Real Time Risk Monitoring in a Processing System using Bayesian Networks

by

© Emily Butt

A Thesis submitted to the

School of Graduate Studies

in partial fulfilment of the requirements for the degree of

Master of Engineering

Faculty of Engineering and Applied Science

Memorial University of Newfoundland

May 2019

St. John's Newfoundland and Labrador

Abstract

Safety and risk are essential components of process industries. The research objective of this thesis is to develop a method to measure and monitor safety in terms of real-time risk of a process system failure. The risk monitoring concept was developed using event trees and Bayesian networks. Process instrument data such as flowrate was used as a basis for the risk probability calculations. The risk monitoring methodology was developed and applied to the Williams Geismar reboiler rupture and fire in 2013. The risk level of the reboiler was examined based on the original design prior to failure and an updated design based on recommendations made by the CSB. The accident probability was decreased by 96% and risk level was reduced by 76.9%. By plotting the risk of a process overtime, future projections of risk can be predicted and action can be taken to prevent accidents before they could occur.

Acknowledgements

First, I would like to thank my thesis supervisors Dr. Faisal Khan and Dr. Nicola Paltrinieri for their expertise, guidance, patience and understanding. Thank you Dr. Khan for first igniting my interest in the study of safety and risk engineering.

I acknowledge the financial support provided by the collaboration between Norwegian University of Science and Technology (NTNU), of Trondheim, Norway and Memorial University of Newfoundland that made this research possible.

Finally, I would like to thank my mom and dad, Elaine and Craig, and my sister Meghan. Their constant encouragement throughout my entire life has inspired and motivated me to do my very best. I would also like to thank my partner and best friend Devin for his love and unfailing support.

Thank you again,

Emily

Table of Contents

List of Figures

List of Tables

1. Chapter 1: Introduction

1.1. Process Safety and Risk

Safety and risk are essential components of process industries. Process safety can be defined the identification of process hazards of and the use of technology to prevent and eliminate the occurrence of accidents (Crowl & Louvar, 2011). In terms of process safety, risk is determined by quantifying the magnitude of loss and the likelihood of an incident. Loss can include human injury, environmental damage and economic loss due to damaged assets and reputation. Nearly all process industries involve the use of hazardous materials and have risks. Risk cannot be eliminated. However, risk can be minimized to an acceptable level.

1.2. Research Objective

The research objective of this thesis is to develop a method to measure and monitor the safety in terms of real-time risk of a process system failure. This objective will be achieved in two parts. The first part of the thesis will explore the development of the methodology and the second part will apply the methodology to a case study to demonstrate real world applications.

The methodology has used Bayesian networks method. The Bayesian networks models are developed and analyzed using GeNie 2.2 Academic by Bayesfusion, LLC, to model Bayesian Networks. (https://download.bayesfusion.com/files.html?category=Academia)

1.3. Thesis Outline

The thesis structure is as follows:

Chapter Two presents a literature review based on safety and risk in process industries. Process safety monitoring and accident modelling techniques are described. Six major accidents within the past 10 years are also discussed here.

Chapter Three presents the methodology for predicting the incident of an overflowing tank and the subsequent risk associated with various physical factors. The simple tank is redesigned six times to show how increasing safety measures reduced the likelihood of an incident and the overall risk. Chapter Four presents a real world case study where the methodology of chapter three is applied. The case studied is the shell and tube heat exchanger rupture and fire in the Williams Geismar Olefins Plant on June 13th of 2013 (CSB, Williams Geismar Olefins Plant Reboiler Rupture and Fire Geismar, Louisiana, 2016). The risk of overpressure of a reboiler associated with olefins or alkenes is discussed. The risk of the heat exchanger operation is assessed real time. Chapter Five summarizes and concludes the impact of the presented work. The potential of future studies based on this work are also discussed.

1.4. Novelty of the Work

The developed methodology presented here is unique and also the application of the methodology. This is a novel attempt to measure safety real time using risk factors. This thesis has presented concept in simple and easy to follow way. The case studies are also presented in simplified form so that readers can follow through the steps and understand the strength of the approach. This work put forward a new way to assess and monitor safety of process operations.

2. Chapter 2: Literature Review Monitoring Process Safety and Risk

In process industries, accident modelling is used to answer these two important questions: why does an accident happen and how does an accident happen (Al-shanini, Ahmad, & Khan, Accident modelling and analysis in process industries, 2014). Risk assessments are part of accident modelling and are vital to the safe design, development and operation of a process. Risk assessments are used to determine how safe a process is and what appropriate safety measures should be installed to minimize any risks. Risk assessments are also used to determine which safety measures are the most economically feasible (Crowl & Louvar, 2011). According to a review completed by Chakraborty et al. there is currently no universally accepted system to detect early signs of safety deterioration and increase in risk (Chakraborty, 2003). This thesis presents a method to measure risk of a process system in real time.

Although there are many safety measures and models developed to make a process safer accidents can still occur. The term accident is used to describe an event that happens unexpectedly and unintentionally. Though the term accident implies that an accident is unexpected many have warning signs that indicate an accident will occur before it happens. Many accident reports indicate that there was safety performance of a process was degrading or non-existent prior to the event (Al-shanini, Ahmad, & Khan, Accident modelling and analysis in process industries, 2014). Table 2-1 describes six process accidents that have occurred in the past 10 years. In the case of the Tesoro Martinez Sulfuric Acid Spill, the same consequence was experienced by two separate accidents within one month of each other.

