
- OREDA, 2002. OREDA Offshore Reliability Data Handbook, 4th ed. DNV, Norway.
- Raiteri, D. C., 2005. The Conversion of Dynamic Fault Trees to Stochastic Petri Nets as a case of Graph Transformation. *Electronic Notes in Theoretical Computer Science*, Vol.127.
- Sekhri, L and Slimane, M. 2014. Modeling the Scheduling Problem of Identical Parallel Machines with Load Balancing by Time Petri Nets. *International Journal of Intelligent Systems and Applications (IJISA)*, Vol. 7, No. 4. pp. 42-48.
- Sekhri, L., Toguyéni, A. K. A., and Craye, E. (2004). Diagnosability of Automated Production Systems Using Petri Net Based Models, (IEEE SMC' 2004), International Conference on Systems, Man and Cybernetics. The Hague, Netherlands.
- Signoret, J.P., 1986. Etude probabiliste des systèmes périodiquement testés (in French), Report N° DGEP/SES/JPS/ co no. 86.009.

- Signoret, J.-P., 2007. High-Integrity Protection Systems (HIPS): Methods and Tools for Efficient Safety Integrity Levels Analysis and Calculations. Proc. Offshore Technol. Conf. 1–6. doi:10.2118/117173-ms
- Siu, N.O., 1994. Dynamic Approaches --- Issues and Methods: An Overview, in: Aldemir, T., Siu, N.O., Mosleh, A., Cacciabue, P.C., Göktepe, B.G. (Eds.), Reliability and Safety Assessment of Dynamic Process Systems. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 3–7. doi:10.1007/978-3-662-03041-7_1
- Srinivasa Kumar, T., Venkatesan, R.; Vedachalam, N.; Padmanabham, J.; Sundar, R., 2016. Assessment of the Reliability of the Indian Tsunami Early Warning System Marine Technology Society Journal, Volume 50, Number 3, 92–108.
- Sunanda, B.E., Seetharamaiah, P., 2015. Modeling of Safety-Critical Systems Using Petri Nets. ACM SIGSOFT Softw. Eng. Notes 40, 1–7. doi:10.1145/2693208.2693238
- Talebberrouane, M., Lounis, Z., 2016. Safety assessment of flare system by fault tree analysis Journal of Chemical Technology & Metallurgy . 2016, Vol. 51 Issue 2, p229-234.
- TOTAL GRIF-Workshop, 2016. SATODEV [WWW Document]. URL <http://grif-workshop.com/grif/tree-module> (accessed 3.3.16).
- US Chemical Safety Board, 2014a. Investigation Report Volume 1. Explosion And Fire At The Macondo Well. Report No. 2010-10-I-Os, US.
- US Chemical Safety Board, 2014b. Investigation Report Volume 2. Explosion And Fire At The Macondo Well. Report No. 2010-10-I-Os, USA.
- US Chemical Safety Board, 2007. Investigation Report Refinery Explosion and Fire BP Texas City, CSB. doi:REPORT No. 2005-04-I-TX, Texas City, TX, USA
- Van Der Aalst, W.M.P., 1998. the Application of Petri Nets To Workflow Management. J. Circuits, Syst. Comput. 8, 21–66. doi:10.1142/S0218126698000043
- Vernez, D., Buchs, D. and Pierrehumbert G. 2003. Perspectives in the use of colored Petri nets for risk analysis and accident modeling. Safety Science, Vol. 41, pp.445–463.
- Volkanovski, A., Čepin, M., Mavko, B., 2009. Application of the fault tree analysis for assessment of power system reliability. Reliab. Eng. Syst. Saf. 94, 1116–1127. doi:10.1016/j.ress.2009.01.004

- Zadakbar, O., Abbassi, R., Khan, F., Karimpour, K., Golshani, M and Vatani, A. 2011. Risk Analysis of Flare Flame-out Condition in a Gas Process Facility. *Oil & Gas Science and Technology – Rev. IFP Energies nouvelles*, Vol. 66, No. 3, pp. 521-530.
- Zadakbar, O., Khan, F and Imtiaz, S. 2014. Development of Economic Consequence Methodology for Process Risk Analysis, Society for Risk Analysis.
- Zhou, M., DiCesare, F., Guo, D., 1990. Modeling and performance analysis of a resource-sharing manufacturing system using stochastic Petri nets. *Proc. 5th IEEE Int. Symp. Intell. Control 1990* 1005–1010. doi:10.1109/ISIC.1990.128577
- Zhou, M., Zurawski, R., 1995. Introduction to Petri Nets in Flexible and Agile Automation, in: Zhou, M. (Ed.), *Petri Nets in Flexible and Agile Automation*. Springer US, Boston, MA, pp. 1–42. doi:10.1007/978-1-4615-2231-7_1

General Conclusion and future works

This thesis provided a critical analysis on some aspects where the quantitative risk assessment is not providing a curative solution or enough explanation of technical failures in the process industry. The topic of efficient risk assessment is vast and complex and out of any evidence about being in safe situation and continue operating. Process operations by nature are always attached to a risk somewhere and in different forms. Major accidents, are by definition, occurrences of massive bad events such as major emission, fire, or explosion. They have generally disastrous consequences on human being in present life and future. Understanding how accidents occur and what leads to each failure and each event with the analysis of the interconnections and interdependencies between phenomenon should be the first priority to undertake any risk assessment study. In this thesis, we have shown how each pillar of the probabilistic modelling works step by step to model the accident scenarios and highlight their particularities, advantages and weaknesses through several applications on process industry. The first research work involving the use of Petri nets modelling in risk assessment has been conducted using Time Petri Nets (TPN). During this stage, we noticed that some aspects need to be more accurately presented. After a deep review of the literature in the field, we realised that the most proper Petri nets formalism to analyze and imitate the reality of the accidental sequences is the Stochastic Petri nets (SPN). This research thesis as any research work has some limitations. It is worth noting that in this work, the technical failures and their mechanisms were considered in details, however the human failures were not fully considered, as they represent a separate and vast area of risk modelling.

