DYNAMIC OPERATIONAL RISK ASSESSMENT WITH BAYESIAN NETWORK

A Thesis

by

SHUBHARTHI BARUA

Submitted to the Office of Graduate Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

August 2012

Major Subject: Safety Engineering

DYNAMIC OPERATIONAL RISK ASSESSMENT WITH BAYESIAN NETWORK

A Thesis

by

SHUBHARTHI BARUA

Submitted to the Office of Graduate Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

Approved by:

Chair of Committee,	M. Sam Mannan
Committee Members,	Carl D. Laird
	Martin A. Wortman
Head of Department,	Charles J. Glover

August 2012

Major Subject: Safety Engineering

ABSTRACT

Dynamic Operational Risk Assessment with Bayesian Network. (August 2012)

Shubharthi Barua, B.Sc., Bangladesh University of Engineering & Technology

Chair of Advisory Committee: Dr. M. Sam Mannan

Oil/gas and petrochemical plants are complicated and dynamic in nature. Dynamic characteristics include ageing of equipment/components, season changes, stochastic processes, operator response times, inspection and testing time intervals, sequential dependencies of equipment/components and timing of safety system operations, all of which are time dependent criteria that can influence dynamic processes. The conventional risk assessment methodologies can quantify dynamic changes in processes with limited capacity. Therefore, it is important to develop method that can address time-dependent effects. The primary objective of this study is to propose a risk assessment methodology for dynamic systems. In this study, a new technique for dynamic operational risk assessment is developed based on the Bayesian networks, a structure optimal suitable to organize cause-effect relations. The Bayesian network graphically describes the dependencies of variables and the dynamic Bayesian network capture change of variables over time. This study proposes to develop dynamic fault tree for a chemical process system/sub-system and then to map it in Bayesian network so that the developed method can capture dynamic operational changes in

process due to sequential dependency of one equipment/component on others. The developed Bayesian network is then extended to the dynamic Bayesian network to demonstrate dynamic operational risk assessment. A case study on a holdup tank problem is provided to illustrate the application of the method. A dryout scenario in the tank is quantified. It has been observed that the developed method is able to provide updated probability different equipment/component failure with time incorporating the sequential dependencies of event occurrence. Another objective of this study is to show parallelism of Bayesian network with other available risk assessment methods such as event tree, HAZOP, FMEA. In this research, an event tree mapping procedure in Bayesian network is described. A case study on a chemical reactor system is provided to illustrate the mapping procedure and to identify factors that have significant influence on an event occurrence. Therefore, this study provides a method for dynamic operational risk assessment capable of providing updated probability of event occurrences considering sequential dependencies with time and a model for mapping event tree in Bayesian network.

DEDICATION

My teachers,

Dr. M. Sam Mannan & Late Sushil Bhattachariya

My parents,

Sathi Priya Barua & Sudipa Barua

My sister,

Shatabdi Barua

My friends,

Amira Yousuf Chowdhury & Mir Abdul Karim

ACKNOWLEDGEMENTS

I would like to express my gratitude to my committee chair, Dr. M. Sam Mannan, the person of my inspiration to work in the field of process safety. I would also like to thank him for giving me the opportunity to work in different industrial projects which helped me to build up teamwork skills, and to attend several meetings and continuing education courses which helped me to improve my communication skills. I would like to thank my committee members Dr. Carl D. Laird and Dr. Martin A. Wortman for the consent to be my committee members and continuous support. I would like to mention Dr. Hans J. Pasman for his time to discuss the scope of my research, provide background information on Bayesian networks, teaching me to use different software, reading my manuscripts, giving suggestions and comments. I would also like to thank my team leader Dr. Xiaodan Gao and Dr. Subramanya Nayak for their assistance, effort, time and valuable suggestions on my research. Also, I would like to express gratitude Dr. William J. Rogers and Dr. Xiaole Yang for their support in conducting this study.

I would like to express my gratitude to my parents, Engr. Sathi Priya Barua and Sudipa Barua, and my younger sister, Shatabdi Barua, for their constant love, unconditional care and consistent support from my childhood to become a better person and encouraging me to pursue MS degree in USA. I would like to mention Dr. Syed Faiyaz Hossainy, a family friend, for his generous support of my higher study in USA. I would also like to express sincere appreciation to my friends, Amira Yousuf Chowdhury

and Mir Abdul Karim, for providing me constant support from my undergrad study and continuing it in MS course of study.

I would also like to acknowledge Valerie Green, Donna Startz and all staff of Mary Kay O'Connor Process Safety Center for their assistance on administrative issues. Also, I want to mention that I have learnt a lot from Dr. Victor Carreto Vazquez and Dr. Dedy NG while working with them in different projects. Assistance, guidance and suggestions from all my friends at Mary Kay O'Connor Process Safety Center have helped me to conduct this study, different projects and job-search. Finally, I must mention and thank all Bangladeshi students of Texas A&M University and their families living at College Station, Texas for being supportive in my personal life for last 2 years.

TABLE OF CONTENTS

Page

ABSTRACT iii

DEDICATION v

ACKNOWLEDGEMENTS vi

TABLE OF CONTENTS viii

LIST OF FIGURES x

LIST OF TABLES xiii

1. INTRODUCTION 1

1.1 Background 1
1.2 Problem Statement 3
1.3 Research Objective 4
1.4 Research Contributions 5
1.5 Organization of This Thesis 8

2. LITERATURE REVIEW 10

2.1 General Background 10
2.2 Conventional Risk Assessment Methodologies 11
2.3 Dynamic Risk Assessment Methods 15
2.4 Overview of Bayesian Network Applications 17

3. THE DEVELOPMENT OF BAYESIAN NETWORK BASED DYNAMIC OPERATIONAL RISK ASSESSMENT METHODOLOGY 19

3.1 Introduction 19
3.2 Research Framework 28

4. APPLICATION OF THE METHODOLOGY 47

4.1 Case Study: A Tank Holdup Problem 47
4.2 Application of the Model 68

Page

5. GENERALIZING EVENT TREE IN BAYESIAN NETWORK 75

5.1 Introduction 75
5.2 Event Tree Mapping into Bayesian Network and Generalization Technique 75
5.3 Case Study 81

6. SUMMARY AND RECOMMENDATIONS 92

REFERENCES 95

VITA 103

LIST OF FIGURES

Page

Figure 1. Researches on dynamic operational risk assessment and Bayesian statistics in MKOPSC 7

Figure 2. Functional/probabilistic dependency gate 21

Figure 3. Spare gates 22

Figure 4. Probability AND-Gate (PAND gate) 24

Figure 5. A simple Bayesian network 26

Figure 6. Framework for the dynamic Bayesian network based dynamic operational risk assessment method 30

Figure 7. Mapping algorithm of AND-gate and OR-gate in Bayesian network 33

Figure 8. Spare gates of dynamic fault tree mapping in dynamic Bayesian network (Montani et al., 2005) 36

Figure 9. Spare gates of dynamic fault tree with intermediate inputs mapping in dynamic Bayesian network 39

Figure 10. FDEP/PDEP gate mapping in dynamic Bayesian network (Montani et al., 2005) 41

Figure 11. A holdup tank (level control system) problem 50

Figure 12. Dynamic fault tree for the holdup tank problem 52

Figure 13. Root nodes, intermediate nodes and top event nodes in Bayesian network 54

Figure 14. Nodes connected through arcs 55

Page

Figure 15. Dynamic Bayesian network with two time-slices without connection among nodes of two time-slices 58

Figure 16. Mapped spare gate in dynamic Bayesian network 59

Figure 17. Dynamic Bayesian network with two time-slices 60

Figure 18. Dry-out probability upon different equipment/components failure using different inspection intervals: weekly, monthly, 3 months, 6 months, 1 year and every 2 year 63

Figure 19. Less or no flow occurrence, automatic protection system failure and outlet valve fails open (failure) probability using different inspection intervals: weekly, monthly, 3 months, 6 months, 1 year and every 2 year 64

Figure 20. Pump system failure and pipe leakage probability using different inspection intervals 65

Figure 21. Primary pump and its system components failure probability using different inspection intervals 66

Figure 22. Standby Pump and its system components failure probability using different inspection intervals 67

Figure 23. Dynamic Bayesian network when maintenance/repair is performed at every 3 months interval (3 months, 6 months etc.) 69

Figure 24. Dryout probability in the system with no maintenance, maintenance work in every 3 months and in every 6 months 72

Figure 25. Less or no flow probability in the system with no maintenance, maintenance work in every 3 months and in every 6 months 72

Figure 26. Automatic protection system failure probability in the system with no maintenance, maintenance in every 3 months and in every 6 months 73

Figure 27. Pump system failure probability in the system with no maintenance, maintenance work in every 3 months and in every 6 months 73

Page

Figure 28. A general event tree....77

Figure 29. A general event tree mapped in Bayesian network....78

Figure 30. A chemical reactor system (Crowl and Louvar, 2002)....82

Figure 31. An event tree of a chemical reactor system....83

Figure 32. Mapped event tree in Bayesian network....84

Figure 33. Bayesian network with 'alarm' node evidence value set to 1....89

LIST OF TABLES

Page

Table 1 Conditional probability table for primary component state at '(n+1)-th' time slice given its state at 'n-th' time slice 36

Table 2 Conditional probability table for the first standby component state at '(n+1)-th' time slice given the state of primary component and first standby component at 'n-th' time slice 37

Table 3 Conditional probability for second standby component state at '(n+1)-th' time slice given state of primary component, first standby and second standby components state at 'n-th' time slice.....38

Table 4 Conditional probability table for primary component state at '(n+1)-th' time slice given its state at 'n-th' time slice for spare gate as in figure 9.....40

Table 5 Conditional probability table for standby component state at '(n+1)-th' time slice given its state at 'n-th' time slice for spare gate as in figure 9.....40

Table 6 Conditional probability table for trigger event at '(n+1)-th' time slice given its state at 'n-th' time slice.....42

Table 7 Conditional probability table for dependent components at '(n+1)-th' time slice given the state of trigger event at 'n-th' time slice 43

Table 8 Conditional probability table for component 'X' at '(n+1)-th' time slice given its state at 'n-th' time slice.....44

Table 9 Component failure mode and failure rate data.....51

Table 10 Prior probabilities of root nodes of first time slice at 1 Week.....61

Page

Table 11 Probability of system dry-out for different equipment/component failure using different inspection internals 62

Table 12 Probability of system dry-out for different equipment/components failure if maintenance/repair takes place at every 3 months....70

Table 13 Probability of system dry-out for different equipment/components failure if maintenance/repair takes place at every 6 months....71

Table 14 Conditional probability table for Event node 'A' 79

Table 15 Conditional probability table for event node 'B' depending on state of event node 'A' 79

Table 16 Conditional probability table for event node 'C' depending on state of event node 'A' and event node 'B' 79

Table 17 Deterministic probability table for consequence node 80

Table 18 Prior probability of initiating event (temperature increase)....85

Table 19 Conditional probability table for alarm node given initiating event (temperature increases) node states 85

Table 20 Conditional probability table for event node 'Operator_notices' given states of initiating event and alarm node....86

Table 21 Conditional probability table for 'operator re-starts cooling' node given state of 'operator_notices' nodes 86

Table 22 Conditional probability table for 'operator shutdowns reactor' given states of 'operator notices temperature increase' and 'operator re-starts cooling'....87

Table 23 Conditional probability table for 'continue operation' consequence node 87

Page

Table 24 Conditional probability table for ‘Safe shutdown’ consequence node....88

Table 25 Conditional probability table for ‘Runaway reaction’ consequence node....88

Table 26 Prior and posterior probability table for all event and consequences 90

1. INTRODUCTION

1.1 Background

The offshore oil/gas, chemical, petrochemical, food, power, papermaking and other process industries consist of numerous equipment and unit operations, thousands of control loops, and exhibit dynamic behavior. These process facilities have to deal with different hazards and several types of risks. At the same time, they have to meet the demand for higher quality of products by following rigorous environmental and safety regulations. Failure to manage or minimize hazards can result into serious incidents. For example, process facilities involve a large number of pumps, compressors, separators, complex piping system and storage tanks, etc. in congested area. A small mistake by an operator or a problem in the process system may escalate into a disastrous event as the process area is congested with process equipment and piping systems, and has limited ventilation and escape routes. Process plants are subjected to different types of risks in daily operations, which include process risks, risks due to reactivity, toxicity and mechanical hazards, fire and explosion risks. Therefore, it is very important to identify hazards, perform risk assessments, and take proper initiatives to minimize/remove hazards and risks; else a catastrophic accident may result.

This thesis follows the style of *Journal of Loss Prevention in the Process Industries*.

From case histories, it has been observed that catastrophic accidents have a significant effect on people, environment, and society. Catastrophic accidents such as the Flixborough disaster, the Bhopal incident, and the Piper Alpha disaster caused fatalities and unbearable economic loss. The U.S. Chemical Safety Board (U.S. CSB, April 06, 2012) completed investigation on sixty-five serious accidents that occurred in the U.S.A. since 1998. Investigations of catastrophic accidents have reported insufficient process safety, inadequate management of change and lack of risk reductions measures as root causes of these accidents. For example, a vapor cloud explosion taking place at BP Texas City refinery in 2005 resulted in 15 fatalities, 180 injuries and $1.5 billion in losses (U.S. CSB, 2007). The investigation revealed that insufficient process safety and lack of risk reduction measures contributed to this catastrophic accident. The U.S. CSB investigation on natural gas explosion at ConAgra foods processing facility North Carolina in 2009, and Kleen Energy power plant Connecticut in 2010, reported failure to adopt inherently safer method from fire and explosion hazard perspective led to explosions (Khakzad et al., 2011). In 2010, a fire and explosion, resulting from a blowout, at the Macondo well resulted in 11 deaths and 17 injuries (U.S. National Commission on BP accident, 2011). Also the continuous spill from the wellhead for 87 days had disastrous effects on the environment and wildlife surrounding the Gulf of Mexico.

Presently, The U.S. CSB has been conducting investigations on fourteen other major accidents in The U.S.A. Disastrous accidents in refineries, power plants and offshore platforms involved fatalities and great financial loss. The accidents have

significantly affected people's perception, and contributed greatly to raise concern to emphasize process safety. It is explicit that effective risk assessment and adequate process safety management can prevent or reduce severity of accidents. Therefore, continuous attention should be provided to improve available risk assessment methodologies. Also, it is important to develop new risk assessment technique that can provide more information and flexibility to the industry for better risk management than the available techniques. The objective of this research is to propose a technique for dynamic operational risk assessment. The following sections in this chapter demonstrate the problem statement, objectives and contributions of this research.

1.2 Problem Statement

The oil/gas, chemical and petrochemical process industries are complicated and dynamic in nature. Dynamic characteristics involve various time-dependent effects such as changes in seasons, aging of process equipment/component, stochastic processes, human error, inspection and testing time intervals, hardware failures, process disturbances, sequential dependencies and timing of safety system operations. It is important to quantify risks arising from above stated time-dependent effects. But, conventional risk assessment methodologies have limited ability to quantify dynamic changes in processes. For example, fault tree or event tree describes the relationship between the final outcome and different component/equipment failure but failed to incorporate system dynamic response to time, variations of process variables, operator actions, sequential dependencies etc. Catastrophic accidents may result when critical

process parameters exceed the safe operating region without being detected (Yang,2010; Yang and Mannan, 2010) due to protective system failure or timing of safety system operations. Yang (2010) described BP Texas City refinery accident as an example of operational failure in process industry. Therefore, it can be stated that available methodologies are not able to provide accurate results because of their inadequate ability to describe the variation of operational risk as time-dependent deviations, or the changes occurring in the process. Hence, it is important to develop a method that has the ability to quantify risk arising due to different time-dependent effects.

1.3 Research Objective

The purpose of this study is to develop a dynamic operational risk assessment method that can provide updated risk with time, model sequential dependencies, demonstrate the effect of inspection and testing time intervals and incorporate other time dependent effects. Bayesian network is used to develop the new dynamic operational risk assessment method. The objectives of this research are to:

- Develop a dynamic risk assessment methodology based on Bayesian network , which is a universally applicable probabilistic cause-effect model structure
- Demonstrate parallelism of Bayesian network based risk assessment methodologies with other available methodologies
- Describe advantages of Bayesian network based risk assessment methodology's application in chemical process safety over other methods

GeNIe (Decision Systems Laboratory, 2010), an open source software developed by Decision System Laboratory, University of Pittsburgh, is used to fulfill the objectives.

1.4 Research Contributions

Conventional risk assessment methodologies are static in nature. They also have limited ability to quantify different time dependent effects such as, inspection and testing time interval, operator response times and equipment/component ageing. This research demonstrates the application of Bayesian network to develop a methodology that has the ability to provide continuous update of risk with time. Furthermore, developed approach allows us to incorporate changes in the failure probability of equipment based on inspection and testing time interval. Bayesian network has widespread application in the field of artificial intelligence, medical diagnostics, financial sector, etc. The application of Bayesian network in the field of chemical process safety, risk analysis and accident modeling is relatively new. Current available studies are only as follows:

- Khakzad et al. (2011) described mapping of fault tree of process industry in Bayesian network based on the method provided by Bobbio et al. (2011)
- Pasman and Rogers (2011) described incorporation of Bayesian network in Layer of Protection Analysis (LOPA)
- Khakzad et al. (2012) further provided methodology for mapping bow-tie analysis in Bayesian network and demonstrate probability adapting

However, the first two studies are static in nature. The authors in the last one described the method as dynamic risk assessment. This method can update probability in

presence of new information. But, this study did not consider the sequential dependency and the effect of time in the model. This research provides a methodology based on Bayesian network that has the ability to show the effect of time and provides updated probability with time in presence of new information. Therefore, this research will provide a new tool for dynamic operational risk assessment that can be useful for oil/gas, chemical, petrochemical and other industries for quantitative risk analysis.

1.4.1 Relationship with previous research at MKOPSC

In figure 1, researches since 2007 done on dynamic operational risk assessment and Bayesian statistics at Mary Kay O'Connor Process Safety Center (MKOPSC) are described.

In 2007, Gen Woong Yun developed the Bayesian-LOPA methodology for performing risk assessment of a LNG importation terminal (Yun et al., 2009). This methodology employs Bayesian statistics to update general data obtained from databases with plant specific data. Generic data for equipment and component are obtained from several databases. LNG plant specific data are used for likelihood estimation and then combined with generic data to get posterior data.

In 2010, Xiaole Yang developed a dynamic operational risk assessment (DORA) methodology that follows semi-markovian approaches (Yang, 2010; Yang and Mannan, 2010). DORA methodology is mainly a stochastic simulation with the ability to quantify events. Component inspection and testing time interval is incorporated in the DORA method as a critical parameter. System state trajectory simulation is performed based on

Monte-Carlo method. The research also demonstrates application of Bayesian statistics for uncertainty reduction.

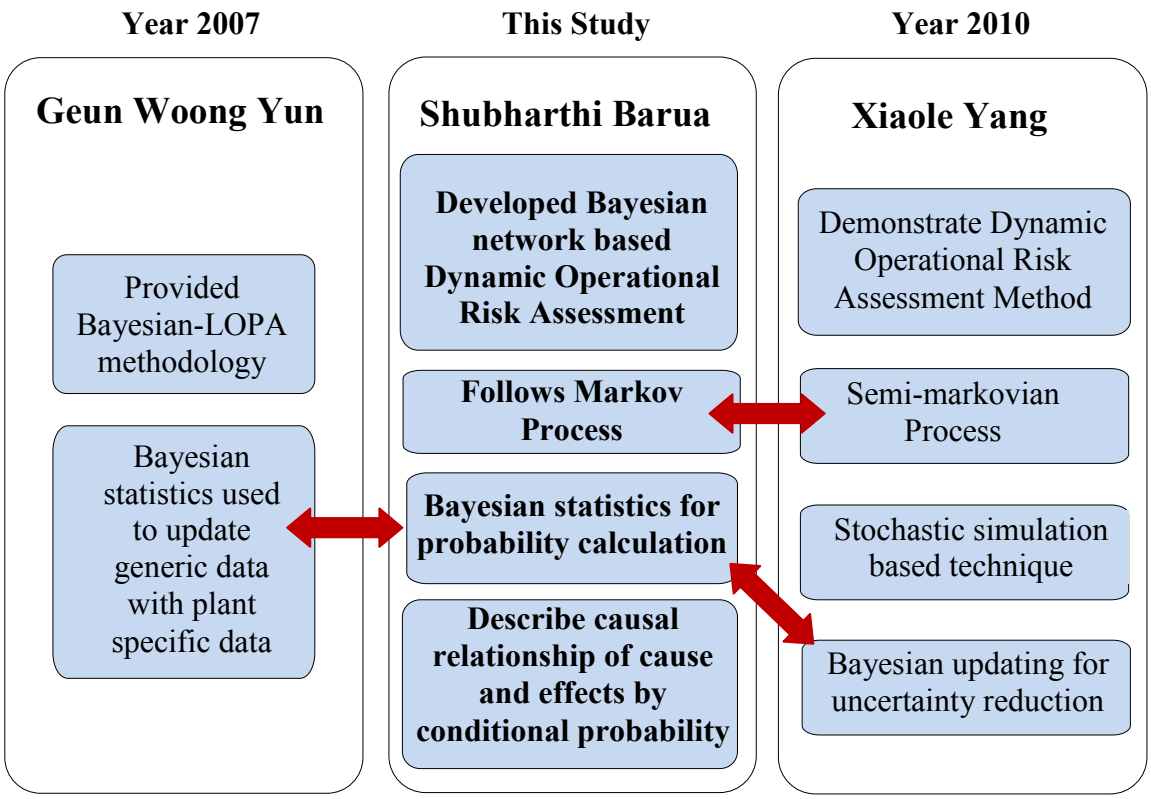


Figure 1. Researches on dynamic operational risk assessment and Bayesian statistics in MKOPSC

In this research, a new method for dynamic operational risk assessment method is demonstrated through applying the Bayesian network, an important subset of the Bayesian statistics. The methodology describes how conventional technique such as

Fault tree, Event tree can be improved by mapping in the Bayesian network and demonstrates the dynamic Bayesian network's ability to capture change in the values of different variables with time. The Bayesian statistics in previous researches are used to reduce uncertainty. In this study, by applying the Bayesian network, causal relationship between causes and effects are described by assigning conditional probability, and then the Bayesian statistics is used for probability estimation. Also, in previous studies, the Bayesian statistics is applied only for probability distribution, not for discrete values. This study has developed discrete time Bayesian network based dynamic operational risk assessment, and demonstrated the application of probability distribution for developing continuous-time Bayesian network based risk assessment method for future work.