Table 2-1: List of Process Industry Accidents

Date	Accident name	Location	Type	Reason	Impact	Safety Factor	Reference
April 20, 2010	Macondo Well Blowout	Northern Gulf of Mexico	Fire, Explosion and Oil spill	Loss of well control to release of Hydrocarbons to the platform, hydrocarbons ignited resulting in fire and explosions that sunk the platform and damaged well bore released oil	11 killed, 63 injured, severe environmental damage	Mechanical; Operational	(CSB, Investigation Report: Drilling Rig Explosion and Fire at the Macondo Well, 2016)
December 9, 2010	AL solutions Metal Dust Explosion and Fire	New Cumberland, West Virginia, USA	Fire and Explosion	titanium and zirconium particulates ignited in the blender that was processing zirconium	3 killed, 1 injured	Mechanical	(CSB, Metal Dust Explosion and Fire , 2014)
June 13, 2013	Williams Geismar Olefins Plant	Geismar, Louisiana, USA	Fire and Explosion	Overpressure of reboiler containing propane	2 killed, 173 injured	Mechanical; Operational; Personnel	(CSB, Williams Geismar Olefins Plant Reboiler Rupture and Fire Geismar, Louisiana, 2016)
February 12, 2014 and March 10, 2014	Tesoro Martinez Sulfuric Acid Spill	Martinez, California, USA	Acid Release	Valve failed spraying acid at two operators; Two operators sprayed when removing some piping	2 seriously injured; 2 seriously injured	Mechanical; Operational	(CSB, Tesoro Martinez Refinery: Process Safety Culture Case Study , 2016)
October 21, 2016	MGPI Processing Inc. Chemical Reaction and Release	Atchison, Kansas, USA	Toxic Release	During sulfuric acid delivery, operator connected the discharge hose to the fill line of the sodium hypochlorite tank. The chemicals mixed and formed a toxic cloud of chlorine gas, which was released to the surrounding areas	140 sought medical attention, 6 seriously injured	Operational; Personnel	(CSB, Key Lessons for Preventing Inadvertent Mixing During Chemical Unloading Operations, 2018)
August 31, 2017	Organic Peroxide Decomposition, Release, and Fire at Arkema	Crosby, Texas, USA	Toxic Release and Fire	During a hurricane the Arkema plant flooded and lost power to the refrigeration trucks	20 sought medical attention	Environmental	(CSB, Organic Peroxide Decomposition, Release, and Fire at Arkema Crosby Following Hurricane Harvey Flooding, 2018)

According to Al-shanini et al. there are three elements of process safety: operational integrity, mechanical integrity and personnel integrity (Al-shanini, Ahmad, & Khan, Accident modelling and analysis in process industries, 2014). These elements are represented in Figure 2-1, where the operational integrity is dependent on the mechanical integrity and both are dependent on the personnel integrity.

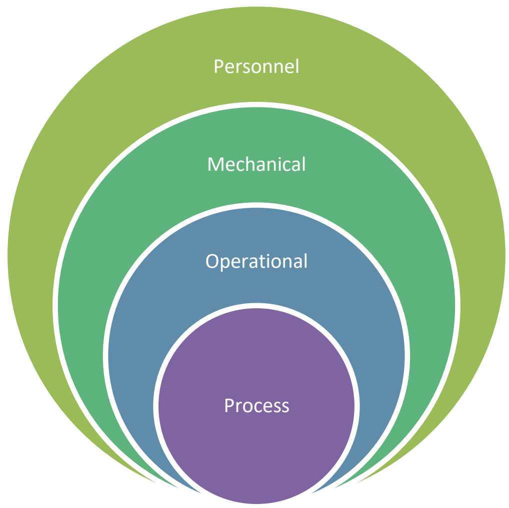

Figure 2-1: The Three Elements of Process Safety

The operational integrity of a process includes the initial design, design modifications, operating procedures and emergency preparedness plans. The mechanical integrity of the process includes material containment, maintenance and inspection and instrumental controls. The personnel integrity of the process includes the human aspects such as skill, work permits, training and communication.

It could be argued that a fourth element of process safety could be added to. Environmental factors would have an impact on the other three elements of process safety. For example, the last accident listed in Table 2-1 was caused by environmental factors. The toxic release and fire at the Arkema plant in Crosby Texas was a direct result of flooding caused by Hurricane Harvey in 2017 (CSB, Organic Peroxide Decomposition, Release, and Fire at Arkema

Crosby Following Hurricane Harvey Flooding, 2018). The Arkema plant produced organic peroxides which must be refrigerated to prevent decomposition and self-ignition. The plant flooded during the hurricane and lost power to the refrigerated storage tanks. The peroxides were moved to refrigerated trucks which were also at risk of losing power. To prevent a larger accident, the trucks were burned in a controlled environment. It was concluded that Arkema did not account for that level of flooding during the plants design. It was recommended by the Chemical Safety Board (CSB) that the company design should consider that level of flooding in future designs for the plant. The environment is essential to protect but also has a negative effect on processes as shown in the Arkema accident example.

When assessing environmental factors, both extreme and common weather types should be considered. Emergency response plans should be created with weather conditions in mind (IADC, 2015). It is known that weather and wind patterns influence design, especially when there are gaseous emissions (Crowl & Louvar, 2011). Figure 2-2 shows an updated model to include the impact of environmental factors on operational, mechanical and personnel integrity.

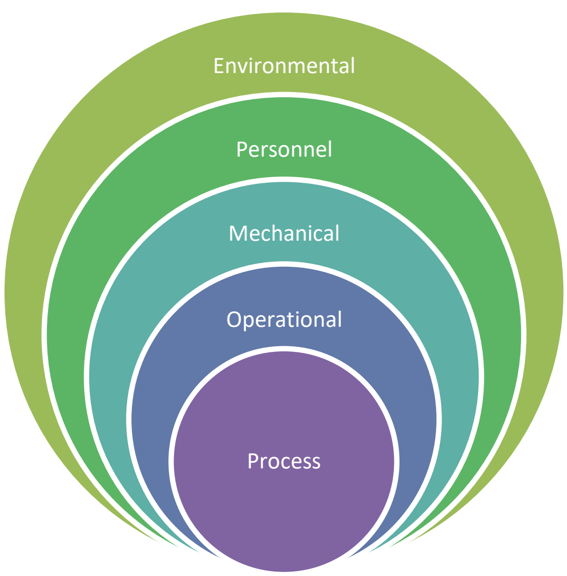

Figure 2-2: Updated Process Safety Model to include Environmental Factors

2.1. Measuring Safety and Risk

The safety and risk of a process system are commonly measured using factors such as OSHA accident and fatality rates, loss time injuries and fatal accident rates of similar industries (Khan, Abunada, John, & Benmosbah, 2009). All of these factors account for the after effects of incidents and accidents once they occur. Process safety and risk can be measured using leading and lagging indicators.

Lagging indicators are a measure of process outputs. These indicators keep track of previous incidents and accidents to predict the frequency and consequences of future accidents. Lagging indicators signify how well a process is functioning based on how goals are being met and how well it is preventing accidents. Lagging indicators are reactive as modifications in operations and goals are made after outputs change (Khan, Abunada, John, & Benmosbah, 2009).

Where lagging indicators measure outputs, leading indicators are a measure of process inputs. Leading indicators are proactive where changes to process are anticipated and modifications are implemented before changes to a process occur. Leading indicators can include: how often risk assessments are completed, how many are completed or how often maintenance is performed.