Bow-tie analysis shows an ease of doing and understanding for non-specialist and non-mathematician but it can model just the system's static behaviour and limited for redundancy and common causes modelling which are better modelled with BN and PN. Compared to others, Bayesian Networks have pointed clarity to describe dependency between events by tracing CPTs and JPTs. Another strong point of BN is their power to manage the data updating and adapting. In other hand, BNs have shown low ability to model a sequence with synchronism, parallelism or conflict situations which is a power point for PNs. In the other hand, the BN graph indicates just ancestry and descendants relationship between nodes and we need the tables (CPTs) to understand the exact relationships. Petri Nets have been more explicit to show data on graph, but

SIMULATION OF INDUSTRIAL ACCIDENTS DUE TO UNCONTROLLED PRESSURES

it cannot be understood by a non-specialist and sometimes even the specialist should refer to the text to understand the graph. PN modelling offers plentiful results that we can exploit with different ways. PNs with its panoply of choice (autonomous, timed, stochastic, coloured, continued, hybrid and lending PN) offer to the specialists a strong capacity of modelling accident scenarios using parallelism, synchronism and conflicts which is close to the reality of facts enchainment.

The rise of modern systems' complexity, made Petri nets need to develop the capability of dealing with systems that we dispose of incomplete data. As a future work, the ongoing research paper aims to emerge a new modelling framework. This new tool aims to provide an imitation of some aspects of the Bayesian networks. Knowing that Bayesian network modelling is time independent and is founded on the conditional dependency between system's components, assuming some evidences. The relations are described in probabilistic way in CPTs. Another improvement will consist of data updating on each moment of inputs variation. The new formalism dispenses real time outputs that can effectively increase the accuracy of the predictive risk assessment.

« Simulation Of Industrial Accidents Due to Uncontrolled Pressures »

Abstract : In process industry, the potential risk is derived from one or more abnormal operations caused by components' failure, human error and/or other external factors. The causes are considered as root elements triggering a chain of events affecting the whole system. The series of these events are defined as industrial incidents. If they cause losses on human (i.e death or injuries) or damage on the infrastructures, industrial incidents will develop to industrial accidents. The simplest and the most used methods to describe and to analyze these accidents are the fault tree analysis (FTA) and the event tree analysis (ETA). They are getting this importance, because of their double aspects, qualitative and quantitative easy to implement and to discuss. On the other hand, Bayesian networks are good modelling tools to describe the conditional dependencies. However, they suffer limited modelling capacities that deal with the time dependency and complex behaviours of modern systems. More sophisticated methods exist, but they require advanced modelling skills and are not graphically explicit. One of these methods is the Petri Net (PN). The Petri nets are widely used as a modelling tool in several technical fields such as computer engineering, electronics and control systems. However, they didn't receive much importance and applications in the safety and risk assessment area. Multiples methodologies developed during this research project are presented in the application parts of the thesis, and have proved the applicability of a new generation of high level Petri nets, called "Generalized stochastic Petri Nets with predicates and assertions". This formalism shows an interesting modelling capability for reliability-availability-maintainability and safety (RAMS) studies due to their unique modelling characteristics like the concurrency, conflicts behaviours' management, the synchronization and resources sharing.

Résumé: Dans l'industrie des procédés, le risque potentiel provient d'une ou plusieurs anormales opérations causées par une défaillance d'un composant, une erreur humaine et/ou des facteurs extérieurs. Les causes sont considérées comme étant des événements déclencheurs qui génèrent un enchaînement de séquences affectant le système dans son entité. Cette série d'événements définissent les incidents industriels. Si ces derniers causent des pertes humaines (par exemple, décès ou blessures) ou dégât au niveau de l'infrastructure, ils se développent en accidents industrielles. Les méthodes les plus simples et les plus répondues pour décrire et analyser ces accidents, sont les analyses par arbres de défaillances et arbres d'événements. Elles ont eu cette importance à cause de leurs doubles aspects : qualitatives et quantitatifs, facile à implémenter et à discuter. D'un autre côté, les réseaux bayésiens sont des très bons outils de modélisation pour la description des dépendances conditionnelles. Mais ces derniers souffrent de limitations dans leurs capacités de modélisation en relation avec les dépendances de temps et les comportements complexes des systèmes modernes. Des méthodes plus sophistiquées existent, mais exigent des compétences de modélisation avancées et elles ne sont pas graphiquement explicites. Les réseaux de Pétri sont largement utilisés comme outil de modélisation dans différents domaines techniques, comme l'ingénierie informatique, l'électronique et le contrôle des systèmes. Mais ils n'ont pas reçu beaucoup d'importance dans le domaine d'applications de la sécurité et de l'évaluation des risques. Des multiples méthodologies ont été développées durant ce travail de recherche et sont présentées dans cette thèse. Elles ont prouvé leurs applicabilité dans une nouvelle génération de réseaux de Pétri de haut niveaux, nommés « Les réseaux de Pétri stochastiques généralisés avec les prédicats et les assertions ». Ce formalisme a montré une capacité de modélisation intéressante pour les études de la fiabilité-disponibilité-maintenabilité et sécurité à cause de leurs uniques caractéristiques de modélisation, comme la concurrence, les conflits, la synchronisation et le partage des ressources.