1.5 Organization of This Thesis

Section 1 is an introductory chapter that provides background information, research scope and objectives. In Section 2, brief introduction on conventional risk assessment methodologies, previous researches on developing dynamic risk assessment techniques and Bayesian network's application for reliability and risk analysis are discussed. The research methodology is presented in the following Section 3. In this chapter, overall research framework is explained. In Section 4, a case study is demonstrated to illustrate the application of developed method. In that chapter, an application of the developed method is provided to demonstrate the advantages of Bayesian network over other methods. In Section 5, an event tree generalization technique using Bayesian network is provided to illustrate parallelism with other

quantitative risk assessment techniques with Bayesian network. Section 6 provides overall summary and recommendations for future research.

2. LITERATURE REVIEW

2.1 General Background

The oil/gas, chemical, petrochemical and other process industries use equipment such as reactors, heat exchangers, distillation columns, storage vessels, pumps, compressors and complicated piping system. High level of heat and mass integration has made chemical process plant operation very complex and any small error can result catastrophic consequences. It is important to identify the hazards in the process and to know the risks posed by these hazards. Risk is a function of probability of any event occurrence and its consequence severity. Risk can be expressed as the measure of potential loss of property, human life, economic loss and other possible effects (Yang, 2010; Yang and Mannan, 2010). The risk assessment process identifies possible risks, characterizes their nature and magnitude, evaluates their occurrence probability, analyzes contributing factors, and assesses risk reduction measures. Risk analysis consists of risk assessment, risk management and risk communication (Yang, 2010; Yang and Mannan, 2010). The objective of performing risk assessment is to identify what can go wrong, how it can go wrong and its likelihood. Several qualitative and quantitative methods are available to perform risk analysis. The risk analysis method to be performed for a process is chosen depending on the scope of study required. This chapter provides brief introduction of the available risk analysis methodologies and demonstrates their limited ability of addressing different time-dependent effects of

dynamic process. Then a concise description of dynamic risk assessment methodologies, their strength and weakness are provided.

2.2 Conventional Risk Assessment Methodologies

A checklist is a methodical approach that lists all possible hazards or problems that may exist in a process industry. It is one of the simplest hazard identification methods (Khan and Abbasi, 1998). A checklist questions are mainly based on the operation and maintenance of a process plant, previous incident history, review of different documents, inspection and interview of plant personnel or based on standards and codes. A checklist development is dependent on the experiences of the personnel and it is very likely that some important aspects can be overlooked in a checklist. A checklist focuses on a single item at a time and has limited ability to detect hazards due to different operating condition in different equipment or unit operations. For these limitations, checklist application is limited.

What-if analysis is a systematic method that ask question starting with "what-if…" to identify potential irregularity in the process. It provides qualitative descriptions of any activity or system problem those results from human errors, abnormal process conditions equipment failures, etc. What-if analysis is especially useful for relatively simple failure scenarios.

A safety audit or review is done to detect safety problems in working zone i.e., process areas, laboratories etc. A safety review is conducted for new process or during modification of existing processes to identify any lacks in operating procedure or to

detect equipment conditions that may lead to an incident. The safety audit/review report provides insight into plant conditions from safety point of view and recommendations for improvements.

Hazard and Operability Study (HAZOP) is the most commonly used hazard identification methods. A multi-disciplinary team of experienced personnel from operations, maintenance and design review process flow diagrams, piping and instrumentation diagrams, process descriptions, operating procedures to identify possible consequences due to deviations from normal conditions and causes of deviations. HAZOP is based on different guidewords and provides primary ideas about hazards associated in a process with recommendations for minimizing or removing them. Like other qualitative methods, the quality of HAZOP is dependent on the experience of the people conducting it. The HAZOP procedure is briefly provided by Yang (2010). Khan and Abbasi (1998) described two main limitations of HAZOP, i.e., limited ability to incorporate spatial features with plant layout and requirement of long time to perform study.

The Norwegian Petroleum Directorate (NPD) was the first to make quantitative risk assessment mandatory for ‘Concept Safety Evaluation’ in their guideline published in 1981 (Norwegian Petroleum Directorate, 1981). But, it has received wide-spread acceptance in the oil and gas industry after the Piper Alpha disaster in 1988. The Lord Cullen investigation report (1990) on the Piper Alpha disaster recommended formulating quantitative risk assessment as an official requirement for the oil and gas industry. The U.K. Safety Case Regulation 1992 (UK HSE, 1992) made quantitative risk analysis

(QRA) mandatory for all existing and new installation in North Sea region. Since then, operators in the North Sea have to perform QRA studies to demonstrate that the potential risk is below the acceptable risk criteria and that actions have been taken to minimize the risk to 'as low as reasonably practicable'. Vinnem (1998) summarized the application of quantitative risk assessment for offshore installations. Several quantitative risk assessment methods are described in this section briefly.

In 1961, Bell Telephone Laboratories developed the fault tree analysis (Khan and Abbasi, 1998). In 1975, the U.S. Nuclear Regulatory Commission introduced the fault tree for nuclear industry (The U.S. Nuclear Regulatory Commission, 1975). Later, the fault tree's application has become extensive in reliability studies in the aerospace and chemical process industries. It is a graphical deductive process that starts reasoning from the top event to the undesirable events. In the conventional fault tree, there are two static gates, i.e. AND-gate, and OR-gate, that connect basic events failure with intermediate events and top event. In this approach, to understand failure mechanism explicitly, focus can be given to particular system failure at a time. But, the fault tree has some disadvantages as it can address common cause failures with limited ability (Khan and Abbasi, 1998). Fault tree has weakness in quantifying risks due to dynamically changing behavior or environment (Siu, 1994; Khan and Abbasi, 1998). Also, the conventional fault tree cannot adequately capture the sequential dependencies of equipment/components failure. Khan and Abbasi (1998) listed several studies that proposed improvement in conventional fault tree. Recently, Magott and Skrobanek (2012) proposed a fault tree based method which is capable of analyzing time-

dependencies. An event tree is an inductive process that demonstrates the sequences of different safeguards and human response failure due to an initiating event that lead to undesired consequences. The U.S. Nuclear Regulatory Commission (1975) introduced the method for nuclear industry and its application in chemical process industry is described by AIChE (2000), Mannan (2005), Delvosalle et al. (2006). Event tree's application is advantageous to determine possible consequences probability due to different initiating event and subsequent safety barriers and protection failure.

The bow-tie method is a combination of an event tree and fault tree. It is a graphical representation of complete accident scenario in which fault tree provides different causes towards a critical event and the event tree describes possible consequences due to the critical event. Delvosalle et al. (2006) demonstrated Bow-tie method's application for accident scenario identification in process industries. Mokhtari et al. (2011) proposed bow-tie based risk analysis method for sea ports and offshore terminals. Markowski and Kotynia (2011) demonstrated application of bow-tie model in layer of protection analysis (LOPA).

Layer of protection analysis (LOPA) is a semi-quantitative method that provides qualitative results of consequence with failure frequency data. It is derived from safety philosophy in the nuclear industry and became introduced to the process industry in the late nineties. The objective of performing layer of protection analysis is to determine sufficient independent safeguards that are available to prevent incidents. It should be noted all safeguards are not always independent layers of protection. Center for Chemical Process Safety (2001) described criteria for safeguards to be considered as

independent layer. Details of LOPA procedure are available at Center for Chemical Process Safety (2001), Markowshi A.S. (2006). Yun, G.W. (2007) incorporated Bayesian statistics to propose Bayesian-LOPA methodology for risk assessment.

2.3 Dynamic Risk Assessment Methods

Conventional risk assessment methods are static in nature. The oil/gas, chemical, petrochemical and other process industries are dynamic in nature. The process condition is dependent on variation of certain process variables which is affected by several time-dependent effects such as season changes, ageing of equipment/components, sequential dependencies, operator experiences and operation time, inspection and testing time interval etc. But, the conventional risk assessment methodologies have limited ability to quantify these time dependent effects. Siu (1994) summarized different methods developed for performing dynamic process systems risk assessment.

The Markov modeling is one of the widely accepted methods for dynamic risk analysis. State transition diagram is constructed to represent possible system states and transition from one state to another. A transition matrix is developed to characterize the Markov process. One of the limitations of the Markov process is that with increase of the system size, number of states also increases. It makes construction of system state transition diagram and computation complex (Reliability Analysis Center, 2003). Also, the Markov theory based models do not consider the effect of inspection on system-state transitions. The Markov model does not define the effect of inspection/testing time schedule.

Dynamic Logical Analytical Methodology (DYLAM) approach was proposed by Cacciabue et al. (1986). Nivolianitou et al. (1986) demonstrated application of DYLAM approach in reliability analysis of chemical processes. This method has the ability to quantify different time dependent effects by incorporating dynamic aspects of a process. It integrates physical behavior of the system and probabilistic modeling for analysis. In DYLAM, physical model for the system and component models for system components are constructed to predict system process variables reactions due to variations in component states. After defining undesired system states, the system model is simulated for all possible accident sequences to detect all possible combinations of status and states and calculate their likelihood. The DYLAM has limited ability to treat large number of scenarios and scenario calculations can be lengthier and more costly (Siu, 1994).

In the dynamic event tree, branching is allowed to take place at different points in time. Analyst defines the basis and required number of branches at any time step. Acosta and Siu (1993) described its application for accident sequence analysis.

Yang and Mannan (2010) proposed a semi-markovian approach named dynamic operational risk assessment (DORA) methodology. The DORA addresses dynamic effects in process industry by integrating process dynamic and system stochastic behavior. It can quantify risks for both component failure and component's abnormal events. The DORA method incorporated inspection/testing time schedule to understand its effect on risk. Monte Carlo simulation is performed to understand system abnormal condition due to each individual component's transition from one state to another and

then prolonged simulation is performed to understand effect of inspection and testing time on the probability of component abnormal event.

2.4 Overview of Bayesian Network Applications

Bayesian network is a probabilistic reasoning technique that can be very useful to represent complex dependencies between random variables. Weber et al. (2012) provides a summary of Bayesian network's application in the field of dependability, risk analysis and maintenance. Application of Bayesian network for process safety, accident analysis and risk assessment is relatively new. As described in section 1.4, Khakzad et al. (2011) described Bayesian network application in accident analysis in the field of process safety based on the work by Bobbio et al. (2001) that demonstrated application of Bayesian network in improvement of dependable system. In the field of dependability, Boudali and Dugan (2005) demonstrated sequential dependencies of events and Montani et al. (2005) included temporal aspects for analyzing reliability analysis. Pasman and Rogers (2011) incorporated Bayesian network in layer of protection analysis. Hudson et al. (2002) described Bayesian network application on anti-terrorism risk management planning. Summary of similar studies in risk analysis is provided by Weber et al. (2012). Khakzad et al. (2012) mapped bow-tie method into Bayesian network. Any study in process safety and risk analysis is yet to conduct on temporal aspects. Using the temporal reasoning, dynamic risk assessment methodology can be provided by incorporating effects of time. This study uses temporal reasoning for

proposing a dynamic operational risk assessment methodology that can easily quantify operational changes due to sequential dependencies of equipment/components.

3. THE DEVELOPMENT OF BAYESIAN NETWORK BASED DYNAMIC OPERATIONAL RISK ASSESSMENT METHODOLOGY

In this section mapping procedure of conventional fault tree and dynamic fault tree in Bayesian network and then development dynamic operational risk assessment methodology based on Bayesian network is illustrated. This section demonstrates how to set up conditional probability tables for different dependent variables and Bayesian network ability to update prior probability with new information into posterior probability. This chapter provides brief introduction of fault tree, dynamic fault tree, Bayesian network and its characteristics and dynamic Bayesian network framework in section 3.1 and demonstrates the research framework with details of the mapping procedure in section 3.2.

3.1 Introduction

Bayesian network based dynamic operational risk assessment methodology, is a new technique developed in this research. This study demonstrates an advancement of application of Bayesian network in process safety. The methodology may provide more reliable description of different equipment or component failure probability with time for any oil/gas, chemical, petrochemical and other process industries. This method is very much helpful for those fields where availability of operational history is limited. In this section, brief description of fault tree, dynamic fault tree with characteristics and description of Bayesian network and dynamic Bayesian network is provided.

3.1.1 Dynamic fault tree

Conventional fault tree has limited ability to capture sequence dependencies in the system. If a system consists of a primary (active) pump and a back-up (standby) pump, then in case of primary pump failure, the back-up pump can become active and continues the system operation. But, if the back-up pump fails before the active pump fails, then the back-up pump fails to become active to substitute primary pump and the system is in failed state when the primary pump fails. Therefore, the failure criteria of the overall system are dependent on both the sequence and combinations of events. Dugan et al. (1990) defined different sequence dependencies and Dugan et al. (1992) introduced dynamic fault tree for fault tolerant computer systems. Dynamic fault tree goes over conventional fault tree by defining following dynamic gates which capture the component's sequential and functional dependencies -

- The functional/probabilistic dependency gate (FDEP)/(PDEP)
- The spare gates (Warm-WSP, Hot-HSP, Cold-CSP)
- The priority AND gate (PAND)
- The sequence enforcing gate (SEQ)

This research work demonstrates development of dynamic fault tree using different dynamic gates introduced by Dugan et al. (1990, 1992). Brief descriptions of these gates are provided in this work.

3.1.1.1 The functional/probabilistic dependency gate (FDEP/PDEP)

In the functional dependency gate/probabilistic dependency gate, there is a trigger event on which some other events are dependent. The dependent events become

inaccessible in case of the trigger event occurrence. Figure 2 represents a function/probabilistic dependency gate. A trigger event can either be a basic event or output of another gate and its occurrence can cause two dependent events X and Y,

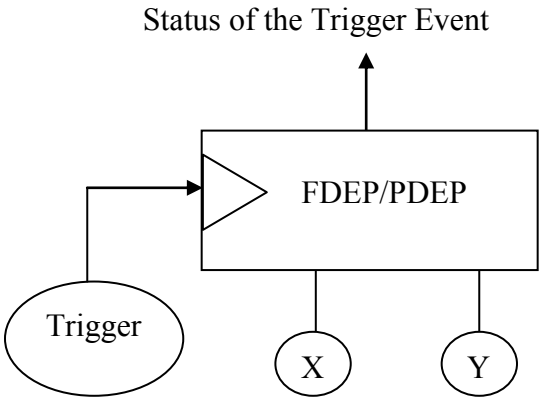


Figure 2. Functional/probabilistic dependency gate

inaccessible or unusable. Non-dependent output of the gate represents trigger event's status.

3.1.1.2 The spare gates

A spare gate generally consists of a primary component/equipment that can be replaced with one or more standby similar component/equipment to perform the same function in case of its failure. Whenever primary equipment/component fails, then the first standby equipment/component becomes active to continue the operation. If the first

standby fails, the next (if available) standby becomes active and so forth. A system with spare gate

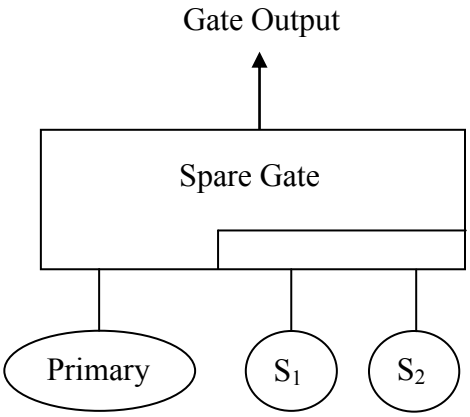


Figure 3. Spare gates

fails, if primary and all standby equipment fails. Also, a standby component can fail while it is not active, but its individual failure has no effect on the overall system until the primary and other standby equipment/component can perform the function.

Figure 3, shows a spare gate, where a primary input has two standby input S_1 and S_2. In case of primary input failure, at first S_1 comes into operation and system continues to function. If S_1 fails, then S_2 comes into operation and if S_2 fails, then the system fails. During Inactive state, the failure rate of the standby components/equipment is lower than that of in active state. Montani et al. (2005) defined dormancy factor, α, whose value can vary between 0 and 1, and stated that if the failure rate of a standby component is λ in

active state, then its failure rate at inactive state is αλ. Spare gates are thus classified into three classes, i.e. Hot spare, Cold Spare and Warm Spare. If the standby component does not fail during inactive state, then it is called cold spare. But if the standby component fails during inactive state, then it is called hot spare. Different values of α, represents different spare gates. For, hot spare, α =1; for cold spare, α =0; and for warm spare, value of α is between 0 and 1. In figure 3, thus the standby input S_1 and S_2 may have dormancy factor, α with any value between 0 and 1, and their failure during inactive state is lower than that of active state. Also, failure of this standby equipment when primary input is active, does not have any effect on the overall system.

3.1.1.3 The priority AND gate (PAND gate)

The priority AND-gate (PAND gate) consists of an AND-gate and pre-assigned order of inputs failure. In figure 4, two events X and Y are in a PAND gate and it is assigned that for the gate failure X has to fail before Y. Therefore, the output of the PAND gate in figure 4 is in failed state if both X and Y fails and X fails before Y. If Y fails before X, then PAND-gate output remains in normal state.

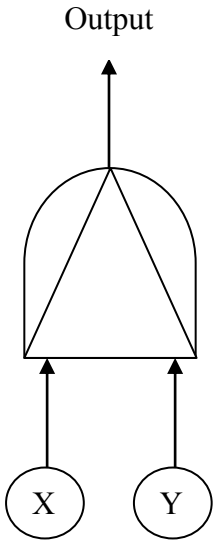


Figure 4. Probability AND-Gate (PAND gate)

3.1.1.4 The sequence enforcing gates (SEQ-gate)

In sequence enforcing gates, the inputs are constrained to fail in a particular order to cause system failure or a critical event to occur. The sequence enforcing gate fails only if its input failure occurs from left to right order. This is the difference between PAND-gate and SEQ-gate. Also, SEQ gates can be represented as spare gates. The difference is that spare gates have one or multiple standby input that can perform the same function as the primary input. But, in SEQ gates, the inputs can be any input performing different function.

3.1.2 Bayesian network

Bayesian network is widely applied in Artificial Intelligence (Pearl, 1988;

Neapolitan, 1990). Heckermann et al. (1995), Vomlel (2005) demonstrated some real life application of Bayesian network. Bobbio (2001) mapped fault trees into Bayesian network for dependability analysis and showed that Bayesian network has the ability to provide more precise reasoning with uncertainty. Recently, some authors applied Bayesian network in the field of process safety and accident modeling (Khakzad et al., 2011; Pasman and Rogers, 2011; Khakzad et al. 2012). Khakzad et al. (2011) demonstrated parallelism between fault tree and Bayesian network and described several advantages of Bayesian network's application in the field of accident modeling and process safety. Pasman and Rogers (2011) incorporated Bayesian network to improve Layer of Protection Analysis. Khakzad et al. (2012) mapped bow-tie analysis in Bayesian network. Bayesian network's application in the field of process safety and risk analysis is still relatively new and therefore, there is a scope for Bayesian network application for different study in this field.

A Bayesian network describes causal influence relations among variables via a directed acyclic graph. It represents a set of random variables in nodes and their conditional dependencies by drawing edges from one node to another. It has the ability to represent dependency among events clearly, accommodate multi- mode and continuous random variables, and incorporate information i.e. generic, system specific and expert judgment to support optimum decision making.

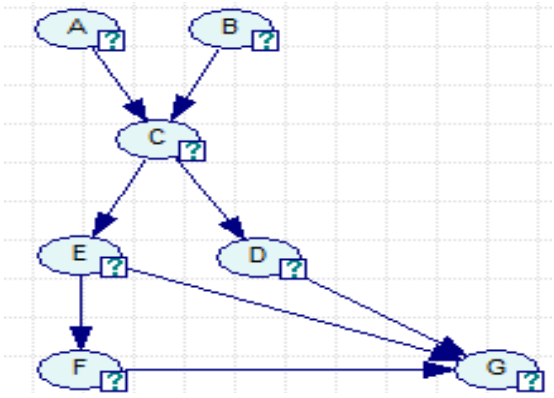


Figure 5. A simple Bayesian network

A simple Bayesian network is shown in figure 5. In a binary network, nodes and arcs represents variables and causal relationships among different nodes. Conditional probability tables or defined probabilistic relationships among nodes represent how one variable is linked another one or multi-variables. The nodes that influence other variables and have unconditional probability are called parent or root nodes. Nodes that are conditionally dependent on their direct parents are called intermediate nodes. The top node is defined as a leaf node.

Let $N = (G, P)$ be a Bayesian network, where, $G = (V, E)$ is a directed acyclic graph; V (random variables) represents nodes; and E represents edges between pairs of nodes of DAG. P represents probability distribution over V and $V = \{X_1, X_2, \dots, X_n\}$ can be either discrete or continuous random variables (Donohue and Dugan, 2003). These random variables are assigned to the nodes and the edges. Bayesian networks can be represented by the joint probability distribution *P(V)*;

$$P(V) = \sum_{X \in V} P\{X|pa(X)\} = P(X_1, X_2, \dots, X_N) = \sum_{i=1}^{n} P\{X_i|pa(X_i)\}$$

Here $pa(X_i)$ = parent nodes of X_i.

A main advantage of the application of Bayesian networks in risk analysis is the ability to update prior data using Bayes' theorem by incorporating new information. Also, Bayesian networks have an advantage of handling different types of uncertainty. Bayesian network can be a very useful tool for the fields where availability of data is limited and in case one wants to exploit the scarce information available best.

3.1.3 Dynamic Bayesian network

A general Bayesian network is static in nature, i.e., the joint probability distribution is usually a representation of a fixed point or an interval of time (McNaught and Zagorecki, 2010). A dynamic Bayesian network describes the evolution of joint probability distribution over time and thus extends general Bayesian network. Discrete time modeling to represent the progression of time in dynamic Bayesian network was proposed by Dean and Kanazawa (1989). In a dynamic Bayesian network, arcs links nodes from previous time slice to that of the next time slice to represent temporal dependencies among them.