Both of these indicators should be used in process industries to monitor safety and risk and prevent accidents (Khan, Abunada, John, & Benmosbah, 2009). If accidents can be anticipated and understood before they occur they can be prevented (Al-shanini, Ahmad, & Khan, Accident modelling and analysis in process industries, 2014). According to the study by Charkaborty et al. industry leaders should identify and monitor lead indicators to signal potential for process safety performance degradation (Chakraborty, 2003). By monitoring lead indicators, the management of process systems can be improved upon.

2.2. Risk Assessments

Shahri et al. stated that safety researchers agree that the greatest challenge of examining risk is that no prediction is completely accurate (Shahri, MahdaviNejad, & AmirKabir, 2016). Predicting the exact behaviour and likelihood of a particular consequence cannot be definitively determined. There are multiple tools and techniques available to assess risk, however, no single method is sufficient and a combination of methods are required. Since every operation is unique there is no "one size fits all" technique to complete the risk assessment.

To complete risk assessments, accident modelling is used to create scenarios and examine the frequency and consequences associated with process hazards. The two most important questions of accident modelling are: why does an accident happen and how does an accident happen. According to the literature review by Al-shanini et al. there are many different types of accident models across. The traditional sequential model types are: the Fault Tree Analysis (FTA), Event Tree Analysis (ETA), Bowtie model and Failure Mode and Effect Analysis (FMEA) (Al-shanini, Ahmad, & Khan, Accident modelling and analysis in process industries, 2014).

The fault tree analysis is a bottom-up graphical technique that is used to deduce and quantify the failure probability of a process system. The event tree analysis is a top-down graphical technique that is inductive and applies logic to determine the consequences of a process system. The event tree is used in the early methodology of the thesis and is described in detail in chapter three. The bowtie model combines the fault tree and event tree for a single accident or initiating event. The failure mode and effect analysis is a step wise analysis that examines all potential faults of a process system and aims to prevent them.

While the traditional models are useful for initial risk assessments they also have some disadvantages. Each of the traditional models are static and cannot be used to represent non-linear or independent relationships of failures within process systems.

A more modern approach to these models are considered dynamic sequential accident models (DSAM) which includes Process Hazard Prevention Accident Models (PHPAM) and Dynamic Risk Assessment (DRA) (Al-shanini, Ahmad, & Khan, Accident modelling and analysis in process industries, 2014). There are currently two models proposed that would be considered process hazard prevention models. The offshore oil and gas model proposed by Kujath et al. (Kujath, Amyotte, & Khan, 2010) and the System Hazard Identification prevention and prediction (SHIPP) model proposed by Samith et al. (Samith, Khan, & Amyotte, 2011).

The offshore oil and gas model begins with examining accidents and potential loss in the offshore field and identifies potential failures from a managerial and occupational perspective. This method emphasises the responsibility of the organization to prevent accidents rather than place blame on an individual. This method examines the barriers from a managerial point of view: release prevention, ignition prevention, escalation prevention, harm prevention and loss prevention. This model was successfully applied to the Piper Alpha and BP Texas City refinery accidents (Al-shanini, Ahmad, & Khan, Accident modelling and analysis in process industries, 2014). A limitation of this model was that it does not examine the effects of some initialing events for accidents such as fire or explosion propagation. The offshore oil and gas model was used a basis for the SHIPP model.

The SHIPP accident model aims to reduce accidents by evaluating hazards and predict and prevent them by using additional barriers based on the offshore model. The barriers examined in the SHIPP method are: release prevention, dispersion prevention, ignition prevention, escalation and emergency management. The barriers are not always physical. These barriers can include operating procedures and emergency response plans. This method also determines ways to continuously monitoring the system. This model can be used with Bayesian analysis to estimate the likelihood of an accident based on previous data. The SHIPP model is both qualitative and quantitative.

Both the offshore and SHIPP models shared a limitation. This limitation was that some barriers may be illogical and unnecessary. For example the examination of ignition barriers is inappropriate for plants where the materials are toxic or non-flammable.

The last accident model to be discussed in this literature review is the dynamic risk assessment also known as the dynamic quantitative risk assessment. The dynamic risk assessment uses the same methodology of the quantitative risk assessment.

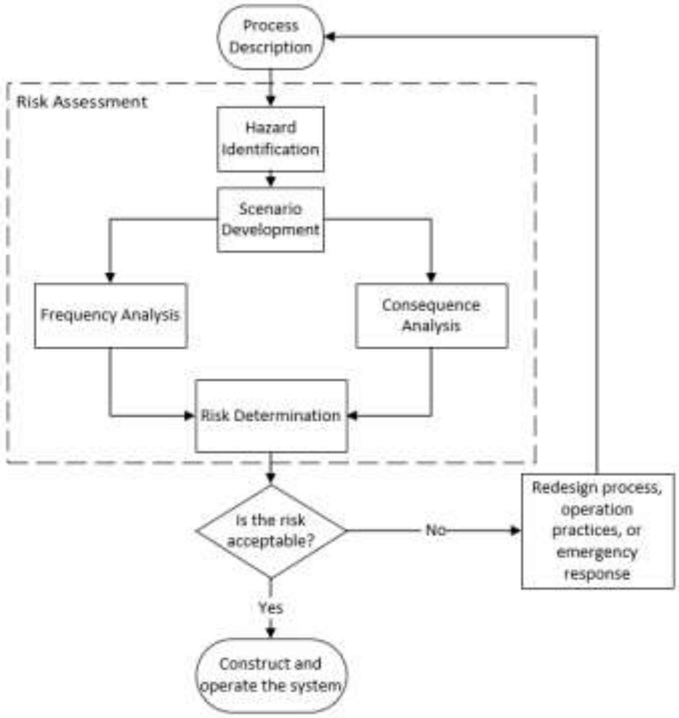

Figure 2-3: Risk Assessment Procedure

Quantitative risk assessments are typically completed in four steps: hazard identification, frequency analysis and consequence analysis, and risk analysis. The step of scenario development is optional (Crowl & Louvar, 2011). The risk assessment process is shown in Figure 2-3. The hazards or dangers of a process are identified in each step of the process. Process hazards are determined during a Hazard and Operability Study (HAZOP). This approach is structured and effective. Process drawings are used as a basis where each component of a system is examined and all possible deviations are determined. The hazards are applied to accident scenarios. In this thesis, the methodology of risk monitoring is applied to a single scenario. The frequency of occurrence and the consequence of the accident are combined to estimate risk. The estimated risk is analyzed whether it is acceptable or manageable the design or operation is approved. If the risk is determined to be unacceptable, the risk must be revaluated and redesigned and the process is started over until the risk is acceptable.

However, the dynamic risk assessment allows for the failure probabilities of the original risk assessment to be updated as new information become available or conditions change. In industry, quantitative risk assessments are typically completed every five years (Khan, Abunada, John, & Benmosbah, 2009). However, by using the dynamic risk assessment approach, the procedure changes and process degradation can be captured. This allows for a higher accuracy and continuous monitoring of risk conditions. The quantitative risk assessment uses event trees to determine consequence. However, Bayesian networks have become increasingly popular as the interdependence of accident causes are more easily mapped.

The Bayesian Network is an approach can account for the possibility that multiple events may occur simultaneously to produce an accident. The Bayesian Network approach has been used successfully to estimate the likelihood of the occurrence of a release of LNG and the subsequent consequences. (Abbassi, Garaniya, & Khan, 2016). The Bayesian network approach was also successfully applied to the Willams Geismar reboiler accident (Guo, Khan, & Imtiaz, 2019). The Bayesian network approach was used in the development of the methodology in chapter three and the case application in chapter four.

3. Chapter 3: Methodology

3.1. Overview

In this section of the thesis, the methodology of the Bayesian Network development and risk monitoring system are outlined. An accident scenario, an overflowing tank, was created as a foundation for the methodology. First the accident probability was determined with an event tree. The same accident scenario was used for the created of the Bayesian network. A Bayesian network is developed to assess risk. The tanks safety systems were updated with additional safety features until the risk level was brought down to an acceptable level. This risk level is combined with simulated data to show the risk of the process system as a function time.

3.2. Event Tree Analysis

The event tree is an inductive analysis method used commonly in risk assessments. This analysis method is extremely effective at determining the pathways to an accident and the probability of the accident occurring. All event trees will begin with an initiating event where final results such as failure, near miss or safe operation are determined by intermediate events. The intermediate events are conditions and safety features of the system. Each event can only have two outcomes such as true or false, success or failure and yes or no. If available, failure data and statistics are used to determine the probability of the final event. The disadvantages of an event trees are their static and linear nature. Event trees rely on accurate data and the events failing in a sequential order (You & Tonon, 2012). The risk associated with this accident could not be developed in an event tree as the inputs and outputs are not binary.

3.3. Bayesian Networks

It is argued in the literature (Marsh & Bearfield, 2008) and (Unnikrishnan, Shrihari, & Siddiqui, 2014) that combining event trees and Bayesian networks allows a more flexible model while maintaining the safety specific logic. To relax the assumption that the accident progression and event failures are linear, the accident scenario was modelled into a Bayesian network. Bayesian networks are dynamic in nature and allow for probabilities to be updated easily when new information is discovered. A Bayesian network is a probabilistic graphical modelling technique. Bayesian networks are both qualitative and quantitative which is making them increasingly popular for accident analysis. These networks are a combination of directed acyclic graphs (DAG), which are qualitative, and their conditional probabilities which are quantitative (Ibe, 2011). The BN is an effective way of representing interdependence between variables.

According to (Darwiche, 2009), there are three steps to developing a Bayesian Network. The first step is to define the relevant variables, next the network relationships must be defined and finally the conditional probabilities are assigned to the variables.

3.3.1. Defining Variables

To predict an accident and the subsequent risk all relevant factors are considered as variables. The characteristics of a variable are represented in nodes. Each characteristic have at least two states or more such as true and false. However, as the number of nodes increases so does the complexity of the network. A network can be made more manageable by reducing the number of nodes. The number of nodes can be reduced by combing the similar characteristics for the variable in a single node. If the states of the characteristics are the same and are considered mutually exclusive then they may be combined in a single node.

Consider the variable weather as an example. Weather, in this example, can be broken down into four characteristics: clear, windy, rainy and stormy. For the weather characteristics there are two states: true and false. Rather than have four nodes with two states, weather may be represented as a single node with four states.

3.3.2. Network Relationships

Once the variables are defined in nodes, the nodes are then categorized and relationships are mapped. Determining the relationships between nodes is also known as defining edges (Darwiche, 2009). There are three nodes categories: evidence, intermediate and query here are also three node mapping relationships: parent, child and leaf. (Darwiche, 2009). Evidence nodes are the input variables and are the first nodes. Evidence nodes must also be independent from each other. Since evidence nodes are first they are also parent nodes. Query nodes are the final outcomes and can be either child or leaf nodes. Child and leaf nodes are connected to a parent node. Intermediate nodes connect the evidence and query nodes. Only child nodes can be intermediate. However, a child node can also be connected to another child node. Leaf nodes do not have any child nodes after them.

In terms of accident and risk analyses, only intermediate and evidence nodes can be set and query nodes are computational and cannot be changed.

3.3.3. Conditional Probabilities

Once the network relationships have been determined, the conditional probabilities are assigned. This is quantitative as the uncertainties are defined. The values of the conditional probabilities can be either objective or subjective. Objective values are ones determined from data, statistics and calculations. Subjective values are ones determined through an expert's reason, beliefs and experience. The conditional probabilities for this thesis are subjective (Darwiche, 2009). These probabilities are for predictive and demonstrational purposes. The conditional probabilities can be updated over time as new information becomes available. Updating the probabilities presented in this thesis is an area for future work.

3.4. Methodology

3.4.1. Event Tree Development

To begin development of this proposed safety and risk monitoring system, a simple open tank was examined. The most severe and likely hazard of an open tank is tank overflow. The basis for calculation and risk plotting is the flow entering the tank. The tank examined as shown in Figure 3-1 has two manual valves. The first valve (V-1) is on the line flowing into the tank and the second valve (V-2) is on the line flowing out of the tank. The probabilities displayed in the following event trees are hypothetical and were not collected from any database and are for demonstration purposes only.

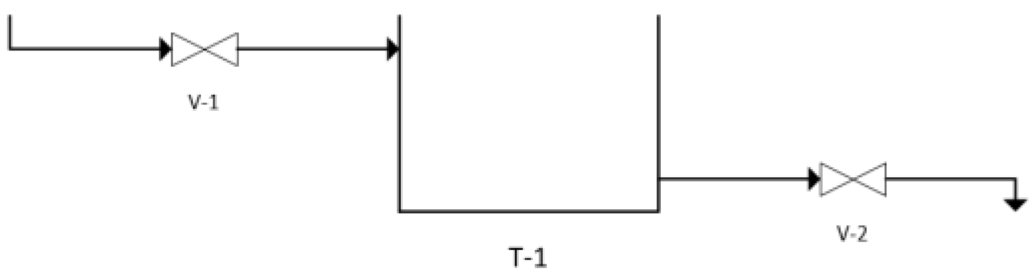

Figure 3-1: Simple Open Tank with Two Manual Valves

After the tank set up was established, an event tree as shown in Figure 3-2 was used to quantify the probability of an accident. The first event was the condition of the flow, if there was no high flow or limited flow then the tank will not overflow. If the flow was high there was an opportunity for the tank to overflow.