Montani et al. (2005) provided detailed mapping procedure of dynamic fault tree into dynamic Bayesian network in dependability analysis. Kjaerulff (1995) demonstrated that Markov assumption can be held true for dynamic Bayesian network if the variable state at future time slice '(n+1)-th' time slice is independent of past given the present 'n-th' time slice. Boyen (1998) (Montani et al. 2005), Murphy (2002) described two-time slice Temporal Bayesian network.

3.1.4 Software

There are numbers of software available for developing and analyzing Bayesian network. Murphy (2007) provides a comparison among Bayesian network software. In this research, GeNIe 2.0, Bayesian network software developed by Decision Systems Laboratory (2010) is used for performing the analysis. This software is available free at http://genie.sis.pitt.edu/about.html and is compatible with other Bayesian network software. GeNIe supports both discrete and continuous variable though combination of both type of variables in a single network is still to be incorporated. GeNIe has temporal reasoning technique using which dynamic Bayesian network can be developed and analyzed. Other available software are: HUGIN (HUGIN EXPERT, 2012), BayesiaLab (BAYESIA SAS, 2010), Uninet (Lighttwist Software, 2008), BNT (Murphy,K., 2007) SAMIAM (AR Group-UCLA, 2010) etc.

3.2 Research Framework

Figure 6 shows overall framework to development dynamic operational risk assessment with Bayesian network. This method has the ability to automatically update probability if failure rate data is provided at the first time slice and conditional dependency is given.

3.2.1 Scope identification & system description

For developing dynamic operational risk assessment methodology based on Bayesian network, it is important to identify scope of work. It is also necessary to describe the system. According to the requirement, the scope can vary from small scale to large scale of system. For system description, process information as process block diagram, process flow diagram (PFD), piping and instrumentation diagram (P&ID), equipment/components in the system and their failure modes should be stated.

3.2.2 Identification of possible initiating event and component failure mode

The next step is to identify possible initiating event that can lead to accident. To identify possible initiating event, it is required to perform any hazards identification method which can be used to develop scenarios. Yang (2010) summarized qualitative hazard identification methods and process of conducting them. The next task is to identify different components failure modes that contribute to the occurrence of top event. In this step it is required to obtain failure rate data for different component. For this research, generic data are gathered from Center for Chemical Process Safety reliability data (AIChE 1989) and Offshore Reliability Data Handbook (SINTEF 2002).

It should be noted that generic data are historical data collected from similar industries and have limitation to properly reflect plant specific condition and characteristics of the plant equipment/component under consideration.

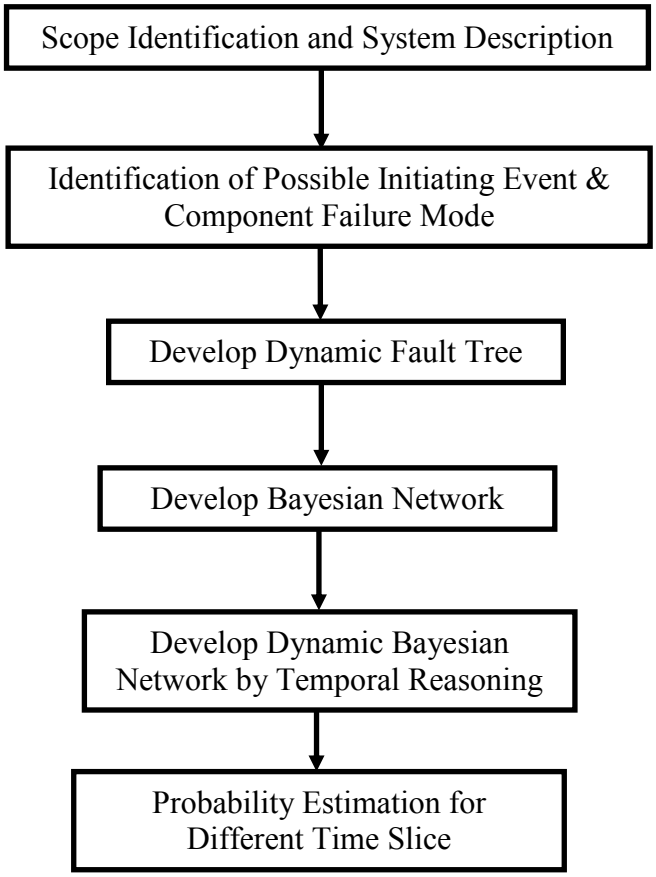


Figure 6. Framework for the dynamic Bayesian network based dynamic operational risk assessment method

3.2.3 Development of dynamic fault tree

Fault tree is a widely accepted method in oil/gas, chemical, petrochemical and other process plant for quantitative risk assessment. But, fault tree has limited capability to incorporate sequential dependencies. Therefore, this research proposes to develop dynamic fault tree for the system conceptually to capture sequential dependencies. Dynamic fault tree build-up is also a deductive process where top event is first identified

and then causes of that top event are detected. Sequential dependencies of different causes are identified and they are presented by dynamic gates as described in section 3.1.2. Events without sequential dependencies are presented by static fault tree gates. Detailed developing procedure of dynamic fault tree is described by Dugan et al. (1992).

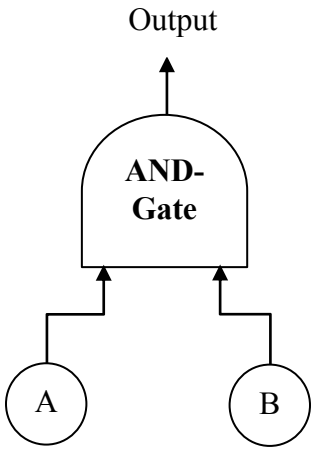
3.2.4 Develop Bayesian network & dynamic Bayesian network

3.2.4.1 Bayesian network mapping

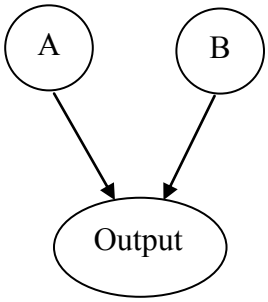
The next part is to map the dynamic fault tree into Bayesian network. Transforming dynamic fault tree in Bayesian network and eventually in dynamic Bayesian network is the important step for developing dynamic operational risk assessment with Bayesian network. The dynamic fault tree consists of two types of gates, i.e., the conventional fault tree gates and the dynamic gates. The conventional fault tree gates, i.e., OR-gate, AND-gate, K/M gates, involve equipment/component which does not show sequential dependencies. On the other hand, the dynamic gates i.e.,

spare gate, PAND gate, FDEP/PDEP gate and SEQ gate, describe sequential dependencies of different equipment/components.

The static part of the dynamic fault tree is mapped in Bayesian network according to the method provided by Bobbio et al. (2001). The mapping algorithm consists of both graphical and quantitative transformation. For graphical mapping, all basic or primary events of fault tree root/parents nodes are created in the Bayesian network. Prior probability is calculated for the component using exponential distribution. Then, intermediate nodes and top event nodes are created for intermediate events and top event of the fault tree respectively. These event occurrences in Bayesian network are conditioned by assigning conditional probability table. In fault tree, the intermediate events are related to the basic or primary event through OR-gate and AND-gate. Figure 7 represents parallel Bayesian network for the OR-gate and AND-gate and their corresponding conditional probability table. Mapping of dynamic gates of dynamic fault tree are mainly based on Montani et al. (2005). Detailed description of different dynamic gates mapping in dynamic Bayesian network is discussed in section 3.2.4.2.



(a.1) AND-gate

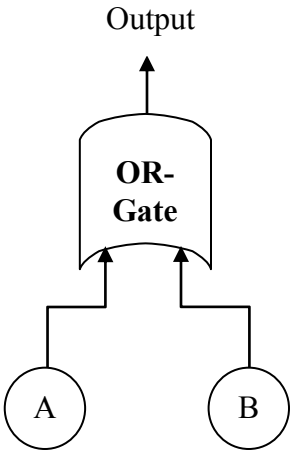


(a.2) Bayesian network of AND-Gate

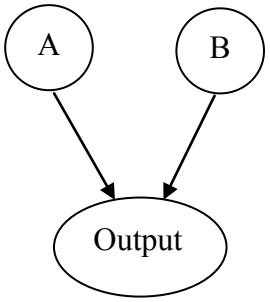
N= Normal state = 0

F= Failed state = 1

A	B	Output
0	0	0
1	0	0
0	1	0
1	1	1



(b.1) OR-gate



(b.2) Bayesian network of OR-Gate

A	B	Output
0	0	0
1	0	1
0	1	1
1	1	1

Figure 7. Mapping algorithm of AND-gate and OR-gate in Bayesian network

3.2.4.2 Dynamic Bayesian network development

The next step of the framework is to develop dynamic Bayesian network (DBN). In DBN, the nodes and their causal relationship are presented for various time slices.

The important step in development of dynamic Bayesian network is to map dynamic gates of dynamic fault tree in dynamic Bayesian network. The mapping procedure of dynamic gates in this study is based on Montani et al. (2005) and is discussed in section 3.2.4.2.1. Then the network is expanded for different time slices as described in section 3.2.4.3.

3.2.4.2.1 Mapping spare gate in Bayesian network

Figure 8 presents spare gates that has a primary component with two stand-by component S_1 and S_2 identical to the primary component. When primary component fails then, the first stand-by S_1 becomes active. If S_1 fails, then S_2 becomes active and keeps the system operating. When primary and both stand-by S_1 and S_2 fail, then the warm spare gates represent failed state of the system. These root nodes are provided with prior probability by using failure rate data in exponential distribution. Then this network is expanded for another time slice.

From figure 8, it is observed that each component node at next time slice is similar to that at the previous time slice. To represent the dependency of component state at different time-slices, an arc is drawn from primary component node, S_1 node and S_2 node of 'n-th' time slice to primary component node, S_1 node and S_2 node of '(n+1)-th' time slice. It demonstrates that component states at '(n+1)-th' time slice are dependent on their state at previous time slice. According to WSP, generally the primary component is in operation and if it fails, then the standby component becomes active. If the first standby component fails, then second standby component comes into operation.

The dependency is shown by drawing an arc from the primary component of 'n-th' slice to the stand-by components, S_1 and S_2 at '(n+1)-th' time slice. Also, as second standby component becomes active after first one's failure, an arc is drawn from S_1 of first time-slice to S_2 of next time slice. Therefore, if the primary component is active at first time slice, then its failure rate will be $\lambda_{primary}$ and at that time standby component can fail with failure rate $\alpha\lambda_{S1}$ and $\alpha\lambda_{S2.}$ If primary component fails at 'n-th time' slice, then S_1 is active and it can fail at '(n+1)-th' time slice with failure rate, λ_{S1} and λ_{S2} still have failure rate equal to $\alpha\lambda_{S2.}$ The overall system become non-operational when primary and its entire standby component fail.

Conditional probability table for components states in spare gates at '(n+1)-th' time slice given the component state at 'n-th' time slice is provided in tables 1, 2 and 3. In tables 1 to 6, Δt represents interval between two time slices, i.e., '(n+1)-th' and 'n-th' time slice. If 'n-th' time slice is at 3 months, and the '(n+1)-th' time slice is at 6 months, then the time interval between the slices is,

$$\Delta t = (6\text{-}3) \text{ months} = 3 \text{ months} = 3\times30\times24 \text{ hours} = 2160 \text{ hours}$$

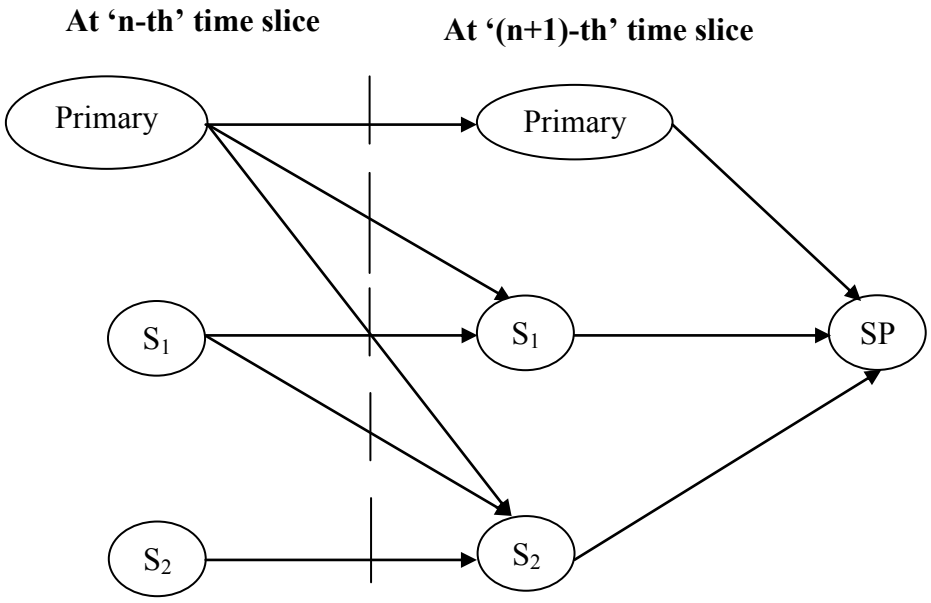


Figure 8. Spare gates of dynamic fault tree mapping in dynamic Bayesian network (Montani et al., 2005)

Table 1 Conditional probability table for primary component state at '(n+1)-th' time slice given its state at 'n-th' time slice

Primary Component		State at 'n-th' Time Slice	
		Normal State	Failed State
State at '(n+1)-th' Time Slice	Normal State	$\text{Exp}(-\lambda_{primary} \times \Delta t)$	0
	Failed State	$1- \text{Exp}(-\lambda_{primary} \times \Delta t)$	1

Table 2 Conditional probability table for the first standby component state at '(n+1)-th' time slice given the state of primary component and first standby component at 'n-th' time slice

		State at 'n-th' Time Slice			
Primary Component		Normal State		Failed State	
First Standby Component		Normal State	Failed State	Normal State	Failed State
State at '(n+1)-th' Time Slice	Normal State	$Exp(-\alpha\lambda_{S1}\Delta t)$	0	$Exp(-\lambda_{S1}\Delta t)$	0
	Failed State	$1-Exp(-\alpha\lambda_{S1}\Delta t)$	1	$1- Exp(-\lambda_{S1}\Delta t)$	1

Table 3 Conditional probability for second standby component state at '(n+1)-th' time slice given state of primary component, first standby and second standby components state at 'n-th' time slice

		State at 'n-th' Time Slice							
Primary		Normal				Failed			
First Standby		Normal		Failed		Normal		Failed	
Second Standby		Nor-mal	Fai-led	Nor-mal	Fai-led	Nor-mal	Fai-led	Nor-mal	Fai-led
At (n+1)-th Time Slice	Normal	Exp(-$\alpha\lambda_{S2}\Delta t$)	0	Exp(-$\alpha\lambda_{S2}\Delta t$)	0	Exp(-$\alpha\lambda_{S2}\Delta t$)	0	Exp(-$\lambda_{S2}\Delta t$)	0
	Failed	1-Exp(-$\alpha\lambda_{S2}\Delta t$)	1	1-Exp(-$\alpha\lambda_{S2}\Delta t$)	1	1-Exp(-$\alpha\lambda_{S2}\Delta t$)	1	1-Exp(-$\lambda_{S2}\Delta t$)	1

If any system consists of a primary component and 'n' number of standby components, then the n-th standby component will have 2^n states in conditional probability table.

The conditional probability given in tables 1, 2 and 3 holds true if the primary and standby equipment failure in spare gate are basic events. However, if they are intermediate events as shown in figure 9, then it is required to incorporate conditional dependency of intermediate events on their respective basic events.

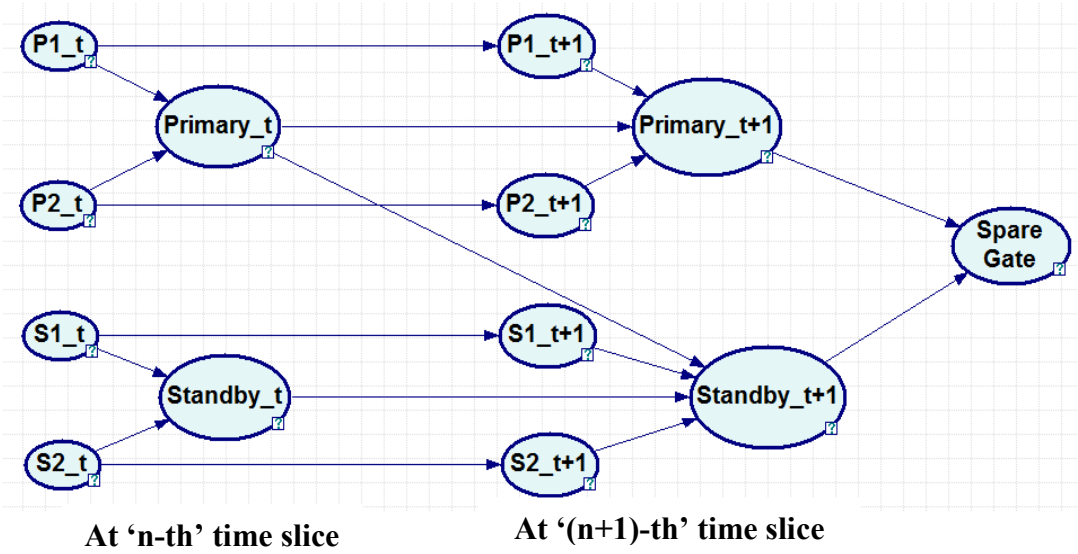


Figure 9. Spare gates of dynamic fault tree with intermediate inputs mapping in dynamic Bayesian network

If the basic events P1_t (failure rate, λ_{P1_t}) and P2_t (failure rate, λ_{P2_t}) are in an OR-gate with the intermediate event Primary_t ((failure probability, $\lambda_{overall}$)) at n-th time slice, then the overall failure rate of Primary_t at n-th time slice is the sum of basic events failure rate. If the basic event s P1_t (failure rate, λ_{P1_t}) and P2_t (failure rate, λ_{P2_t}) are in an AND-gate with the intermediate event Primary_t ((failure probability, $\lambda_{overall}$)) at n-th time slice, then the overall failure rate of Primary_t at n-th time slice is the product of basic events failure rate. The above statements are also true for standby equipment. Therefore, the primary event node i.e. Primary_t+1 at (n+1)-th time slice is dependent on Primary_t of n-th time slice, P1_t+1 and P2_t+1 of (n+1)-th time slice. Similar dependency exists for standby_t+1 node. The conditional probability table for

primary and standby node at (n+1)-th time slice are given in tables 4 and 5.

Table 4 Conditional probability table for primary component state at '(n+1)-th' time slice given its state at 'n-th' time slice for spare gate as in figure 9

Primary_t		N				F			
P1_t+1		N		F		N		F	
P2_t+1		N	F	N	F	N	F	N	F
Primary_t+1	N	$\exp(-\lambda_{overall\times}\Delta t)$	0	0	0	0	0	0	0
	F	$1-\exp(-\lambda_{overall\times}\Delta t)$	1	1	1	1	1	1	1

Table 5 Conditional probability table for standby component state at '(n+1)-th' time slice given its state at 'n-th' time slice for spare gate as in figure 9

Primary_t		N								F							
Standby_t		N				F				N				F			
S1_t+1		N		F		N		F		N		F		N		F	
S2_t+1		N	F	N	F	N	F	N	F	N	F	N	F	N	F	N	F
Primary_t+1	N	P1	0	0	0	0	0	0	0	P2	0	0	0	0	0	0	0
	F	1-P1	1	1	1	1	1	1	1	1-P2	1	1	1	1	1	1	1

The value of P1 and P2 are as follows:

$$P1 = \exp(-\lambda_{overall\_standby} \times \Delta t)$$

$$P2 = \exp(-\alpha \times \lambda_{overall\_standby} \times \Delta t)$$

3.2.4.2.2 Mapping functional/probabilistic dependency gate in Bayesian network

In function/probabilistic dependency gate (FDEP/PDEP), the status of the trigger event readily determines the states of the dependent event. The mapping procedure of FDEP/PDEP is based on work by Montani et al. (2005).

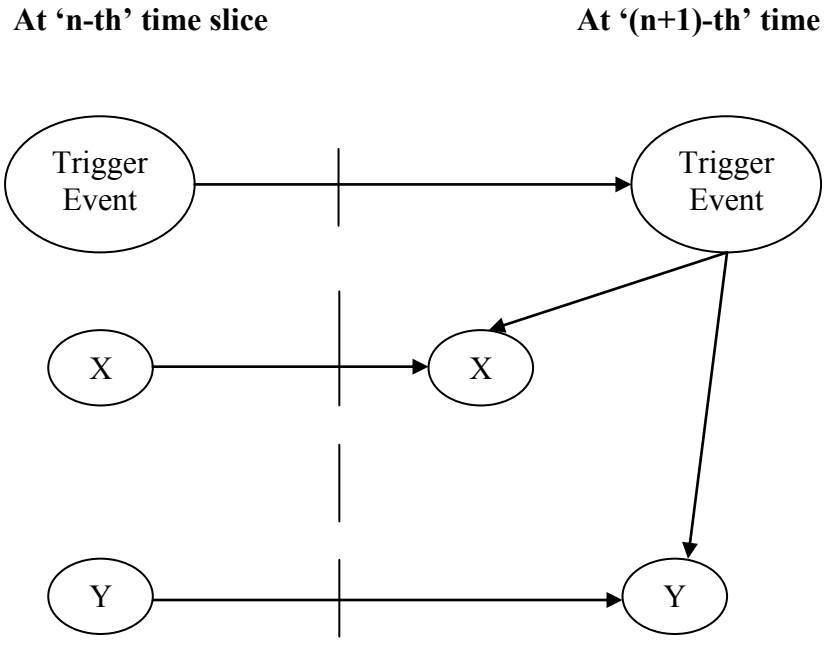


Figure 10. FDEP/PDEP gate mapping in dynamic Bayesian network (Montani et al., 2005)

In FDEP/PDEP gates, an arc connects the trigger event node at 'n-th time slice' with that node at the '(n+1)-th' time slice. The dependent components, X and Y, on trigger event also have an arc from present to future time slice. Also, the trigger event has two arcs connected to the dependent components representing that the status of trigger event at a time-slice has impact on the dependent components. Detailed conditional probability table for FDEP/PDEP gate is provided in tables 6 and 7.