The second event was if the operator of the manual valves noticed that the flow was high. For this event, either the operator notices the high flow and reduces it or the operator does not notice the high flow and the condition continues.

The third event would be the operator opening valve V-2 to increase the flow leaving the tank to prevent an overflow or not open the valve allowing for the overflow to occur. If V-2 is not opened, the next event would be for the operator to close V-1 to reduce the flow to the tank and prevent an overflow from occurring. If the operator does not close V-1 then an overflow will occur.

The “X” at the beginning of the event tree represents the flow data before the first valve. The high flow condition would be picked up by a sensor before the process for a specified threshold. The occurrences of high flow conditions over a time frame, say one day of operation, out of how ever many data points are collected in the time frame would be multiplied by the probability of an accident occurring to display the safety of the process system any given day.

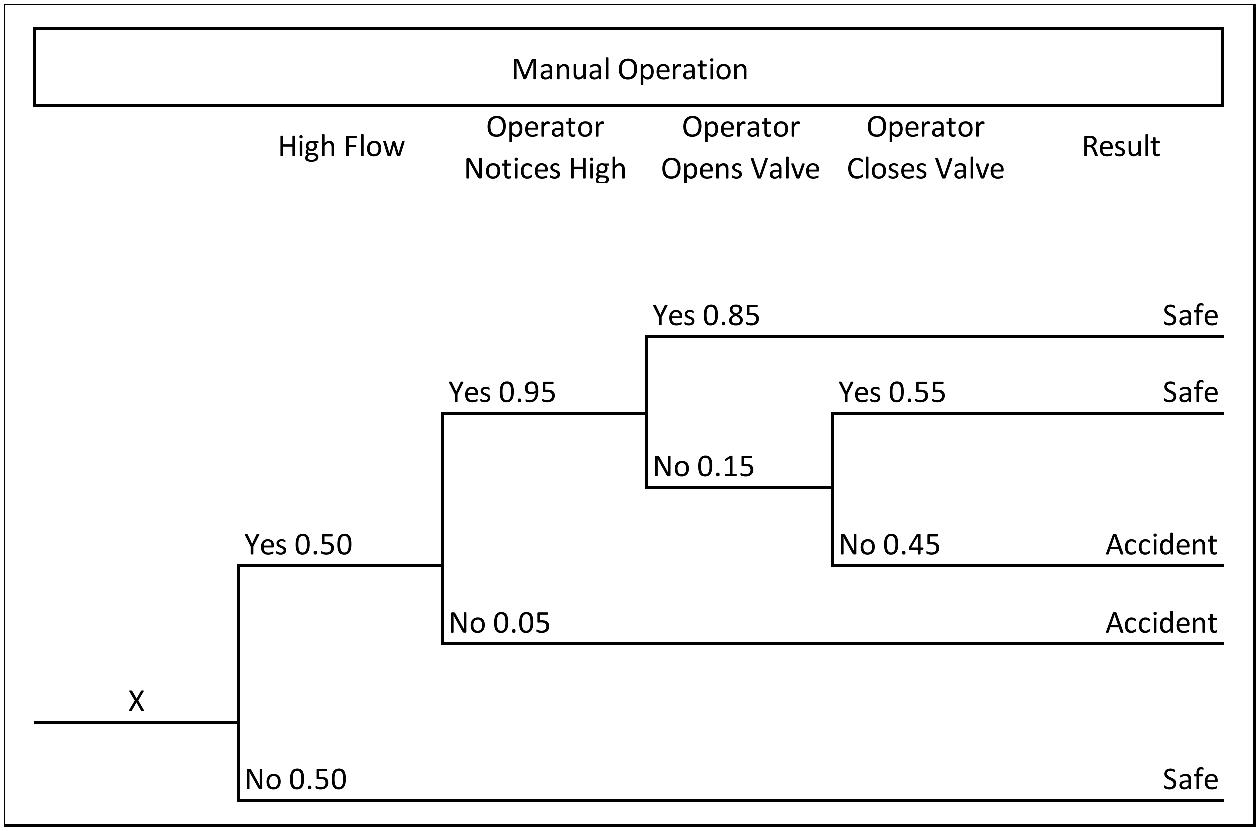

Figure 3-2: Event Tree of Overflowing Tank with Two Manual Valves

As discussed before, the probabilities for the events are calculated by multiplying the values of the branches of the event tree. A sample calculation can be found below in Figure 3-3. Figure 3-4 shows all of the branches with the final probabilities calculated.

$$P(Safe) = X * 0.50 * 0.95 * 0.85$$

$$P(Safe) = 0.4038X$$

Figure 3-3: Sample Calculation for Top Branch of Event Tree

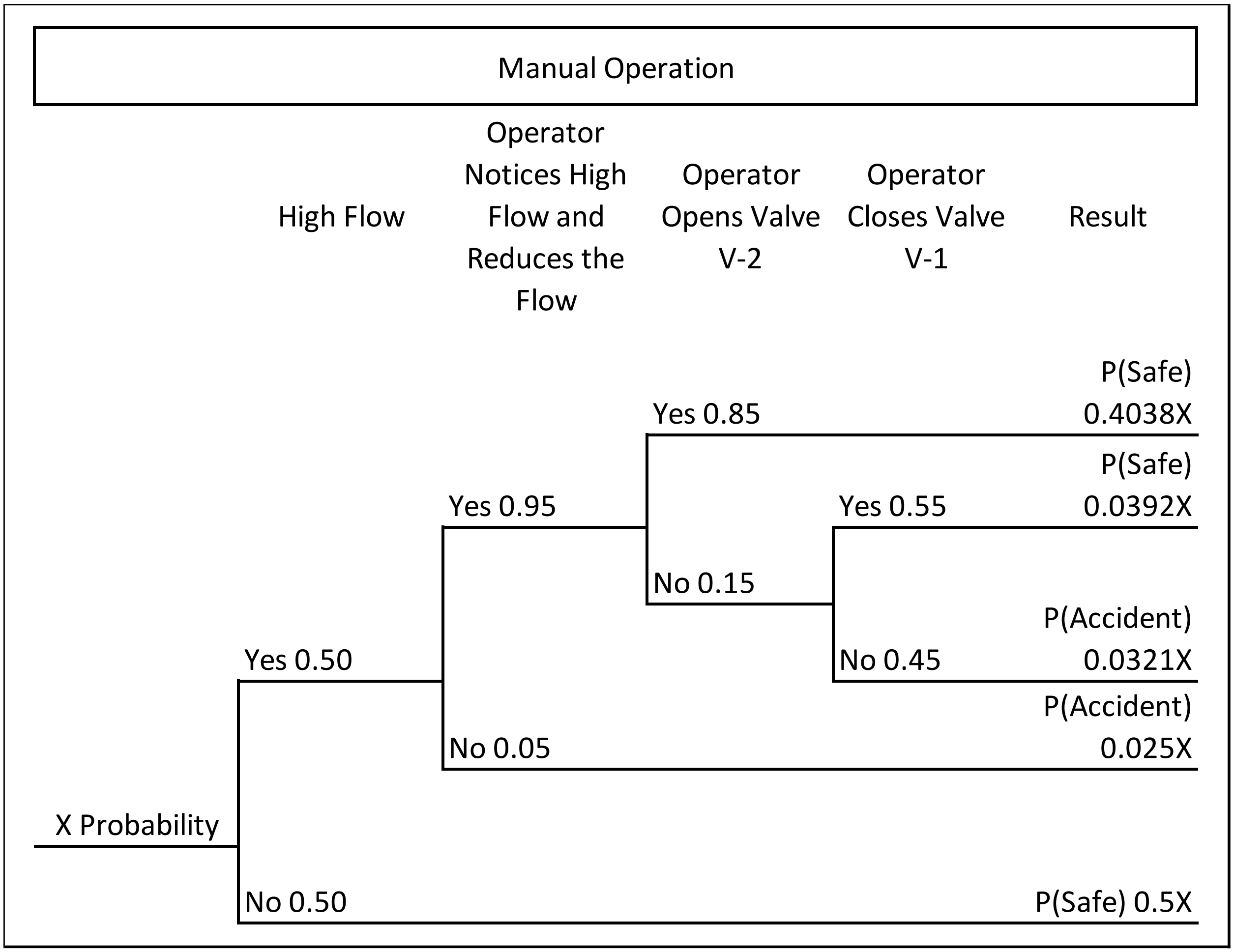

Figure 3-4: Event Tree of Overflowing Tank with Calculated Probabilities

The final calculated values for the branches with the same outcome can be added for a final probability. Therefore the probability of an overflow accident is 0.0571 or 5.71% and the probability of safe operation is 94.29% for this tank example.

By improving the safety features of the tank the probability of an accident can be reduced. Using the same tank with a bypass pipeline added to the flow line entering the tank as shown in Figure 3-5. If both V-2 and V-1 were unavailable then the operator could open the bypass valve V-3 and reduce the flow entering the tank.

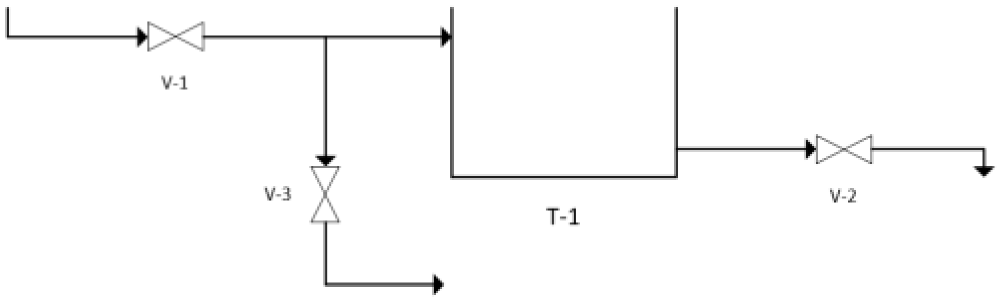

Figure 3-5: Tank with Bypass Line and Three Manual Valves

The event tree created above was updated with the additional bypass valve in Figure 3-6. With the calculated probabilities of the updated event tree the resulting probability of an overflow accident was 0.0282 and for safe operation was 0.9718. One additional safety measure reduced the probability of an accident for this example by 51%.