Table 6 Conditional probability table for trigger event at '(n+1)-th' time slice given its state at 'n-th' time slice

Trigger Event		State at 'n-th' Time Slice	
		Normal State	Failed State
State at '(n+1)-th' Time Slice	Normal State	$Exp(-\lambda_T \times \Delta t)$	0
	Failed State	$1- Exp(-\lambda_T \times \Delta t)$	1

Here, 'λ_T' represents the failure rate data of the trigger event and Δt gives the time interval between (n+1)-th and n-th time slice.

Table 7 Conditional probability table for dependent components at '(n+1)-th' time slice given the state of trigger event at 'n-th' time slice

		State Trigger Event and Dependent Component at 'n-th' Time Slice			
Trigger Event		Normal State		Failed State	
State of Component at '(n+1)-th' Time Slice		Normal State	Failed State	Normal State	Failed State
First Dependent Component, X	Normal State	$Exp(-\lambda_X \Delta t)$	0	0	0
	Failed State	$1-Exp(-\lambda_X \Delta t)$	1	1	1
Second Dependent Component, Y	Normal State	$Exp(-\lambda_Y \Delta t)$	0	0	0
	Failed State	$1-Exp(-\lambda_Y \Delta t)$	1	1	1

The structure of conditional probability tables for all dependent components is same. Hence, if the system has more dependent components than shown above, they will also have a similar conditional probability table.

3.2.4.2.3 Mapping priority AND-gate (PAND Gate)

The priority AND-gates require failure of all components in a pre-assigned order. Following are the conditional probability tables for the PAND-gate shown in figure 4, in which there are two components X and Y respectively and PAND-gate fails if X fails before Y fails.

Table 8 Conditional probability table for component 'X' at '(n+1)-th' time slice given its state at 'n-th' time slice

Component 'X'		State at 'n-th' Time Slice	
		Normal State	Failed State
State at '(n+1)-th' Time Slice	Normal State	$Exp(-\lambda_X \times \Delta t)$	0
	Failed State	$1- Exp(-\lambda_X \times \Delta t)$	1

According to Montani et al. (2005) component Y can stay in operating or failed state before component X fails or failed after component X state fails. PAND gate will result in failure only if component X and component Y both fail and X fails before Y. Therefore, the values to put in conditional probability tables for component Y are given below:

Pr{Y(t+1) = failed before X at (n+1)-th time slice | Y(t) = failed before X at n-th time slice} = 1

Pr{Y(t+1) = failed before X at (n+1)-th time slice | X(t), X(t+1) and Y(t) = working} = 1- exp ($-\lambda_B \times \Delta t$)

Pr{Y(t+1) = failed after X at (n+1)-th time slice | Y(t) = failed after X at n-th time slice} = 1

Pr{Y(t+1) = failed after X at (n+1)-th time slice | X(t), X(t+1) and Y(t) = working} = 1- exp ($-\lambda_B \times \Delta t$)

Pr{Y(t+1) = failed after X at (n+1)-th time slice | X(t)=failed at n-th time slice, X(t+1) and Y(t) = working} = 1- exp ($-\lambda_B \times \Delta t$)

Therefore, the final status of PAND-gate at (n+1)-th time slice depends will be in fail state if X at (n+1)-th time slice fails before Y at (n+1)-th time slice. Else, it will be in working state.

3.2.4.3 Dynamic Bayesian network development for different time slices

To develop dynamic Bayesian network, the mapped dynamic fault tree according to the method described in section 3.2.4.1 is considered as the network for first time slice. Then this network from first time-slice is expanded to several time-slices. Network of present time slice has causal influence from the network of previous time slice. Number of time slices required is decided by the person performing the study.

3.2.5 Probability estimation

Montani et al. (2005) demonstrated procedure for dynamic Bayesian network development. Full specification is given below:

- Prior probabilities of all basic events at the first time slice (for a certain time)
- Conditional probability tables should be assigned for all intermediate events for the first time slice
- Provide conditional probability tables for all basic and intermediate events for future time slices. Conditional probability table structure is discussed in section 3.2.4.2

GeNIe software is used to perform the analysis. When the network is developed and all nodes are provided either prior or conditional probability, then the software does the calculation and provides probability for all nodes.

4. APPLICATION OF THE METHODOLOGY

The application of the methodology is provided with a case study on a tank hold up problem. The problem is demonstrated step by step and then how inspection time interval can affect the risk is shown. Then possible effect of repair is incorporated in the model to describe modeling flexibility of the Bayesian network based model for risk analysis.

4.1 Case Study: A Tank Holdup Problem

4.1.1 Scope identification and system description

A holdup tank problem shown in figure 11 is provided to illustrate the methodology. Similar types of holdup tank problem were studied by Aldemir (1987), Siu (1992) and Hurdle (2009). Under normal condition, the level of the system is maintained between 'x_1' and 'x_2'. In normal circumstances, liquid flows out through the outlet valve, which is partially open. A primary pump supplies liquid to the system. Sensor, S_1 sends signal to controller C_1, to actuate valve-, V_1 either to open to supply more liquid or close to reduce supply of liquid to maintain the level between 'x_1' and 'x_2'. If the liquid level goes above 'h', then an overflow scenario may happen. High level sensor, S_2 detects the level and sends signal to high level alarm, LAH. If high level alarm sounds, then an operator goes to open manual safety valve so that liquid also flows out through it to bring the liquid level in the desired region. When level comes to the operating region,

then the operator closes the manual safety valve. If the liquid level goes below'd', then a dryout scenario may happen. Sensor S_3 is low level sensor and if level goes beyond 'd', then it sends a signal to the controller C_3 to actuate valve, V_3 to close so that liquid cannot go out the system and level can return to the desired operating region. When level stables, the outlet valve opens again to the previous condition. In case of primary pump failure, a standby pump starts and continues delivery of liquid to the system.

4.1.2 Identification of possible top event and component failure mode

Two types of scenario can occur in the system i.e., overflow and dry-out. Dry-out occurs in the system when the liquid level goes below 'd' due to no or less flow to the system, protection system fails and the outlet valve, V_3 fails. If there is any leakage in the pipe or if the pump system fails, then there can be no or less flow to the system. Pump system failure can occur in two ways, i.e. either both pumps fails or flow control system associated with the pumps fails.

In normal condition, the primary pump is supposed to deliver liquid to the system. So, if the primary pump is stopped spuriously then the standby pump has to start immediately to continue liquid supply to the system. If the standby pump fails to start on demand then there will be no flow from the pump to the system. Flow control system to the pump consists of a controller, level sensor and the control valve. Sensor can also have spurious operation and fail to send signal to the controller. Also, the controller can fail to actuate the valve or the valve can have mechanical failure. Equipment and components failure modes that lead to the dry-out, scenario in the system are listed in

table 9. Their failure rates are also provided in table 9. These data are generic data obtained from OREDA (OREDA 2002) and CCPS (AIChE 1989).

4.1.3 Develop dynamic fault tree

The next step in the framework is to develop a dynamic fault tree for the system. As the system has a primary pump system which can be substituted by a standby pump, the system experiences operational change while standby pump becomes active in case primary pump fails. Figure 12 represents developed dynamic fault tree for the tank holdup problem. It is discussed in the methodology that dynamic fault tree consists of both dynamic and static gates. The developed dynamic fault tree has one type of dynamic gate i.e., spare gate and two static gates, i.e., OR-gate and AND-gate.The top event of the tree is dry-out in the system. Dry-out can occur if protection system fails or less or no flow or outlet valve, V3 fails open. The low level sensor S3 and the controller C3 are part of automatic protection system against dry-out. Failure of anyone can result in the protection system's failure. The system can experience no or less flow if there is any leakage in pipe or pump system fails. Pump system is the output of a spare gate that can be in failed state if the primary pumping system fail stop and the standby pump system fails to start of demand. Therefore, primary pumping system and the standby pumping system are input to the spare gate. Both the pumping systems consist of a pump, a level sensor S_1, a controller (C1 for primary pump and C_2 for standby pump) and a pump discharge valve.

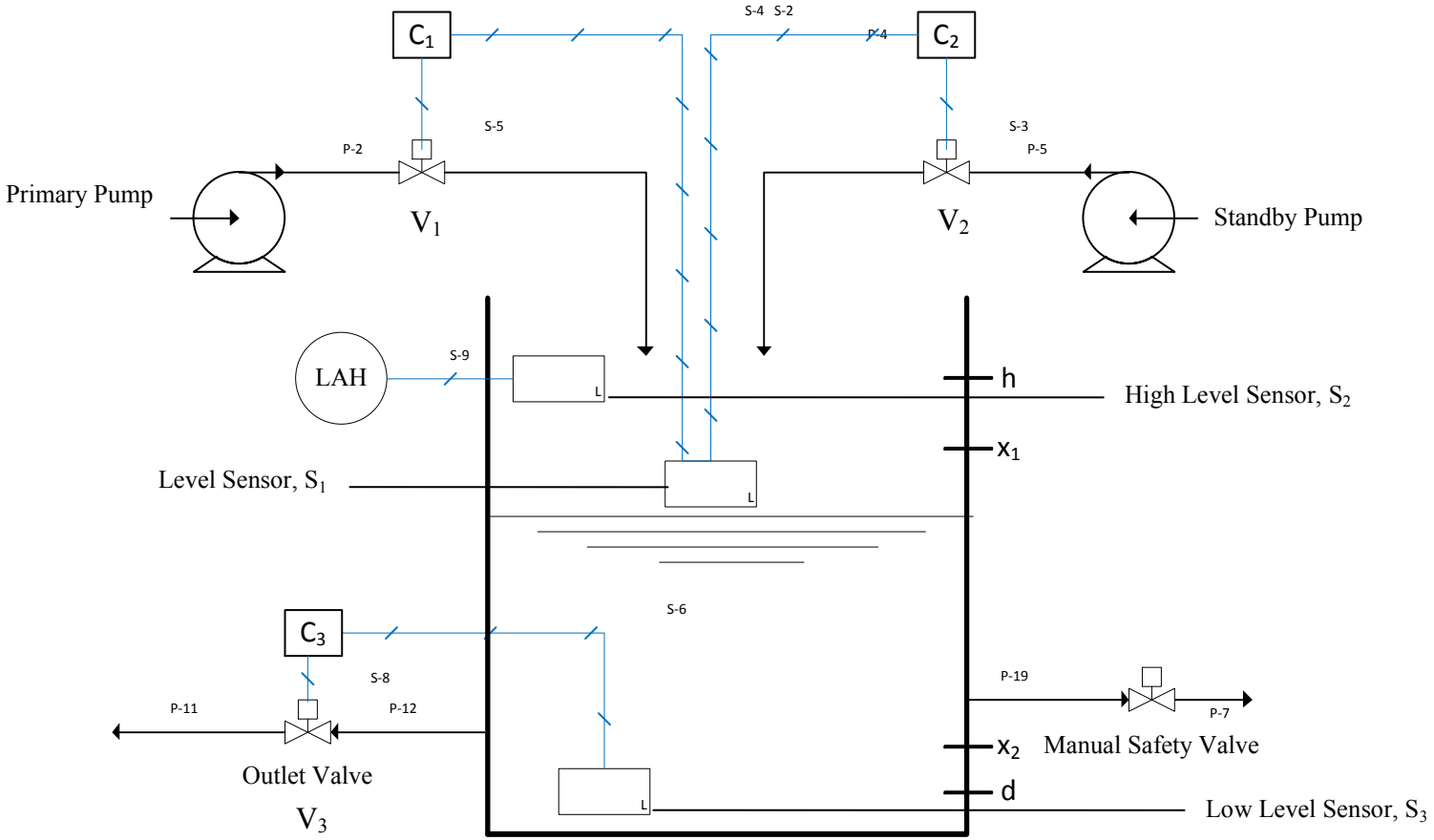


Figure 11. A holdup tank (level control system) problem

Table 9 Component failure mode and failure rate data

Component	Failure Mode	Failure Rate (per Hour)	Data Source
Primary pump	Spurious stop	5.69×10^{-6}	OREDA
Standby Pump	Fail to start on demand	2.52×10^{-6}	OREDA
Controller, C_1	Pneumatic controller failure	4.34×10^{-5}	CCPS
Primary Pump Outlet Valve, V_1	Failed to regulate	5.5×10^{-7}	OREDA
Sensor, S_1	Failed to function on demand	1.72×10^{-6}	OREDA
Controller, C_2	Pneumatic controller failure	4.34×10^{-5}	CCPS
Standby Pump Outlet Valve, V_1	Failed to open on demand	2.81×10^{-6}	OREDA
Sensor, S_3	Spurious operation	1.72×10^{-6}	OREDA
Controller, C_3	Pneumatic controller failure	4.34×10^{-5}	CCPS
Pipe Leakage	Leakage Lined pipe straight section	0.442×10^{-6}	CCPS
Outlet Valve, V3	Fails open	2.31×10^{-6}	OREDA

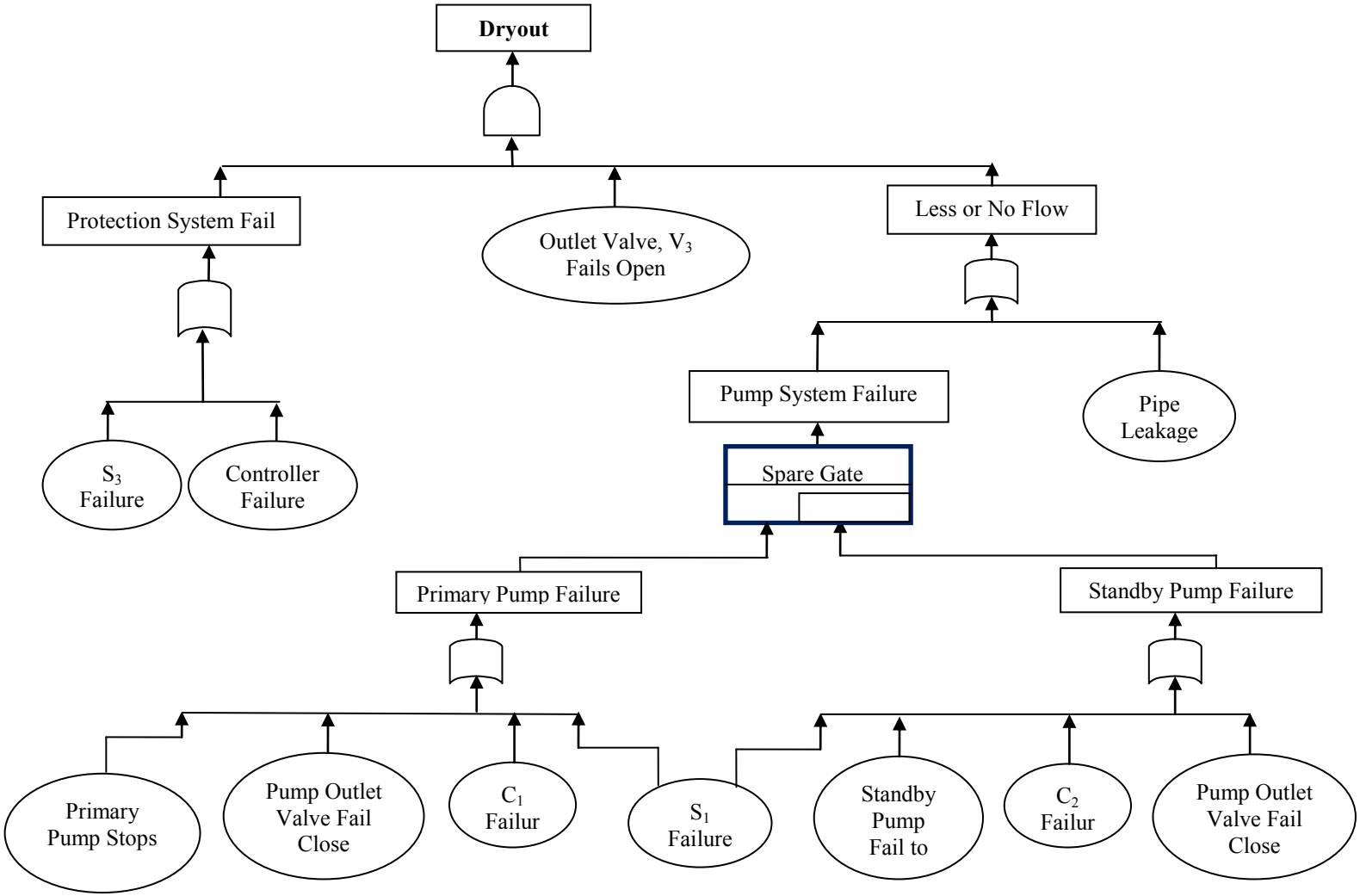


Figure 12. Dynamic fault tree for the holdup tank problem

4.1.4 Develop Bayesian network

Bayesian network development is an important step of this study. Step by step procedure is as follows to demonstrate the procedure of Bayesian network development.

- For each basic, intermediate and top event, root, intermediate and top event node are created respectively. They are shown in figure 13.
- Intermediate nodes are connected by arcs from those root nodes that cause the intermediate events from the basic events. Then top event node is connected by arcs from intermediate nodes and from one root node, as it directly affects the final top event. It is shown in figure 14.

4.1.5 Develop dynamic Bayesian network

The developed Bayesian network represents the causal structure for a single time slice. Also, the sequential dependency of the primary pump and the standby pump cannot be demonstrated graphically in a single time slice, though the dependency can be captured in a conditional probability table. Dynamic Bayesian network can graphically represent that dependency. Also, the objective of the methodology is to provide a technique that can update the probability of different equipment/components failure with time. To make a dynamic network, the network has to be expanded over different time slices. For this case study, the dynamic Bayesian network is developed for 6 time slices: the first network representing 1 week, the next 1 month, 3 months, 6 months, 12 months and 24 months. To illustrate how a dynamic Bayesian network is developed, here only construction of two time slices is described to prevent complexity.

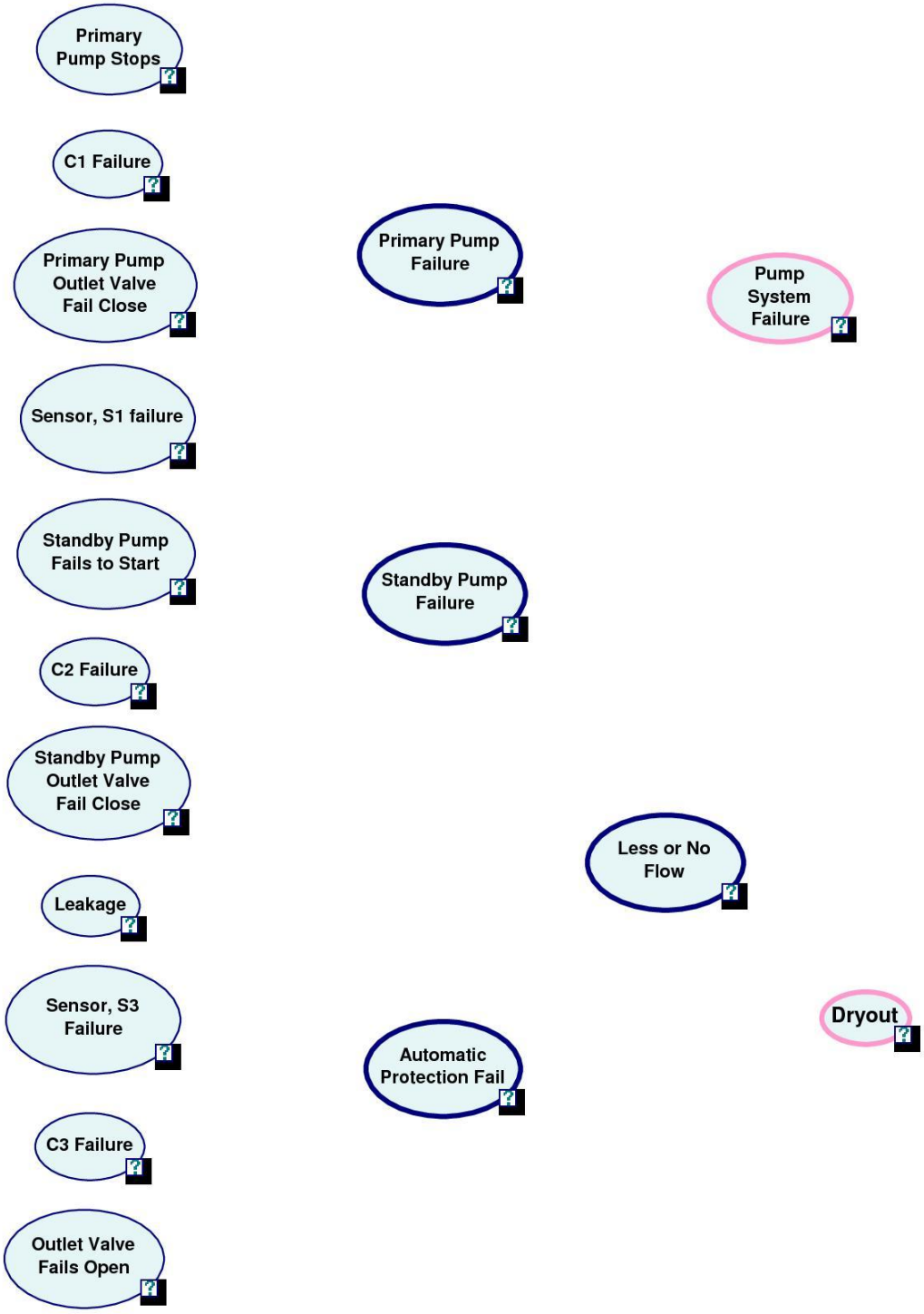


Figure 13. Root nodes, intermediate nodes and top event nodes in Bayesian network