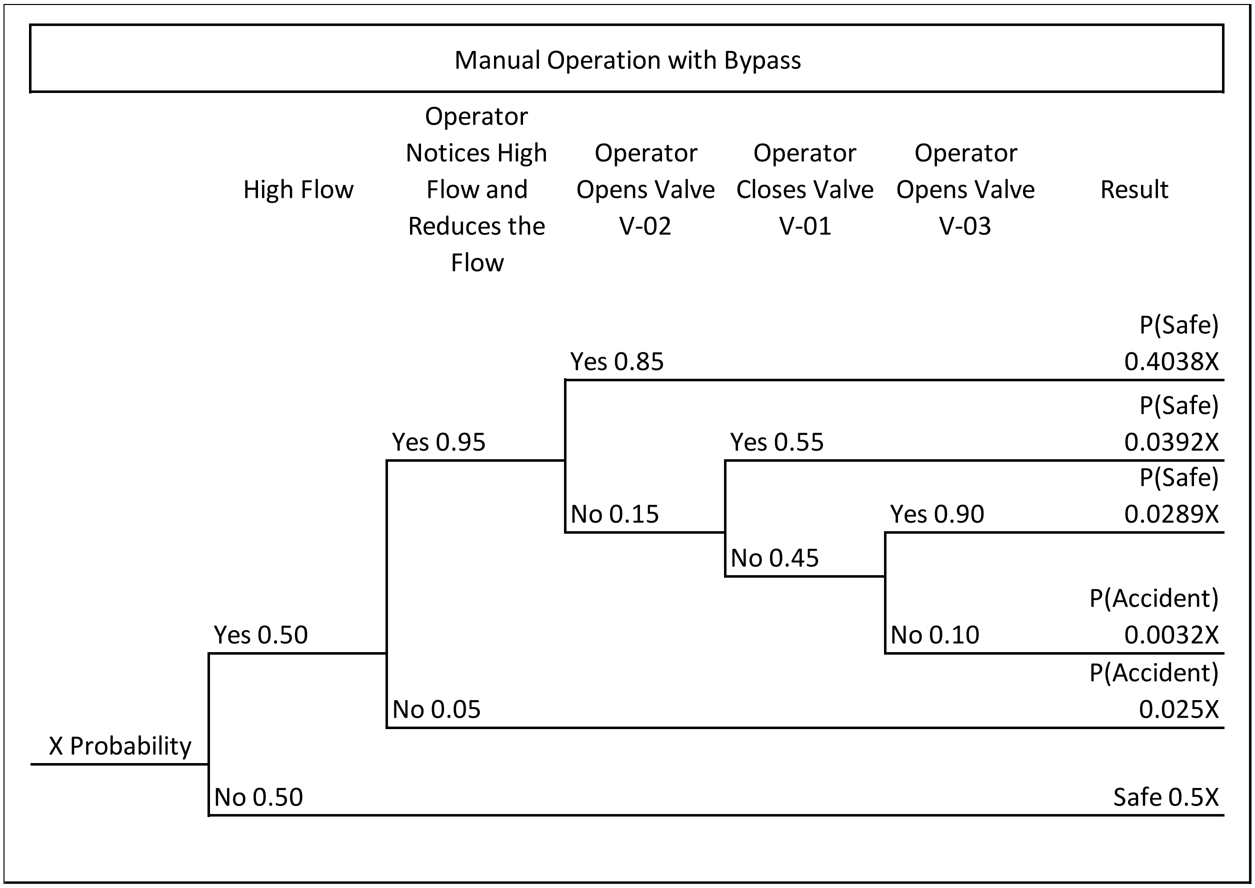

Figure 3-6: Event Tree of Overflowing Tank with Bypass Line and Calculated Probabilities

3.4.2. Proposed Bayesian Network Based on Event Tree

The first Bayesian network was developed directly from the event tree of Figure 3-2. The risk of the system was also examined by creating a risk network. The Bayesian networks were created using GeNie 2.2 Academic, a software created by BayesFusion, LLC. For the first model, a total of 12 nodes were used. The breakdown of the node relationships and states are shown in Tables 3-1 and 3-2 respectively.

The event tree of the tank with manual valves shown in Figure 3-2 was first directly translated into a Bayesian network as shown in Figure 3-7. The resulting probability of an accident for the same tank example was the same as the initial event tree.

Table 3-1: Bayesian Network Node Characterization and Relationships for the Tank with Manual Valves

Node	Node Name	Parent	Child	Characterization
1	Flow Conditions	N/A	Operator notices high flow and reduces flow	Evidence
2	Operator notices high flow and reduces flow	Flow Conditions	Valve 2 Conditions	Intermediate
3	Valve 2 Conditions	Operator notices high flow and reduces flow	Valve 1 Conditions	Intermediate
4	Valve 1 Conditions	Valve 2 Conditions	Operating Conditions	Intermediate
5	Operating Conditions	Valve 1 Conditions	Risk	Intermediate
6	Weather	N/A	Environmental impact	Evidence
7	Material type	N/A	Environmental impact	Evidence
8	Value of asset	N/A	Impact	Evidence
9	Population	N/A	Impact	Evidence
10	Environmental impact	Weather/Material Type	Impact	Intermediate
11	Impact	Environmental impact/ Population/Value of asset	Risk	Intermediate
12	Risk	Impact	N/A	Query

Table 3-2: Bayesian Network Node States

Node	Node name	States
1	Flow Conditions	High Flow; No High Flow
2	Operator notices high flow and reduces flow	Reduces High Flow; Does Not Reduce High Flow; No High Flow
3	Valve 2 Conditions	Open Valve 2; Does Not Open Valve 2; No High Flow; Does Not Reduce High Flow
4	Valve 1 Conditions	Open Valve 2; Close Valve 1; Does Not Close Valve 1; No High Flow; Does Not Reduce High Flow
5	Operating Conditions	Safe; Accident
6	Weather	Clear; Windy; Rainy; Stormy
7	Material type	Normal; Flammable; Toxic; Corrosive
8	Value of asset	High; Moderate; Low
9	Population	High; Moderate; Low
10	Environmental impact	Severe; Moderate; Low
11	Impact	Severe; Moderate; Low
12	Risk	High; Moderate; Low

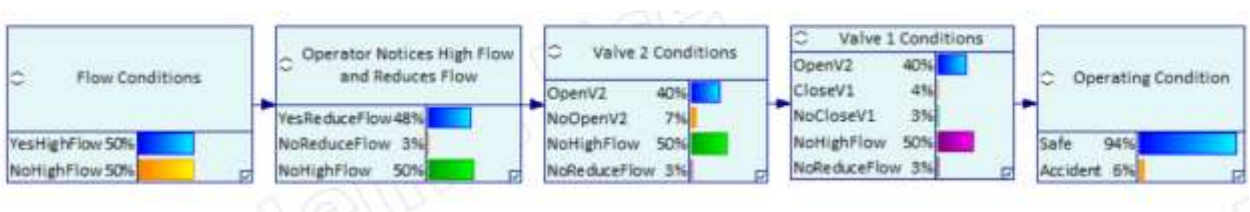

Figure 3-7: Bayesian Network of the Tank with Two Manual Valves

Once the operating condition probabilities were determined a risk matrix was developed. The risk matrix used for the tank case is shown in Figure 3-8. The environmental impact considers the type of material and the weather conditions. The types of materials include flammable, toxic, corrosive and normal. The term normal was used for materials that are not considered dangerous. The types of weather considered were clear, windy, rain and stormy. The term stormy was used to consider more extreme weather such as both rainy and windy weather.

The environmental impact, asset cost and the population of the surrounding area were considered for the overall impact. The population and cost of the asset were divided into high, moderate and low. The impact was related to the final risk. For example, the environmental impact of flammable materials and windy weather was given a higher severity than normal material and any type of weather. This matrix was combined with the final operation condition of the tank to give the risk for any period of time.