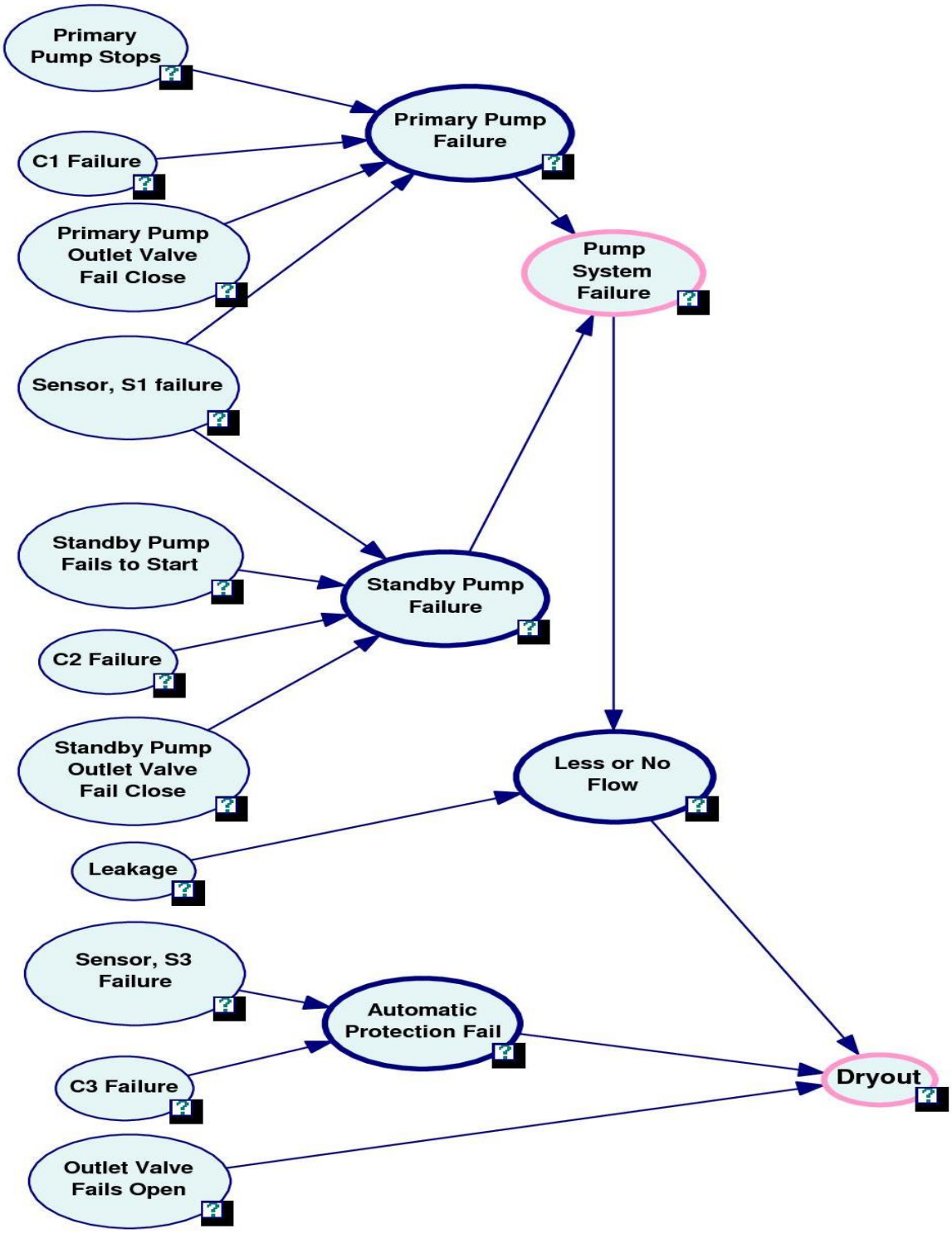


Figure 14. Nodes connected through arcs

- A similar new network, developed in section 4.1.4, is developed. The first network is presented for first time slice and the new network is presented for second time slice. This is shown in figure 15.
- Procedure of mapping a spare gate in Bayesian network is described in section 3.2.4.2.1. From primary pump system node of first time slice two arcs connects primary pump system node and stand-by pump system node of second time slice. Then an arc is drawn from standby pump system node of first time slice to that of the next time slice to complete the mapping of spare gate. Mapped spare gate in Bayesian network is provided in figure 16.
- Then, all root nodes of second time slice are connected with the nodes from first time slice to represent the conditional dependency of second time slice nodes on that of the first time slice. The complete dynamic Bayesian network is shown in figure 17.

4.1.5 Probability estimation

To estimate probability, the root nodes at first time slice are provided the prior probability calculated for a definite time. The prior probabilities of root nodes calculated for 1 week are given in table 10. Then, conditional probability tables for all intermediate and the complete dynamic Bayesian network is developed for six different inspection time intervals. They are 1 week, 1 month, 3 months, 6 months, 1 year and 2 years. For standby item, the dormancy factor, $\alpha = 0.5$, is considered. It is observed that with the increase in inspection interval, the probability of top event, dryout of the system, increases with time. It is shown in figure 18. top event nodes of first time slice are

provided following the methodology as described in section 3.2.4.2. The nodes in the second time slice are also given conditional probability values as described in the same section. Then the probabilities for all nodes are calculated in GeNIe software.

From table 11 it is apparent that all equipment/components failure probability increase with the inspection time interval increase. Figure 18 represents the dry-out probability upon less or no flow, automatic protection system failure and outlet valve fails open, using different inspection interval. Dry-out probability increases with increase of inspection intervals due to occurrence of less or no flow probability, automatic protection system failure probability and outlet valve fails open probability.

In figure 19 it is observed that the failure, less or no flow occurrence, automatic protection system failure and outlet valve, V_3, fails open probability increases with inspection interval increases. Less or no flow and automatic protection system failure are much more critical than the outlet valve fails open for dry-out scenario in the system. As less or no flow can occur due to pump system failure and pipe leakage, hence, their individual probability for different inspection intervals are plotted in figure 20. From figure 20, it is apparent that pipe leakage probability is very low. Therefore, it can be concluded that the pump system failure is mainly responsible for less or no flow and leakage in pipe has negligible effect on that.

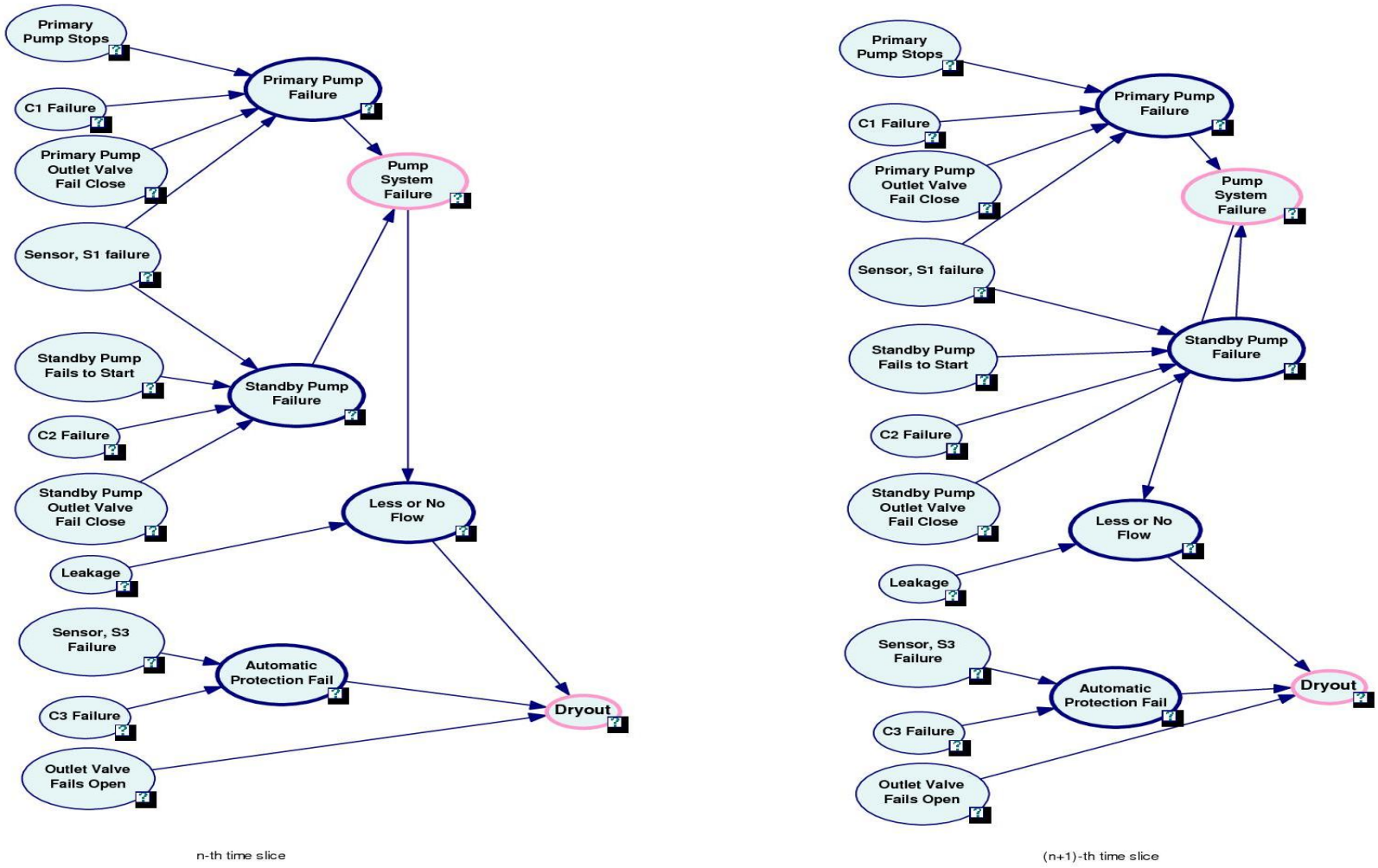


Figure 15. Dynamic Bayesian network with two time-slices without connection among nodes of two time-slices

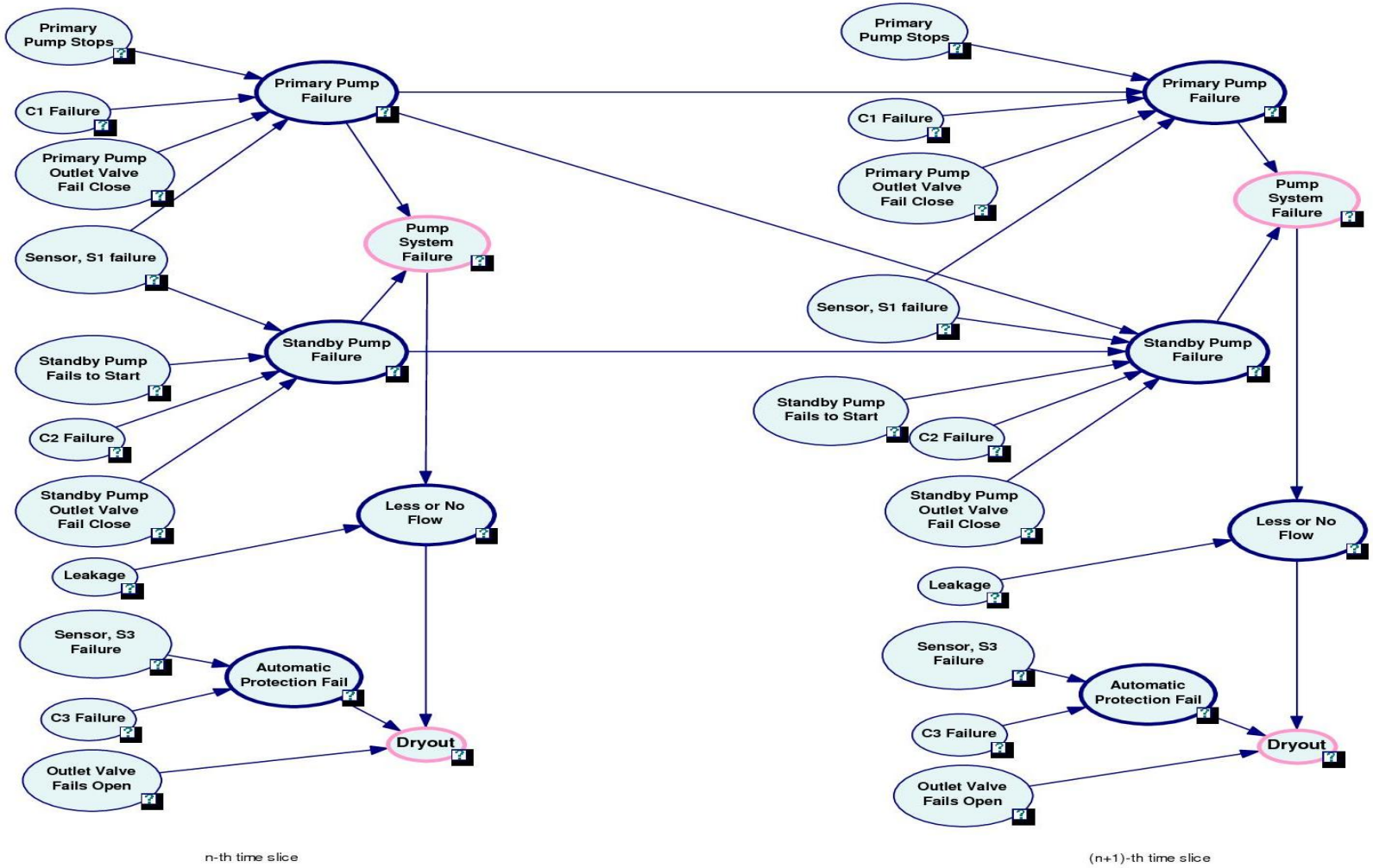


Figure 16. Mapped spare gate in dynamic Bayesian network

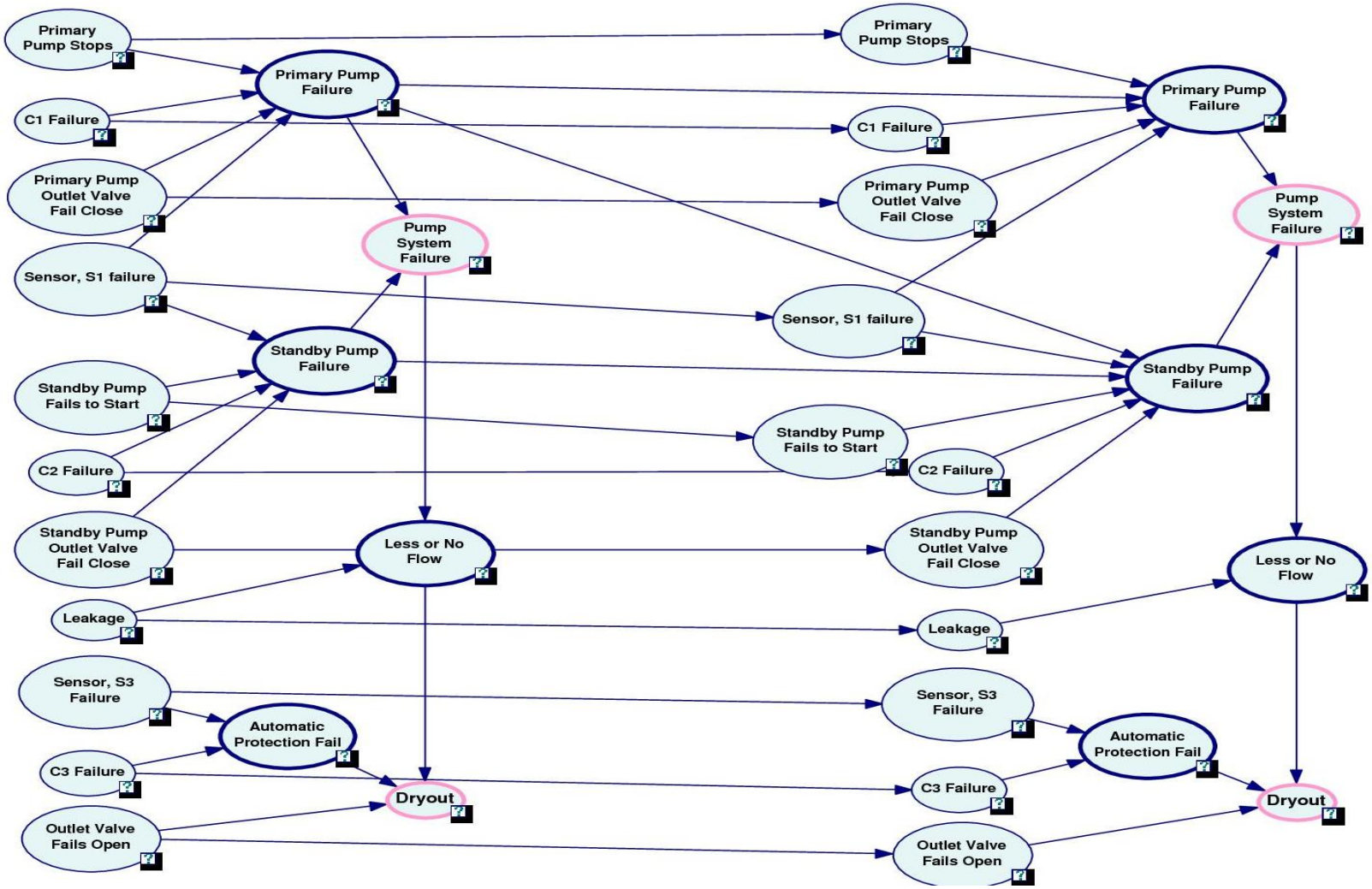


Figure 17. Dynamic Bayesian network with two time-slices

Table 10 Prior probabilities of root nodes of first time slice at 1 Week

Component	Failure Rate (per Hour)	Prior Probability at 1 Week
Primary pump	5.69×10^{-6}	1×10^{-3}
Standby Pump	2.52×10^{-6}	4×10^{-4}
Controller, C_1	4.34×10^{-5}	7×10^{-3}
Primary Pump Outlet Valve, V_1	5.5×10^{-7}	9×10^{-5}
Sensor, S_1	1.72×10^{-6}	3×10^{-4}
Controller, C_2	4.34×10^{-5}	7×10^{-3}
Standby Pump Outlet Valve, V_1	2.81×10^{-6}	5×10^{-4}
Sensor, S_3	1.72×10^{-6}	3×10^{-4}
Controller, C_3	4.34×10^{-5}	7×10^{-3}
Pipe Leakage	0.442×10^{-6}	7×10^{-5}
Outlet Valve, V3	2.31×10^{-6}	4×10^{-4}

Table 11 Probability of system dry-out for different equipment/component failure using different inspection internals

Component	Weekly	Monthly	3 Months	6 Months	1 Year	2 Year
Primary pump	1×10^{-3}	4×10^{-3}	0.012	0.024	0.048	0.094
Standby Pump	4×10^{-4}	0.002	0.005	0.011	0.022	0.043
Controller, C_1	7×10^{-3}	0.031	0.089	0.171	0.313	0.53
Primary Pump Outlet Valve, V_1	9×10^{-5}	3.9×10^{-4}	0.001	0.002	0.005	0.01
Sensor, S_1	3×10^{-4}	0.001	0.004	0.007	0.015	0.029
Controller, C_2	7×10^{-3}	0.031	0.089	0.171	0.313	0.53
Standby Pump Outlet Valve, V_1	5×10^{-4}	0.002	0.006	0.012	0.024	0.048
Sensor, S_3	3×10^{-4}	0.001	0.004	0.007	0.015	0.029
Controller, C_3	7×10^{-3}	0.031	0.089	0.171	0.313	0.53
Pipe Leakage	7×10^{-5}	3.1×10^{-4}	0.00095	0.002	0.004	0.008
Outlet Valve, V3	4×10^{-4}	0.002	0.005	0.01	0.02	0.039
Primary Pump System	0.008	0.063	0.192	0.353	0.585	0.831
Standby Pump System	0.008	0.049	0.149	0.284	0.502	0.772
Pump System	4×10^{-4}	0.004	0.033	0.11	0.307	0.65
Automatic Protection System	0.007	0.032	0.093	0.177	0.323	0.544
Less or No Flow	4×10^{-4}	0.005	0.034	0.111	0.31	0.652
Dry-out	0	0	1.6×10^{-5}	0.0002	0.002	0.014

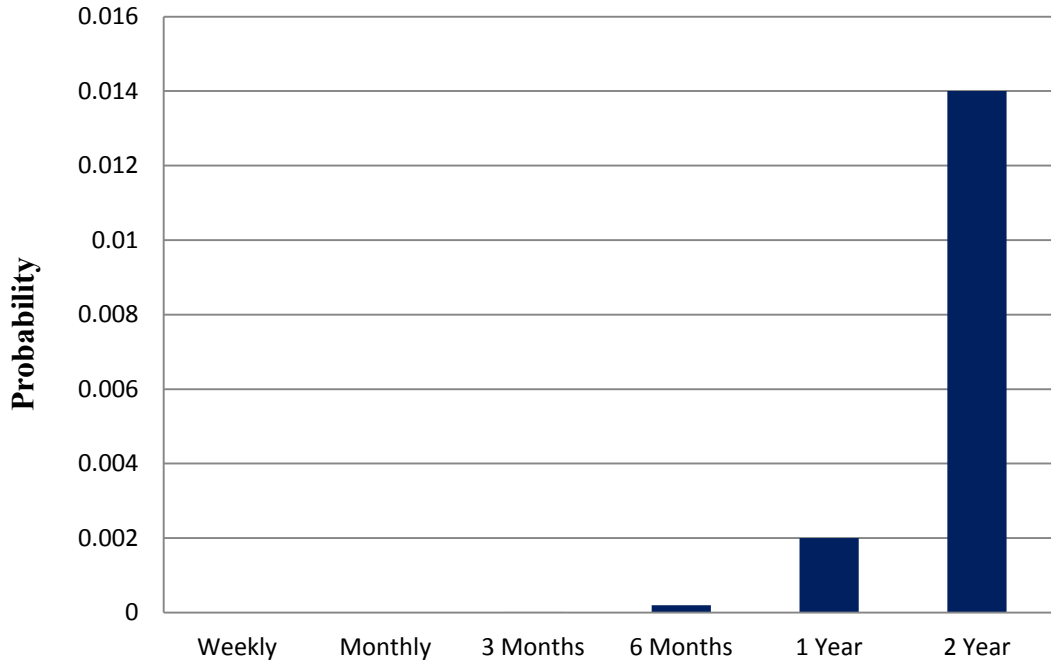


Figure 18. Dry-out probability upon different equipment/components failure using different inspection intervals: weekly, monthly, 3 months, 6 months, 1 year and every 2 year

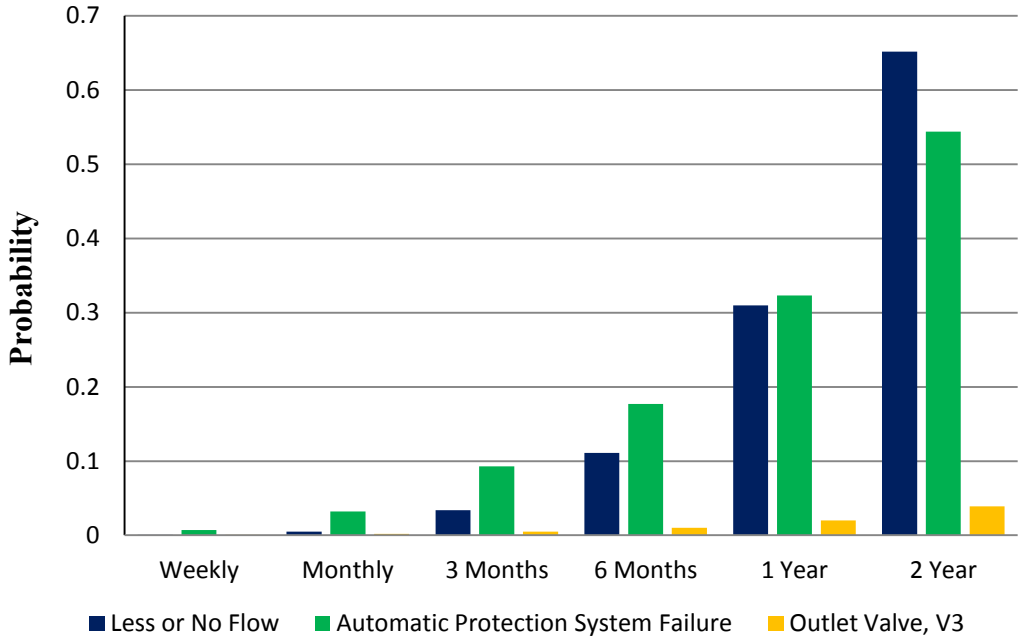


Figure 19. Less or no flow occurrence, automatic protection system failure and outlet valve fails open (failure) probability using different inspection intervals: weekly, monthly, 3 months, 6 months, 1 year and every 2 year

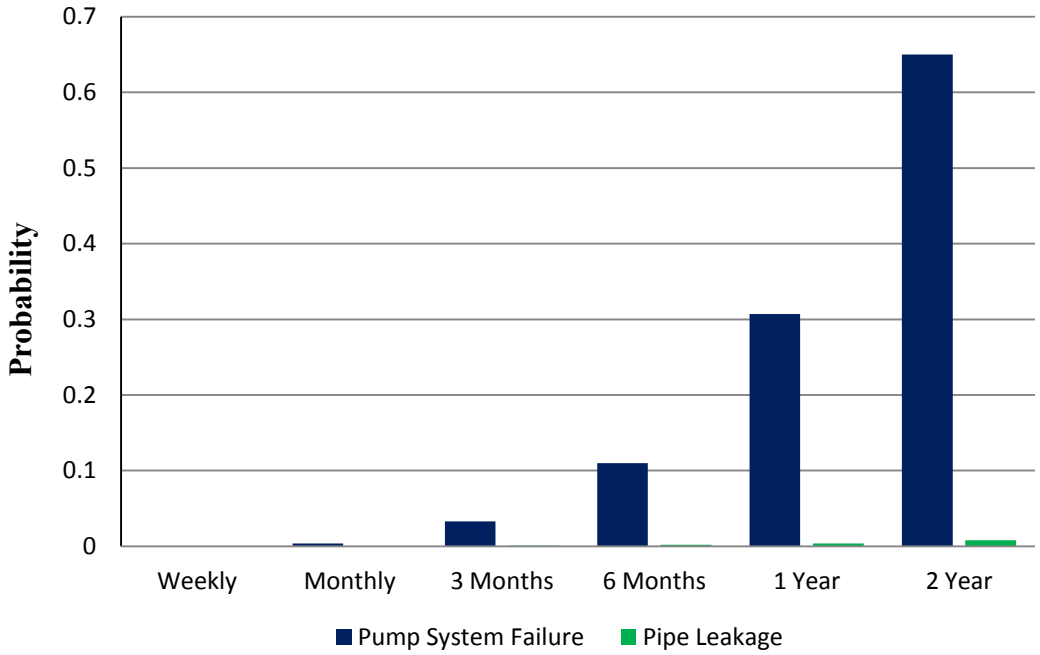


Figure 20. Pump system failure and pipe leakage probability using different inspection intervals

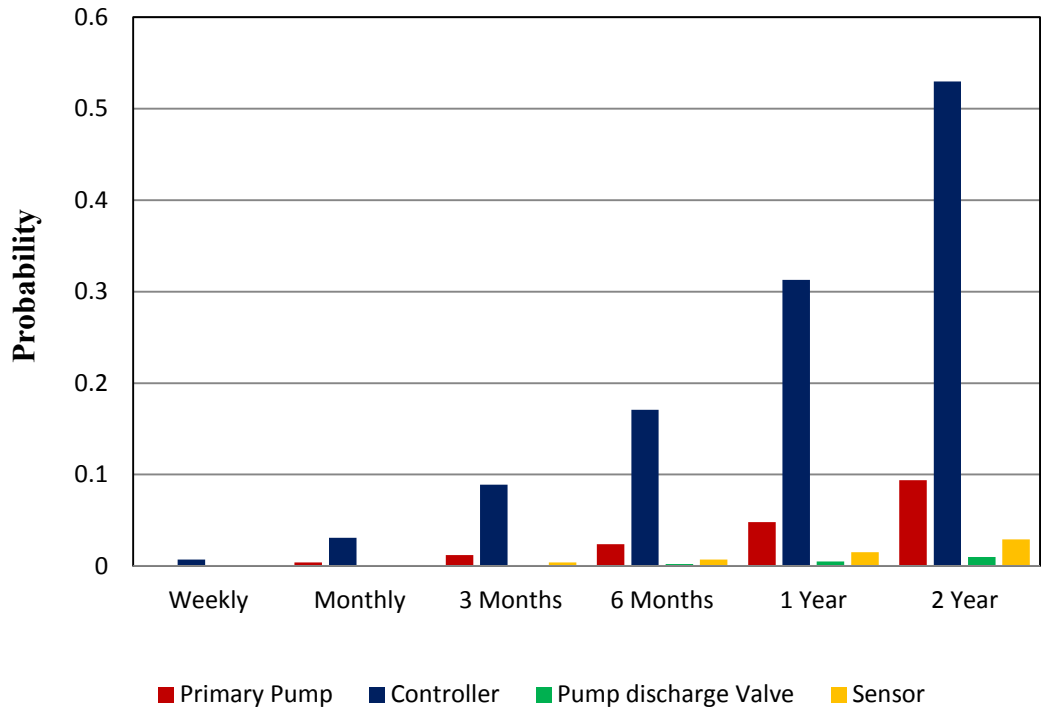


Figure 21. Primary pump and its system components failure probability using different inspection intervals

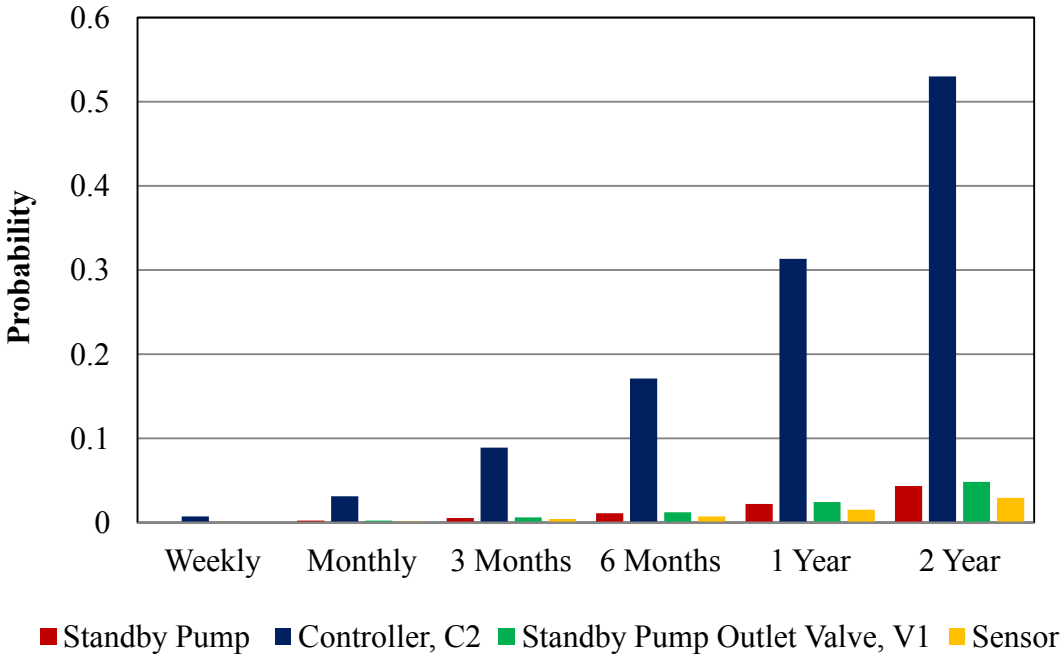


Figure 22. Standby Pump and its system components failure probability using different inspection intervals

In figure 21 and 22, the primary pump and its system components, standby pump and its system components failure probability using different inspection intervals are presented. Controller failure is more critical than other equipment/components failures in the system as its failure probability is much higher than others.

In this case study, a tank hold up problem is studied to demonstrate the effect of sequential dependency of one equipment/component on another equipment/component contributes to the risk.

4.2 Application of the Model

Bobbio et al. (2001) demonstrated Bayesian network's advantage in probability updating in presence of new information over other method. Khakzad et al. (2011) described other modeling prospects of Bayesian network such as incorporating multi-state variables, uncertainty handling. Bobbio et al. (2005) discussed potential of integrating effect of repair on the overall system. In this study, analysis is done to examine the effects of maintenance/repair in the system. Following maintenance schedule analysis is performed to demonstrate how the developed tool can be useful to provide optimum maintenance schedule:

- Every 3 months (3 months, 6 months, 9 months, 1 year)
- Every 6 months (6 months and 1 year)

For simplicity, it is assumed that maintenance work performed at any time slice will restore equipment/components conditional failure probability to the initial state i.e., failure probability will be equal to the failure probability of first time slice.

To demonstrate maintenance effect on the overall system, a node, named quality maintenance, is created in the Bayesian network. It is a deterministic node with two states, i.e., maintenance work performed or not performed. Quality maintenance has arc on the nodes of primary and stand-by pump system and automatic protection system. It refers that if maintenance work is performed that these nodes are conditionally dependent on the quality maintenance node. All the nodes in all time slices are provided their respective conditional probability. Figure 23 presents two-time slice Bayesian network of the tank holdup problem with quality maintenance node.

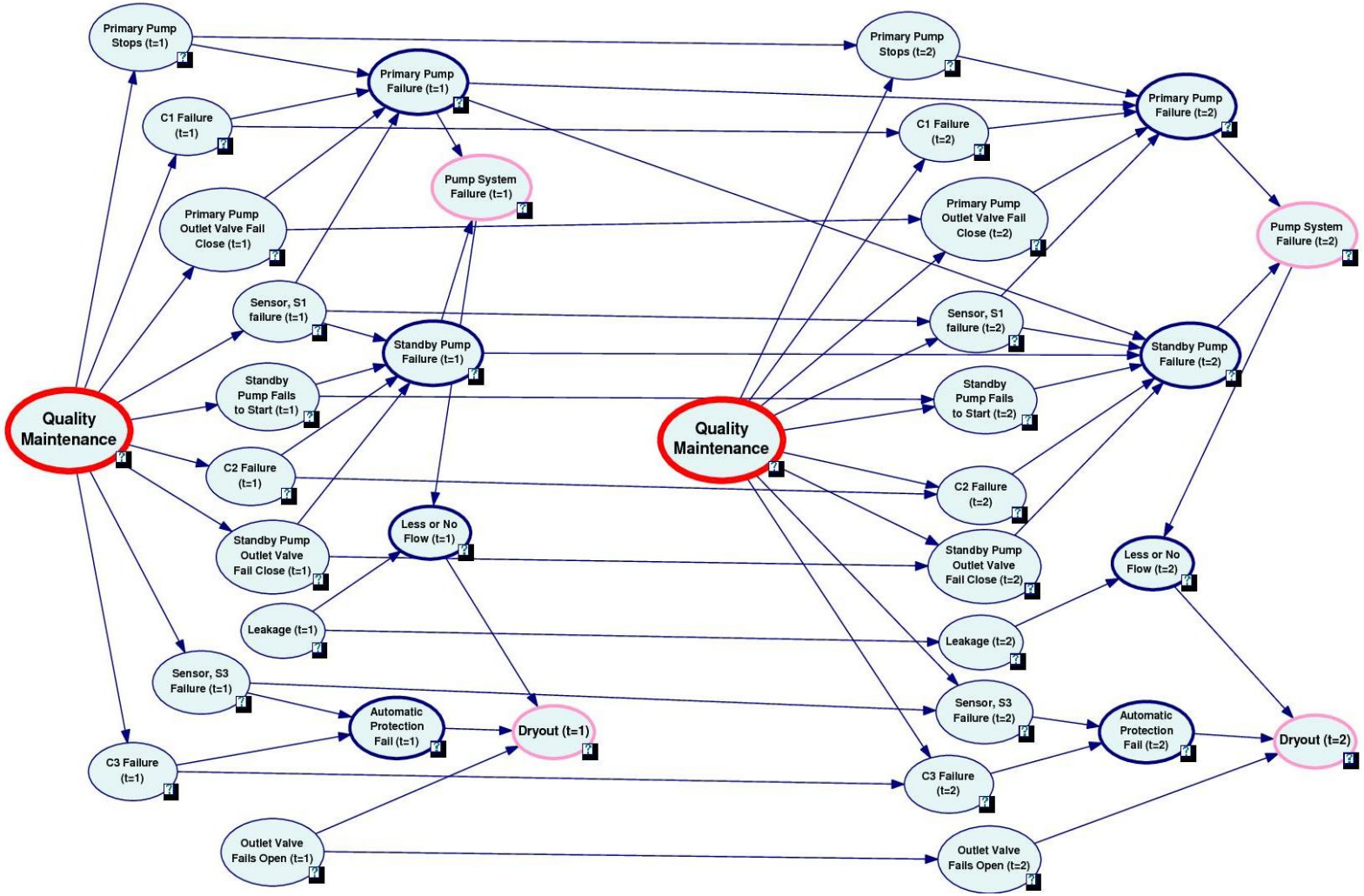


Figure 23. Dynamic Bayesian network when maintenance/repair is performed at every 3 months interval (3 months, 6 months etc.)

Table 12 Probability of system dry-out for different equipment/components failure if maintenance/repair takes place at every 3 months

Maintenance Schedule	3 Months	6 Months	9 Months	1 Year
Maintenance/Repair	Yes	Yes	Yes	Yes
Primary pump	0.011	0.012	0.012	0.012
Standby Pump	0.005	0.006	0.006	0.006
Controller, C_1	0.082	0.009	0.009	0.009
Primary Pump Outlet Valve, V_1	0.001	0.00099	0.00099	0.00099
Sensor, S_1	0.003	0.004	0.004	0.004
Controller, C_2	0.082	0.082	0.082	0.082
Standby Pump Outlet Valve, V_1	0.006	0.006	0.006	0.006
Sensor, S_3	0.003	0.004	0.004	0.004
Controller, C_3	0.082	0.082	0.082	0.082
Pipe Leakage	0.00097	0.002	0.003	0.005
Outlet Valve, V3	0.005	0.01	0.015	0.02
Primary Pump System Failure	0.13	0.213	0.314	0.465
Standby Pump System Failure	0.116	0.239	0.361	0.502
Pump System Failure	0.018	0.058	0.125	0.25
Automatic Protection System Failure	0.085	0.086	0.086	0.086
Less or No Flow	0.019	0.06	0.128	0.254
Dry-out	8.09×10^{-6}	5.16×10^{-5}	0.00016	0.00043

Table 13 Probability of system dry-out for different equipment/components failure if maintenance/repair takes place at every 6 months

Maintenance Schedule	3 Months	6 Months	9 Months	1 Year
Maintenance/Repair	No	Yes	No	Yes
Primary pump	0.012	0.012	0.024	0.012
Standby Pump	0.005	0.006	0.012	0.006
Controller, C_1	0.089	0.009	0.018	0.009
Primary Pump Outlet Valve, V_1	0.001	0.00099	0.002	0.00099
Sensor, S_1	0.004	0.004	0.008	0.004
Controller, C_2	0.089	0.082	0.163	0.076
Standby Pump Outlet Valve, V_1	0.006	0.006	0.012	0.006
Sensor, S_3	0.004	0.004	0.008	0.004
Controller, C_3	0.089	0.082	0.163	0.076
Pipe Leakage	0.00097	0.002	0.003	0.005
Outlet Valve, V3	0.005	0.01	0.015	0.02
Primary Pump System Failure	0.13	0.213	0.314	0.0465
Standby Pump System Failure	0.116	0.239	0.361	0.502
Pump System Failure	0.018	0.058	0.125	0.25
Automatic Protection System Failure	0.093	0.085	0.17	0.079
Less or No Flow	0.019	0.06	0.128	0.254
Dry-out	8.79×10^{-6}	5.13×10^{-5}	0.00032	0.0004

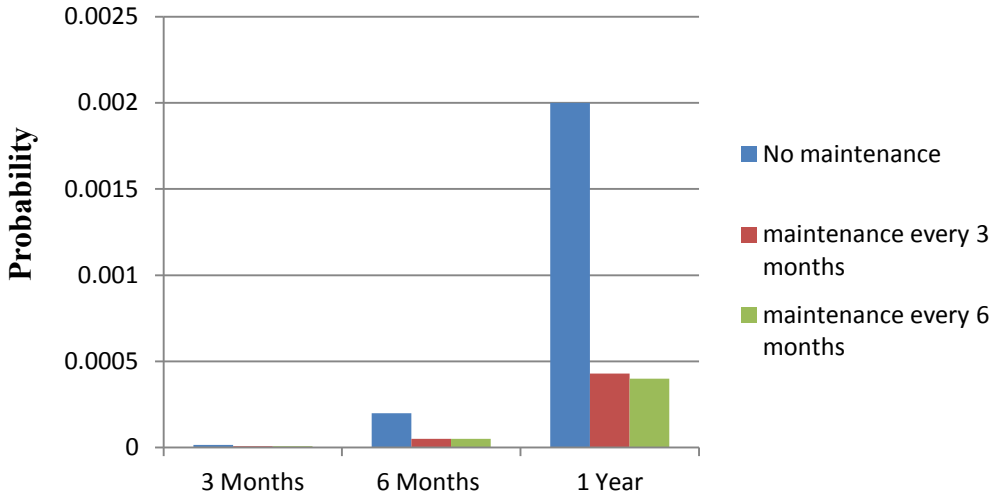


Figure 24. Dryout probability in the system with no maintenance, maintenance work in every 3 months and in every 6 months

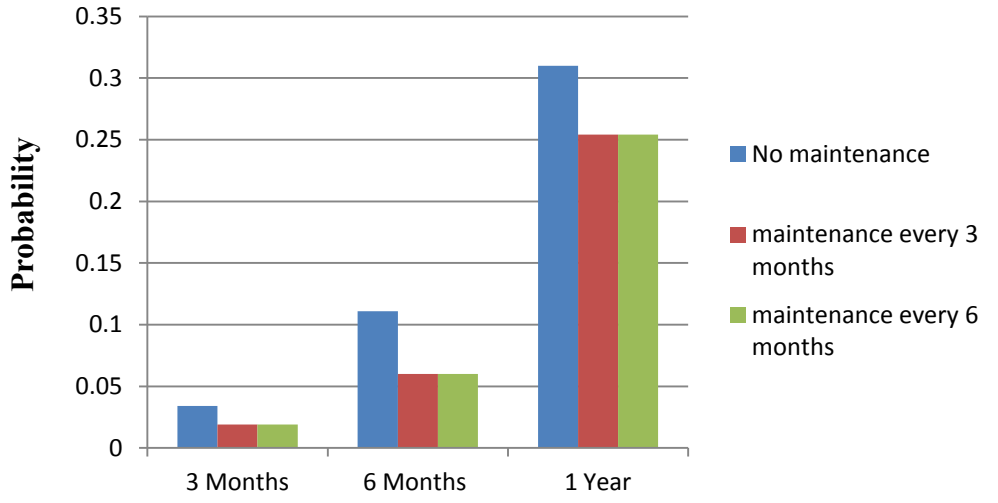


Figure 25. Less or no flow probability in the system with no maintenance, maintenance work in every 3 months and in every 6 months

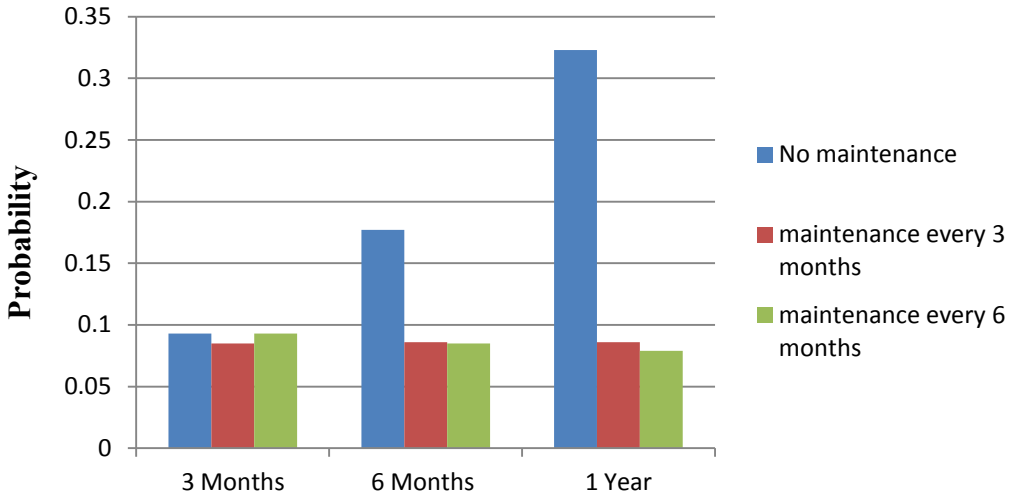


Figure 26. Automatic protection system failure probability in the system with no maintenance, maintenance in every 3 months and in every 6 months

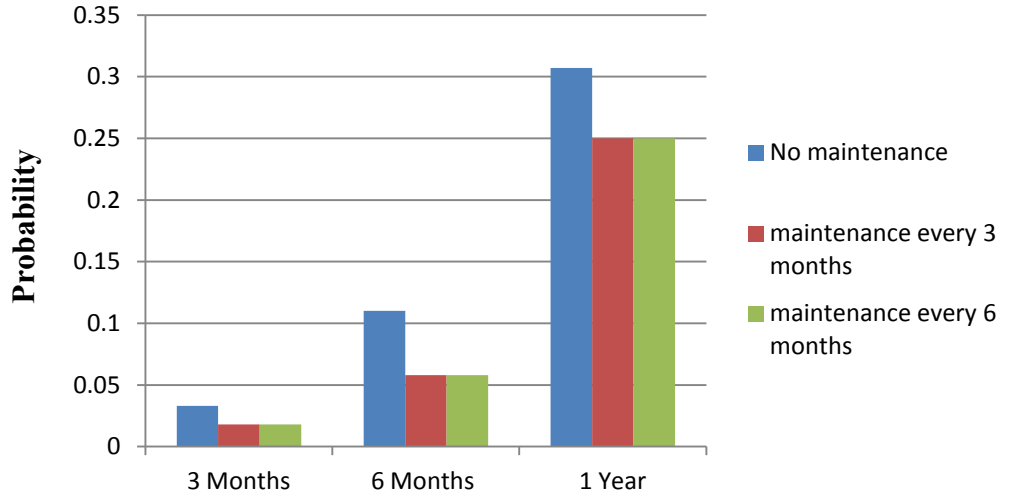


Figure 27. Pump system failure probability in the system with no maintenance, maintenance work in every 3 months and in every 6 months

In tables 12 and 13, the posterior probability obtained considering quality maintenance at every 3 months and 6 months are listed. Then the probabilities of dry-out in the system and major intermediate events, as automatic protection system failure, less or no flow probability, pump system failure probabilities after maintenance work at either 3 months or 6 months are plotted with the probability of equipment/component failure with no maintenance work in figure 24, 25, 26 and 27. From the figures, it is apparent that maintenance work can significantly reduce failure probability. Though, for this case study, maintenance work in every 3 months or 6 months does not provide significant differences. If cost of inspection, loss due to equipment downtime, parts replacement cost is available, then cost-benefit analysis should be done for optimum maintenance scheduling.

In this section, the application of developed method is demonstrated by case study on a tank hold up problem. Potential application of developed method and advantages are also described. It can be concluded that the developed method has the ability to quantify time-dependent effects on the process and provide updated probability with time.

5. GENERALIZING EVENT TREE IN BAYESIAN NETWORK

5.1 Introduction

An event tree graphically describes possible consequence scenarios if a critical event occurs and different safety barriers either function or not. It is an inductive approach that starts with an initiating event and it describes the sequences of different safeguards and human response. Application of event tree is very helpful to understand the logical relationship between the top event and safety barriers success or failure states. However, the event tree has limitation to explicitly represent all the factors that influence its construction and also to quantify the risk of dynamic system. Bayesian network has the ability to incorporate factors influencing event tree structure. In Bayesian network, the relationship of different events is described by the conditional probability table and clearly shows how an event is dependent on an earlier event. Also, any event tree mapped in Bayesian network can be expanded to include factors influencing all events occurrence. Thus precise estimation of risk can be obtained.

This chapter at firstly demonstrates a methodology of event tree of a chemical process systems mapping in Bayesian network based on Bearfield and Marsh (2005). Then it provides a graphical structure that shows different influencing factors of event occurrence.

5.2 Event Tree Mapping into Bayesian Network and Generalization Technique

Bearfield and Marsh (2005) described methodology of mapping event tree of

train derailment accident into Bayesian network and then provided some generalization procedure. Khakzad et al. (2012) adopted the procedure for demonstrating bow-tie analysis in Bayesian network. In section 5.2.1.1, general mapping procedure is demonstrated, followed by a case study in section 5.2.1.3 and then in section 5.2.1.4 exploiting Bayesian network modeling's capability to simplify procedure of mapping event tree is described. A case study on reactor system illustrates this procedure.

5.2.1 Mapping

The following procedure of mapping and generalizing event tree in Bayesian network is based on Bearfield and Marsh (2005):

- Create individual nodes for initiating event and all safety functions/barriers, i.e., if there is an initiating event and 'n' numbers of safety functions/barriers available to respond to that initiating event, then create 'n+1' nodes representing the initiating event and all safety barriers/functions
- All developed event nodes can have two states, i.e., failure and success.
- Create either a single consequence nodes and define 'p' number of states for different consequences or create 'p' numbers of individual consequence nodes with two states i.e., occur or not occur
- Connect arcs from one node to another depending on the events sequences and logical consequences

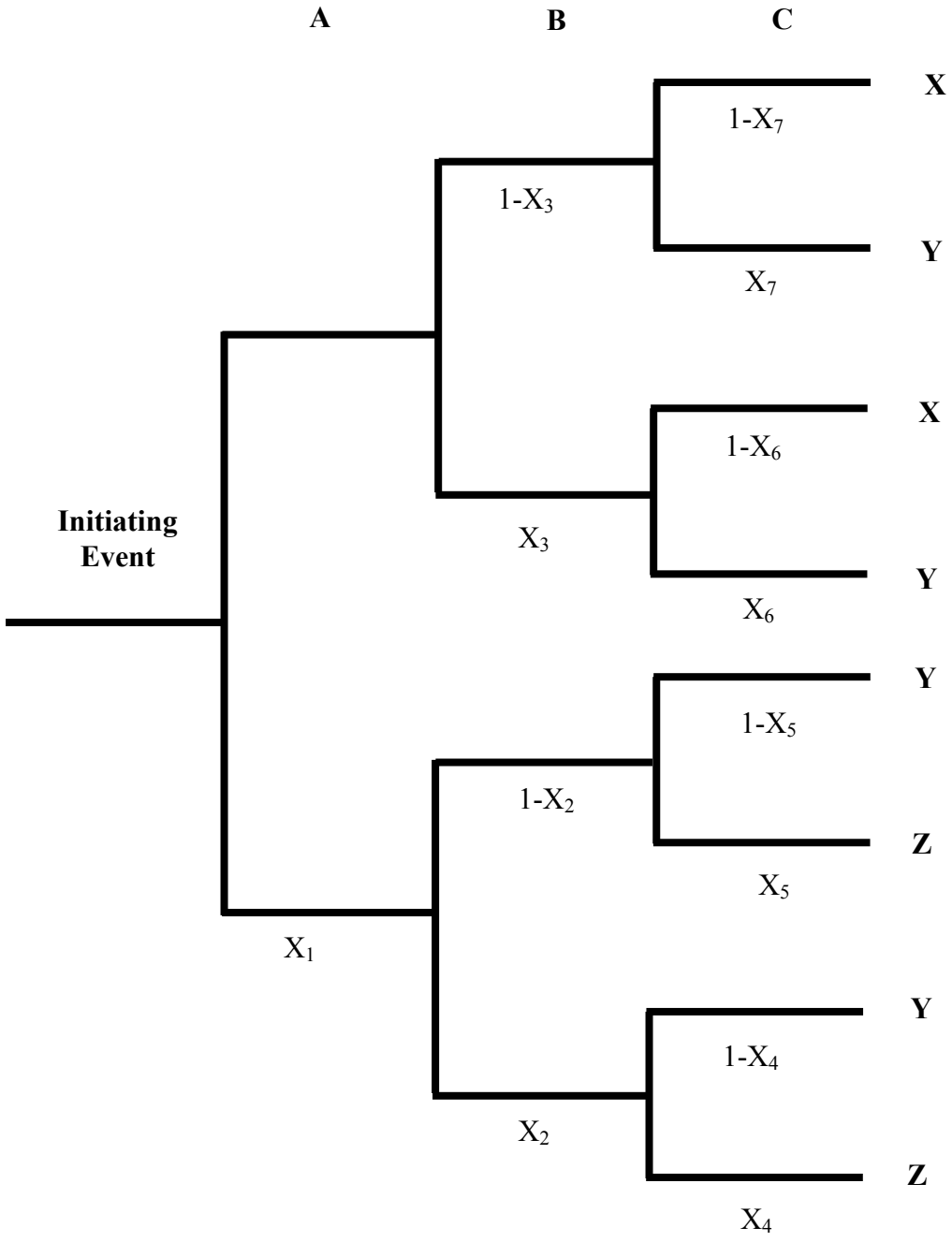


Figure 28. A general event tree

- All dependent nodes are provided with conditional dependency table
- Setting up conditional probability is illustrated with an example of event tree given in figure 28 and the relative its mapped Bayesian network is shown in figure 29. Tables 14, 15, 16 presents conditional probability tables for different events.

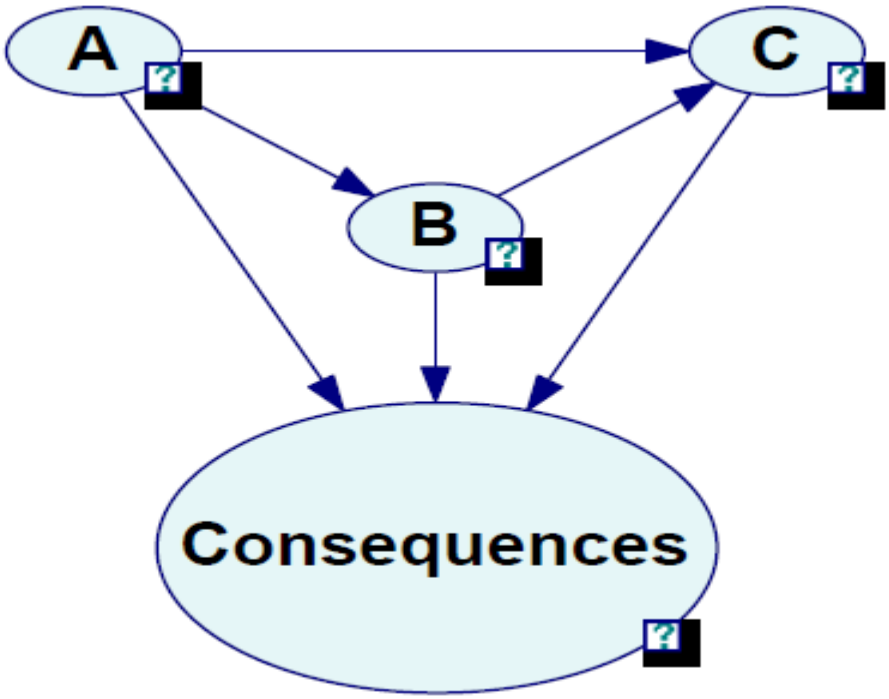


Figure 29. A general event tree mapped in Bayesian network

Table 14 Conditional probability table for Event node ‘A’

Failure Probability	X_1
Success Probability	$1-X_1$

Table 15 Conditional probability table for event node ‘B’ depending on state of event node ‘A’

Event A		Failure	Success
Event B	Failure	X_2	X_3
	Success	$1- X_2$	$1-X_3$

Table 16 Conditional probability table for event node ‘C’ depending on state of event node ‘A’ and event node ‘B’

Event A	Failure		Success	
Event B	Failure	Success	Failure	Success
Event C	X_4	X_5	X_6	X_7
	$1- X_4$	$1- X_5$	$1- X_6$	$1- X_7$

Table 17 Deterministic probability table for consequence node

Event A	Failure (F)				Success (S)			
Event B	Failure (F)		Success (S)		Failure (F)		Success (S)	
Event C	F	S	F	S	F	S	F	S
X	0	0	0	0	0	1	0	1
Y	0	1	0	1	1	0	1	0
Z	1	0	1	0	0	0	0	0

If all the consequences are presented in a single consequence node, then the conditional probability for different consequences is assigned as table 17. If the consequences are presented in different nodes, then conditional probability table for each consequence node has to be assigned separately.

5.2.2 Generalization

- An arc from an event node to the consequence node can be removed if the logical formulae refers that the event has no effect on the consequence
- An arc from one event node to another event node can be removed if that event's failure or success probability does not depends on the previous event node, i.e., the failure or success has the same probability of occurrence irrespective of the previous event state.

5.3 Case Study

Crowl and Louvar (2002) described a reactor system as shown in figure 30. In this reactor system, the temperature of reactor increases due to cooling system failure can lead to a runway reaction with pressure above the reactor bursting pressure. The cooling system is employed to remove excess energy of reaction. There is a thermocouple to measure the temperature inside the reactor and a temperature controller to actuate a control valve to maintain cooling water flow rate. In case of automatic protection system failure, a high temperature alarm is provided to alert the operator. Four safety functions are available. The first safety function is high temperature alarm to alert operator and the rest three functions depend on operator actions such as operator noticing high temperature, restart cooling and manual shut down of the reactor. Figure 31 is the event tree for the reactor system provided in figure 30. The success of failures of the safety barriers can lead to following three consequences:

A: Continue operation

B: Safe shutdown

C: Runway reaction

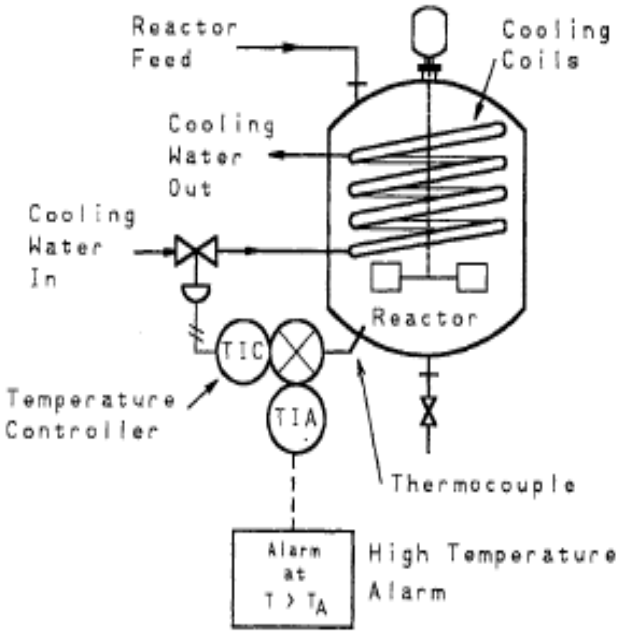


Figure 30. A chemical reactor system (Crowl and Louvar, 2002)

The description of the event tree is as follows:

- Initiating event for the event tree in figure 31 is loss of cooling which can be observed as an increase of temperature. In figure 32, a node named 'T increase' is created to represent the initiating event
- High temperature alarm alerts operator if alarm functions properly in case of temperature increases. Also, if alarm fails, then operator can either notice temperature increase by observing other indicators in the process or fails to notice it
- If operator notices temperature increase, then he starts restarting cooling. If restart of cooling succeeds, then system operation will continue. If it fails,

then the operator has to shutdown the operation to prevent runaway reaction. But, if operator fails to shut-down properly, then a run-away reaction results.

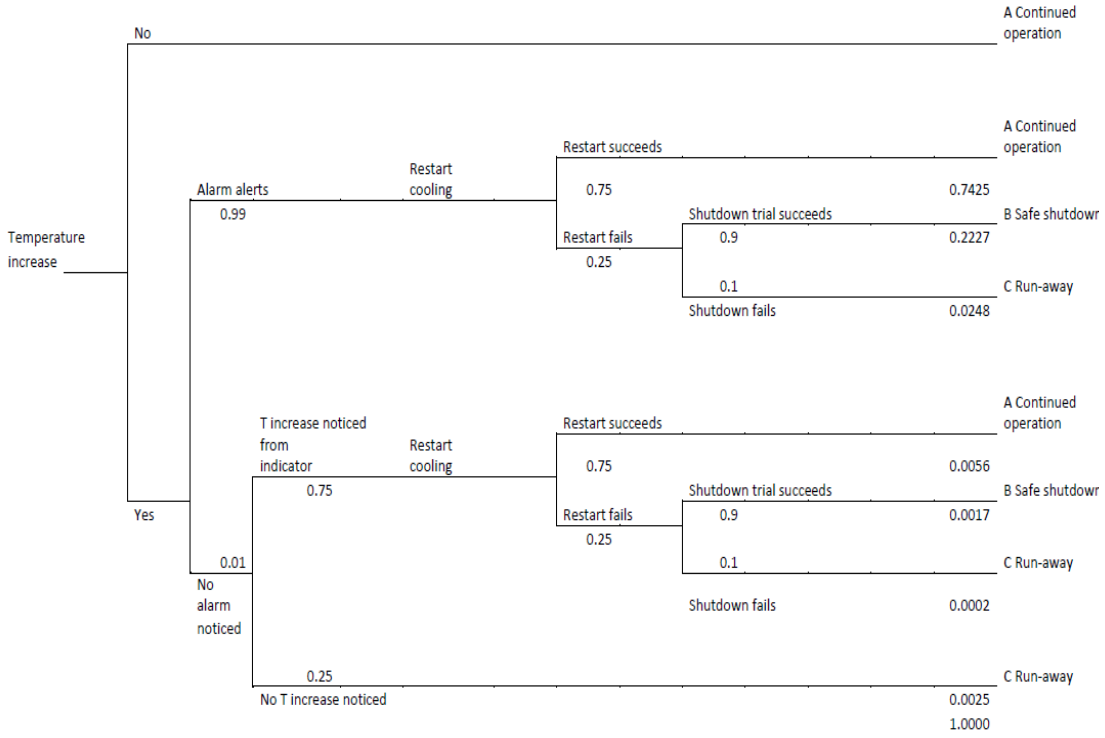


Figure 31. An event tree of a chemical reactor system

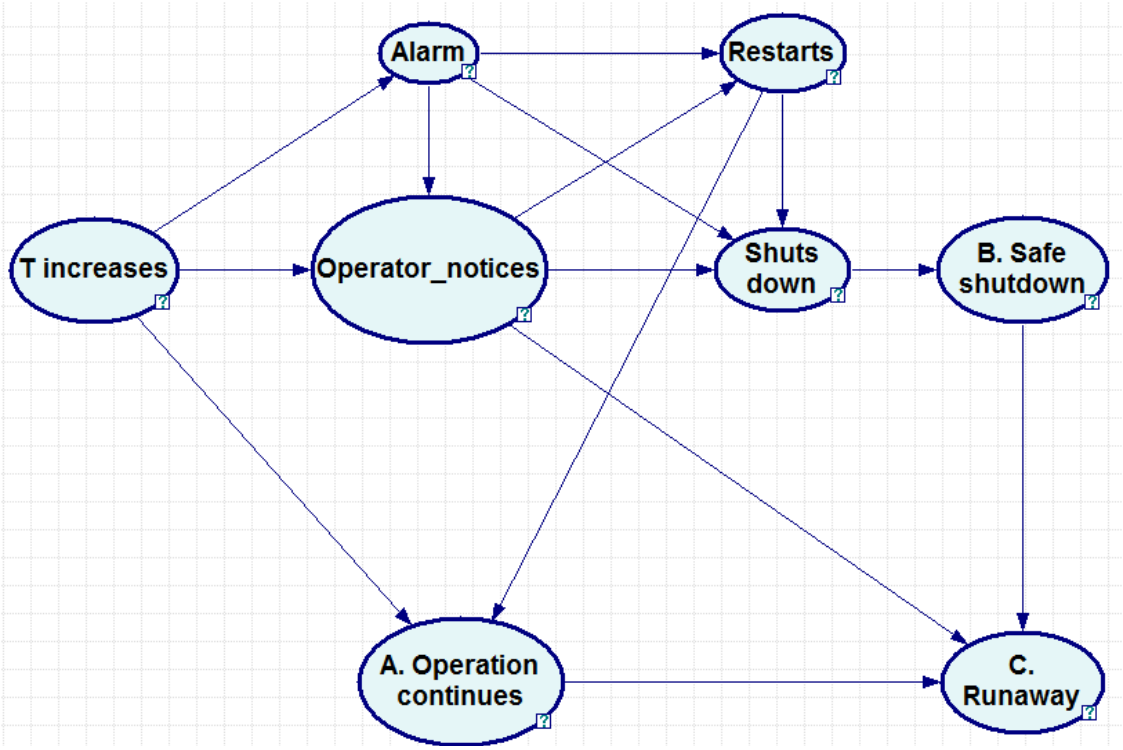


Figure 32. Mapped event tree in Bayesian network

In figure 32, the event tree is mapped into Bayesian network. Mapping procedure is as follows:

- For initiating event, temperature increase, a node is created and named 'T increase'
- For four safety functions, four event nodes are created and three consequences nodes are created for three consequence states
- Initiating event node has direct influence on the alarm and operator notices node. Therefore, two arcs from that node connects 'alarm' and 'operator-notices' node
- All safety function nodes are connected among each other through arcs

- As different consequences results from the initiating event and subsequent safety barriers failure, arcs are connected from initiating event node and safety function nodes to each consequence nodes
- Consequences nodes are also connected among themselves to represent their sequences

Conditional probability table for each event is provided in following tables 18, 19, 20 and 21.

Table 18 Prior probability of initiating event (temperature increase)

Event Not Occurred (No)	0
Event Occurred (Yes)	1

Table 19 Conditional probability table for alarm node given initiating event (temperature increases) node states

Temperature increase		No	Yes
Alarm	Not sound	1	0.01
	Sounds	0	0.99

Table 20 Conditional probability table for event node 'Operator_notices' given states of initiating event and alarm node

Temperature Increase		No		Yes	
Alarm		Not Sound	Sounds	Not Sound	Sounds
Operator Notices	Yes	0	0	0.75	0
	No	1	1	0.25	1

Table 21 Conditional probability table for 'operator re-starts cooling' node given state of 'operator_notices' nodes

Operator Notice		Yes	No
Re-start Cooling	Yes	0.75	0.75
	No	0.25	0.25

Table 22 Conditional probability table for 'operator shutdowns reactor' given states of 'operator notices temperature increase' and 'operator re-starts cooling'

Operator notices		No		Yes	
Operator re-starts cooling		Yes	No	Yes	No
Operator shutdowns reactor	Yes	0	0.90	0	1
	No	1	0.10	1	0

Table 23, 24 and 25 presents conditional probability tables for the consequence nodes.

Table 23 Conditional probability table for 'continue operation' consequence node

Temperature increases		No		Yes	
Operator re-starts cooling		Yes	No	Yes	No
Continue Operation	Not_continue	0	0	0	1
	Continued	1	1	1	0

Table 24 Conditional probability table for 'Safe shutdown' consequence node

Shutdown		Yes	No
Safe Shutdown	Succeeds	1	0
	No-shutdown	0	1

Table 25 Conditional probability table for 'Runaway reaction' consequence node

Continue Operation		Not_continue				Continues			
Operator notices temperature increasing		Yes		No		Yes		No	
Safe Shutdown		Succeeds	No-Shutdown	Succeeds	No-Shutdown	Succeeds	No-Shutdown	Succeeds	No-Shutdown
	Yes	0	0	0	1	0	0	0	0
	No	1	1	1	0	1	1	1	1

Calculated final probabilities of the consequences are:

A. continues operation probability is 0.748

B. Safe shutdown probability is 0.224

C. Runaway reaction probability in 0.027

In this section, an event tree mapping in Bayesian network is discussed. Bayesian network can easily propagate the conditional dependency of one event occurrence on

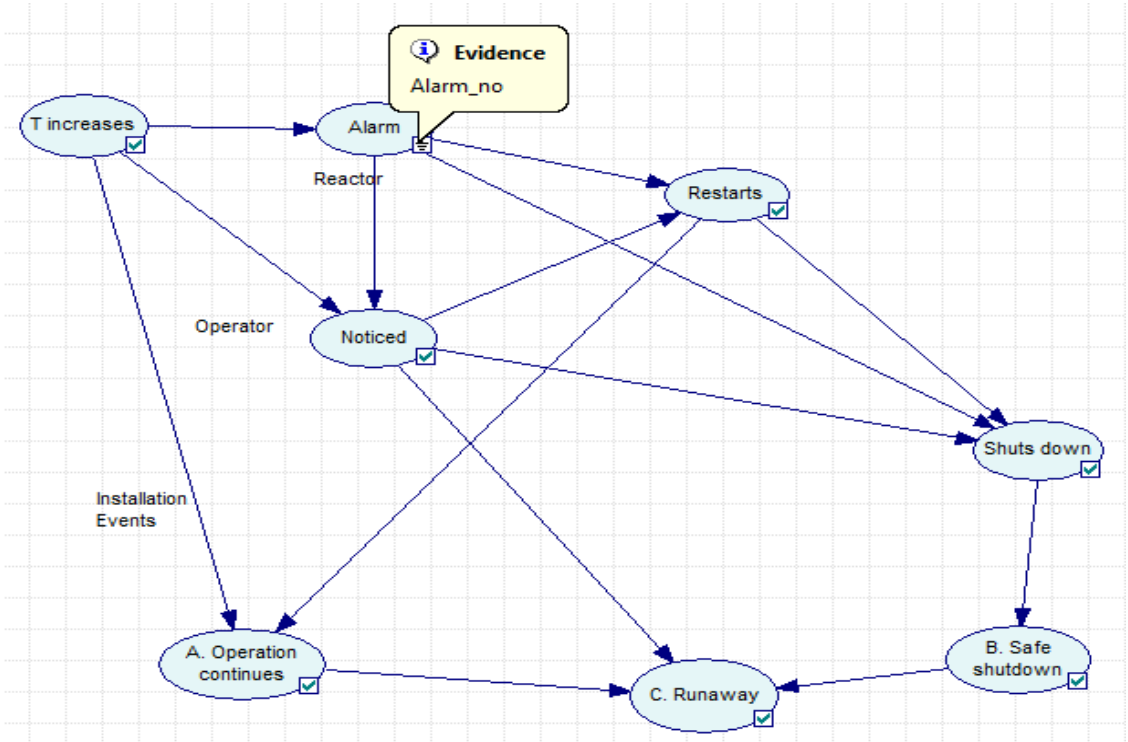


Figure 33. Bayesian network with 'alarm' node evidence value set to 1

another event and represent sequence of safety function/barriers failure results a particular consequence. For example, in Bayesian network, evidence can be set at any node and posterior probability and event propagation can be easily obtained. For example, in the Bayesian network shown in figure 33, the evidence of 'alarm' node is set up 1 which means that the alarm fails to alert the operator. In table 26, the prior and posterior probability of different safety function/barriers failure after the observation

Table 26 Prior and posterior probability table for all event and consequences

Event and Consequences	Prior Probability	Posterior Probability Probability (Each event/consequence occurrence | alarm fails to alert operator)
Temperature increase	1	1
Alarm	0.01	1
Operator notices	0.25	0.25
Operator re-starts cooling	0.25	0.438
Operator shut-down process	0.224	0.831
Operation continues	0.75	0.57
Safe shutdown	0.224	0.17
Runaway reaction	0.027	0.26

that alarm fails alert the operator are provided. From table 26, it can be concluded that if alarm fails to alert the operator, then the probability of operator failure to re-start cooling and shut-down process increases largely. Therefore, the consequences probability also changes. The probability of operation continues decreases from 0.75 to 0.57 and safety shutdown probability also decreases from 0.224 to 0.17 while the chances of a runaway reaction increase largely from 0.027 to 0.26. Thus setting different evidence in every node, the effect on other nodes can be easily obtained in Bayesian network.

Then, Bayesian network modeling is very flexible. The factors influencing each safety functions/barriers failure can be incorporated in Bayesian network using its modeling flexibility. For example, for above discusses case study, the initiating event is the increase in temperature due to loss of cooling. Different factors can cause loss of cooling i.e., cooling water supply system may fail, and pipeline may have blockage or leaks. The factors such as fatigue, job stress may cause operator failure to perform different actions. Conventional event tree has limitation to represent these factors which can be easily represented in Bayesian network. Thus, Bayesian network application provides advantages over event tree.

6. SUMMARY AND RECOMMENDATIONS

Bayesian network is relatively new technique in the field of process safety and risk analysis. Application of Bayesian network in risk analysis is very advantageous as it can combine the expert judgment and quantitative knowledge to estimate risk. Also, Bayesian network demonstrates changes of variables with time through reasoning process. Bayesian network is very much helpful for the area where availability of data is limited.

This study demonstrates discrete time dynamic Bayesian network for dynamic operational risk assessment. This methodology has the ability to provide updated probability with time, to incorporate inspection and testing time interval, which shows its effect on the critical event probability. As this technique is based on Bayesian network, it has the advantages of flexibility in modeling. This technique is very efficient to estimate risk in comparison to other techniques with respect to time and efforts. A case study on tank holdup problem demonstrates its application. In the next part, event tree is mapped and generalized using Bayesian network so that different factors influencing event tree construction can be incorporated. Case studies are provided to demonstrate the method.

This method provides methodology of dynamic operational risk assessment on discrete-time Bayesian network. Therefore, future work is intended to develop methodology of dynamic operational risk assessment on continuous time Bayesian network. For continuous time Bayesian network, probability distribution is required.

Thus using the concept of Bayesian statistics, the probability distribution obtained from generic data bases can be combined with plant specific data to obtain posterior information. Boudali and Dugan (2006) and Nodelman et al. (2002, 2003 and 2005) will be good starting points for this work.

In this study, brief application of dynamic Bayesian network is demonstrated for optimum risk based maintenance scheduling. Weber et al (2012) described different researches in this field in brief, which can be used for further reference. Celeux et al. (2006) described designing preventive maintenance using Bayesian network and Jones et al. (2010) demonstrated an application of Bayesian network for manufacturing industry's maintenance planning. There are scopes for detailed analysis for maintenance scheduling by incorporating different maintenance concepts such as "as good as new" and "as bad as old", different factors such as maintenance actions for chemical process industries. Also cost-benefit analysis can be performed within GeNIe software if cost of inspection, downtime, repair etc. is available.

Another dynamic aspect of process plant is equipment/components ageing phenomenon. In this research, the failure rate values are considered constant with time, but in practical life, due to ageing the failure rate tends to increase with time. Therefore, it is suggested to develop models in Bayesian network with the capability of quantifying ageing. It should be noted that when ageing is considered, then Weibull distribution is to be used in lieu of exponential distribution as the later one has memory-less property.

One of the objectives of this study is to demonstrate different risk assessment techniques parallelism with Bayesian network. In this study, mainly focus is given on

quantitative risk assessment techniques and their mapping in Bayesian network. For future work, it is recommended to map qualitative technique such as HAZOP, FMEA in Bayesian network and to develop risk ranking matrix based on the results. Therefore, Bayesian network may provide a unifying platform for risk analysis.

REFERENCES

Acosta, C. and Siu, N. (1993). Dynamic event trees in accident sequence analysis: application to steam generator tube rupture. *Reliability Engineering and System Safety*, 41(2), 135-154.

AIChE. (2000). *Guidelines for chemical process quantitative risk analysis*. New York: Center for Chemical Process Safety of the American Institute of Chemical Engineers.

Aldemir, T. (1987). Computer-assisted Markov failure modeling of process control systems. *IEEE Transactions on Reliability*, 36 (1), 133-144

Automated Reasoning Group, University of California, Los Angeles. (2010). *Samiam*. <http://reasoning.cs.ucla.edu/samiam/>. Accessed on 04/24/2012

BAYESIA SAS. (2010). *BayesiaLab 5.0*. <http://www.bayesian.com/en/products/bayesialab.php/>. Accessed on 04/24/2012

Bearfield, G. and Marsh, W. (2010). Generalising event trees using Bayesian networks with a case study of train derailment. *SAFECOMP 2005, LNCS 3688* –R. winther, B.A. Gran. and G. Dahll (Editors), Berlin: Springet-Verlag.

Bobbio A, Portinale L, Minichino M and Ciancamerla E. (2001). Improving the analysis of dependable systems by mapping fault trees into Bayesian networks. *Reliability Engineering and System Safety*, 71(3), 249-260.

Boudali, H. and Dugan, J.B. (2005). A discrete-time Bayesian network reliability modeling and analysis framework. *Reliability Engineering and System Safety*, 87 (3), 337-349.

Boudali, H. and Dugan, J.B. (2006). A continuous-time Bayesian network reliability modeling, and analysis framework. *IEEE Transactions on Reliability*, 55(1), 86-97

Cacciabue, P., Amendola, A. and Cojazzi, G. (1986). Dynamic logical analytical methodology versus fault tree: the case of the auxiliary feedwater system of a nuclear power plant. *Nuclear Technology*, 74(2), 195.

Celeus, G., Corset, F., Lannoy, A. and Ricard, B. (2006). Designing a Bayesian network for preventive maintenance from expert opinions in a rapid and reliable way. *Reliability Engineering and System Safety*, 91(7), 849-856.

Center for Chemical Process Safety (CCPS). (1989). *Guidelines for process equipment reliability data with data tables*. New York: Center for Chemical Process Safety of the American Institute of Chemical Engineers.

Center for Chemical Process Safety (CCPS). (2001). *Layer of protection analysis-simplified process risk assessment*. New York: Center for Chemical Process Safety of the American Institute of Chemical Engineers.

Crowl, D.A. and Louvar, J.F. (2002). *Chemical process safety: fundamentals with applications (2nd edition)*. New Jersey: Prentice Hall PTR.

Cullen, W. (1990). *The public inquiry into the Piper Alpha Disaster*. London: Stationery Office Books.

Dean, T. and Kanazawa, K. (1989). A model for reasoning about persistence and causation. *Computational Intelligence*, 5,142-150.

Decision Systems Laboratory, University of Pittsburgh. (2010). *GeNIe (Graphical Network Interface and SMILE (Structural Modeling, Inference, and Learning Enginer)*, Version 2.0 software. <http://genie.sis.pitt.edu/ Accessed 04/22/2012>.

Delvosalle, C. , Fievez, C., Pipard, A. and Debray, B. (2006). ARAMIS project: a comprehensive methodology for the identification of reference accident scenarios in process industries. *Journal of Hazardous Materials*, 130, 200-219.

Donohue, S.K. and Dugan, J.B. (2003). Modeling the "Good enough to release" decision using V&V preference structure and Bayesian belief networks. *Annual Reliability and Maintainability Symposium.* < http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1182051>.

Dugan, J.B., Bavuso, S.J. and Boyd, M.A. (1990). Fault trees and sequence dependencies. *Proceedings of Annual Reliability and Maintainability Symposium*. 286-293. < http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=00067971>.

Dugan, J.B., Bavuso, S.J. and Boyd, M.A. (1992). Dynamic fault-tree models for fault-tolerant computer systems. *IEEE Transactions on Reliability*, 41(3), 363-377.

Heckerman, D. (1995). *Technical report-a tutorial on learning with Bayesian networks*. Washington: Microsoft Research. < http://research.microsoft.com/pubs/69588/tr-95-06.pdf>.

Hudson, L., Ware, B., Laskey, K. and Mahoney, S. (2002). *Technical report-an application of Bayesian networks to antiterrorism risk management for military planners*. Digital Sandbox, Inc. <http://digilib.gmu.edu:8080/jspui/bitstream/1920/268/1/Antiterrorism.pdf>.

HUGIN EXPERT. (2012). *HUGIN graphical user interface/HUGIN decision engine 7.6*. <http://www.hugin.com/productsservices/products/release-notes/>. Accessed on 04/24/2012

Hurdle, E.E., Bartlett, L.M. and Andrews, J.D. (2009). Fault diagnostics of dynamic system operation using a fault tree based method. *Reliability Engineering and System safety*, 94(9), 1371-1380

Jones, B., Jenkinson, I., Yang, Z. and Wang, J. (2010). The use of Bayesian network modeling for maintenance planning in a manufacturing industry. *Reliability Engineering and System Safety*, 95(3), 267-277.

Khakzad, N., Khan, F. and Amyotte,P. (2011). Safety analysis in process facilities: Comparison of fault tree and Bayesian network approaches. *Reliability Engineering and System Safety*, 96, 925-932.

Khakzad, N., Khan, F. and Amyotte, P. (2012). Dynamic safety analysis of process systems by mapping bow-tie into Bayesian network. *Process Safety and Environment Protection*, http://dx.doi.org/10.1016/j.psep.2012.01.005. Accessed 04/12/2012.

Khan, F.I. and Abbasi, S.A. (1998). Techniques and methodologies for risk analysis in chemical process industries. *Journal of Loss Prevention in the Process Industries*, 11(4), 261-277.

Kjaerulff, U. (1995). A computational system for dynamic time-sliced Bayesian networks. *International Journal of Forecasting*, 11, 89-101.

Lighttwist Software. (2008). *Uninet*. <http://www.lighttwist.net/wp/>. Accessed on 04/24/2012

Magott, J. and Skrobanek, P. (2012). Timing analysis of safety properties using fault trees with time dependencies and timed state-charts. *Reliability Engineering and System Safety*, 97 (1), 14-26.

Mannan, M.S. (2005). *Lees' loss prevention in the process industries: hazard identification, assessment and control.* Massachusetts: Butterworth-Heinemann.

Markowski, A.S. (2006). *Layer of protection analysis fir the process industries*. Polish Academy of Sciences.

Markowski, A.S. and Kotynia, A. (2011). Bow-tie model in layer of protection analysis. *Process Safety and Environmental Protection*, 89(4), 205-213.

McNaught, K.R. and Zagorecki, A. (2010). Using dynamic Bayesian networks for prognostic modeling to inform maintenance decision making. *The IEEE International Conference on Industrial Engineering and Engineering Management*, Hong Kong.

Mokhtari, K., Ren , J., Roberts, C. and Wang, J. (2011). Application of a generic bow-tie based risk analysis framework on risk management of sea ports and offshore terminals. *Journal of Hazardous Materials*, 192(2), 465-475.

Montani, S., Portinale, L. and Bobio, A. (2005). Dynamic Bayesian networks for modeling advanced fault tree features in dependability analysis. *Advances in Safety and Reliability*-Kolowrocki (ed.), London: Taylor and Francis Group.

Murphy K. (2002). *Dynamic Bayesian networks: representation, inference and learning*. PhD Thesis, University of California, Berkley, CA.

Murphy, K. (2007). Software for graphical models: a review. *International Society for Bayesian Analysis Bulleting*, 14(4), 13-15.

Murphy, K. (2007). *Bayes net toolbox (BNT) for Matlab*. <http://code.google.com/p/bnt/>. Accessed on 04/24/2012

Neapolitan, R.E. (1990). *Probabilistic reasoning in expert systems-theory and algorithms*. New York: John Wiley and Sons.

Nivolianitou, Z., Amendola, A. and Reina, G. (1986). Reliability analysis of chemical processes by the DYLAM approach. *Reliability Engineering*, 14, 163-182

Nodelman, U., Shelton, C.R. and Koller, D. (2002). Continuous time Bayesian networks. *Proceedings of the Eighteenth Conference on Uncertainty in Artificial Intelligence*, 378-387.

Nodelman, U., Shelton, C.R. and Koller, D. (2003). Learning continuous time Bayesian networks. *Proceedings of the Nineteenth Conference on Uncertainty in Artificial Intelligence*, 421-458.

Nodelman, U., Koller, D. and Shelton, C.R. (2005). Expectation propagation for continuous time Bayesian networks. *Proceedings of the Twenty-First Conference on Uncertainty in Artificial Intelligence*, 431-440.

The Norwegian Petroleum Directorate (NPD). (1981). *Guidelines for safety evaluation of platform conceptual design*. Stavanger: Norway.

Pasman, H. J. and Rogers, W.J. (2011). BBN, a tool to make LOPA more effective, QRA more transparent and flexible, and therefore to make safety more definable. *14th Annual Symposium*, Mary Kay O'Connor Process Safety Center, College Station, Texas.

Pearl, J. (1988). *Probabilistic reasoning in intelligent systems: networks of plausible inference*. Morgan Kaufmann Publishers Inc.

Reliability Analysis Center. (2003). The applicability of Markov analysis methods to reliability, maintainability and safety. *START-selected topic in assurance related technologies*, 10(2).

SINTEF Industrial Management. (2002). *OREDA offshore reliability data handbook*. Norway: OREDA participants

Siu, N. (1994). Risk assessment for dynamic system: an overview. *Reliability Engineering and System Safety*, 43(1), 43-73.

The U.K. Health and Safety Executive. (1992). *The Offshore installations (safety case) regulations 1992*. <http://www.legislation.gov.uk/uksi/1992/2885/introduction/made/>. Accessed on 04/23/2012

U.S. Chemical Safety and Hazard Investigation Board (CSB). (2007). *Investigation Report: refinery explosion and fire, Bp Texas City, Texas, March 23, 2005*, <http://www.csb.gov/assets/document/CSBFinalReportBP.pdf>.

U.S. Chemical Safety and Hazard Investigation Board (CSB). (2012). <http://www.csb.gov./ Accessed 04/06/2012>. Accessed on: 04/06/2012

US National Commission on BP Deepwater Horizon Oil Spill and Offshore Drilling. (2011). *Deepwater: The gulf oil disaster and the future of offshore drilling*. <http://www.oilspillcommission.gov/final-report/>. Accessed 04/09/2012.

US Nuclear Regulatory Commission. (1975). *Reactor Safety Study (WASH-1400 (NUREG-75/014)*.

Vinnem, J.E. (1998). Evaluation of methodology for QRA in offshore operations. *Reliability Engineering and System Safety*, 61(1/2), 39-52.

Vomlel, J. (2005). *Some applications of Bayesian networks. Institute of Information Theory and Automation*-Academy of Sciences of the Czech Republic. <http://www.wtia.cas.ca/vomlel/>. Accessed on 04/23/2012.

Weber, P., Medina-Oliva, G., Simon, C. and Lung, B. (2012). Overview on Bayesian networks applications for dependability, risk analysis and maintenance areas. *Engineering Applications of Artificial Intelligence*, 25(4), 671-682.

Yang, X. (2010). *The development and application of dynamic operational risk assessment in oil/gas and chemical process industry*. PhD dissertation, Texas A&M University, College Station, TX.

Yang, X. and Mannan, M.S. (2010). The development and application of dynamic operational risk assessment in oil/gas and chemical process industry. *Reliability Engineering and System Safety*, 95, 806-815.

Yun, G.W., Rogers, W. J. and Mannan, M.S. (2009). Risk assessment of LNG importation terminals using the Bayesian-LOPA methodology. *Journal of Loss Prevention in the Process Industries*, 22, 91-96.

VITA

Shubharthi Barua received his Bachelor of Science degree in chemical engineering from Bangladesh University of Engineering and Technology, Dhaka, Bangladesh in March 2009. After that, he worked for Tyser Risk Management Bangladesh Limited as a Risk Engineer and Karnaphuli Fertilizer Company Limited (KAFCO) as Trainee Engineer for one and one-half years. He enrolled in the Safety Engineering program offered by Department of Chemical Engineering at Texas A&M University in August 2010. Besides research, he has been involved in several industrial and academic projects at Mary Kay O'Connor Process Safety Center. He received his M.S. degree in August 2012. His research interests include quantitative risk assessments, consequence modeling, abnormal situation management, offshore and refinery process safety.

His contact information is: Shubharthi Barua, C/O: Dr. M. Sam Mannan, 3122 TAMU, Room 244, College Station, TX 77843-3122.. He can be reached by email at shubharthi.barua@yahoo.com