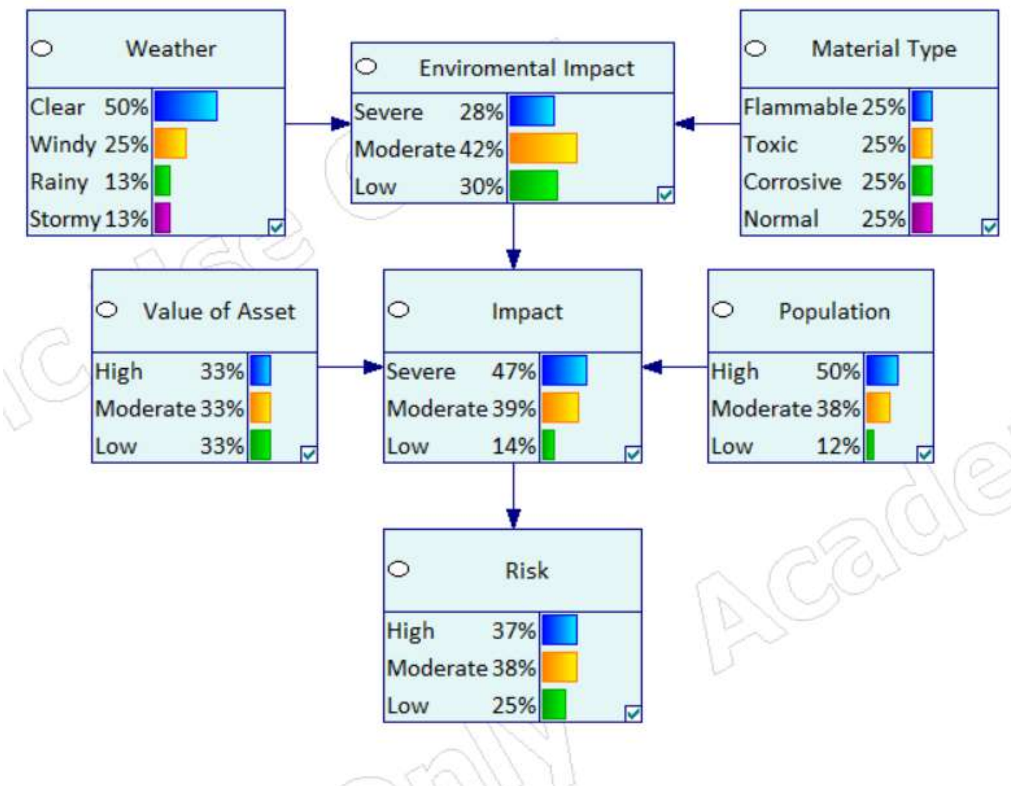

Figure 3-8: Risk and Impact Bayesian Network

The risk and impact network was combined with the operating condition network to create the overall risk for the tank operation. The combined networks are shown in Figure 3-9.

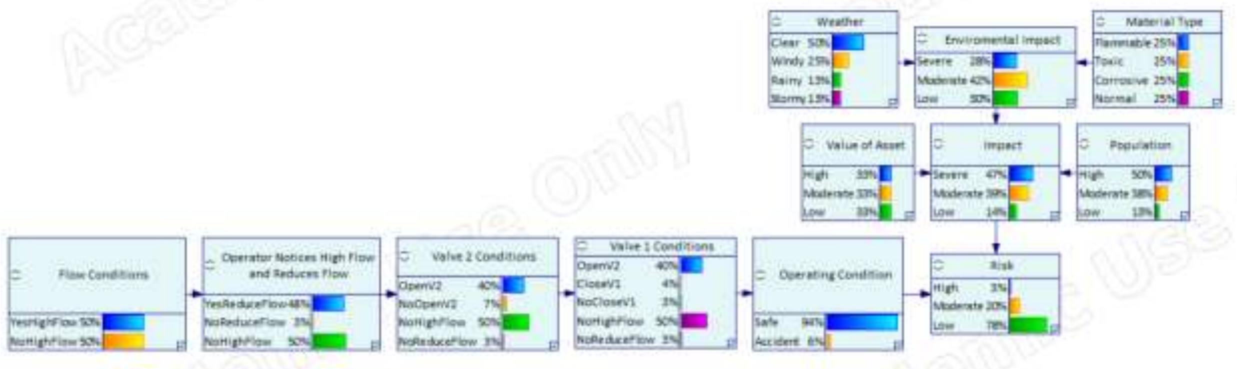

Figure 3-9: Operating and Risk Impact Networks Combined

In Figure 3-9, the likelihood of an accident and the overall impact gave a high risk value of 3.30%. If the material is changed to flammable the high risk will increase to a value of 3.83%. If the material is changed to toxic and the population to high the risk will increase to 4.47%.

3.4.3. Updated Bayesian Network Development

To relax the linear nature of the event tree, the Bayesian network was updated to allow for either valve to be opened without having one of the valve actions fail. The updated Bayesian network for the two valve system is shown in Figure 3-10. Additional nodes were added to include conditions of the valves changing and if the valve action was effective enough to stop an overflow action. The probability of an overflow accident for the tank is now 0.0508 or 5.08% and the probability for safe operation was reduced to 94.92%. The high risk probability was reduced to 2.94%.

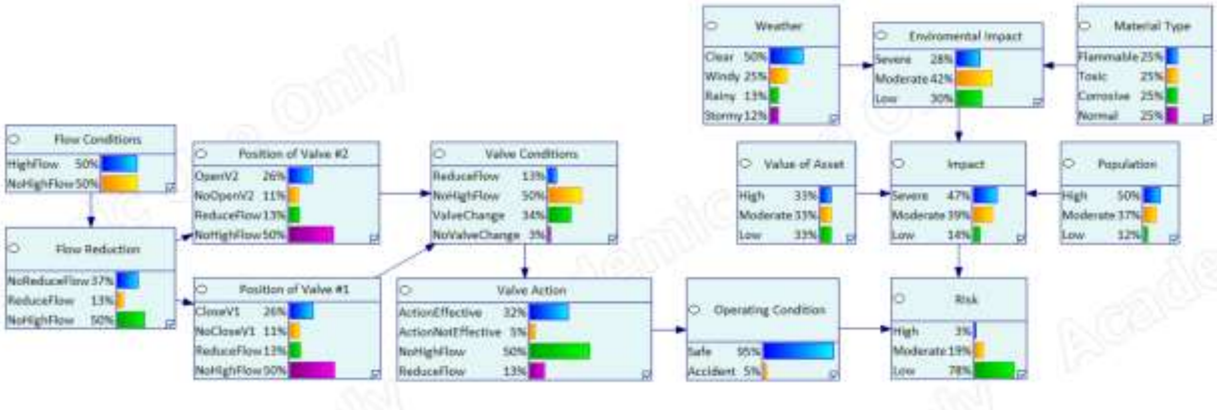

Figure 3-10: Updated Bayesian Network of Two Valve Tank

The two valve model of Figure 3-10 was updated to include the use of the bypass valve V-3 as shown in Figure 3-11. The probability of an overflow accident for the tank with bypass was 0.0348 or 3.48% and the probability of safe operation was 96.52%. The high risk probability was again reduced to a value of 2.01%.

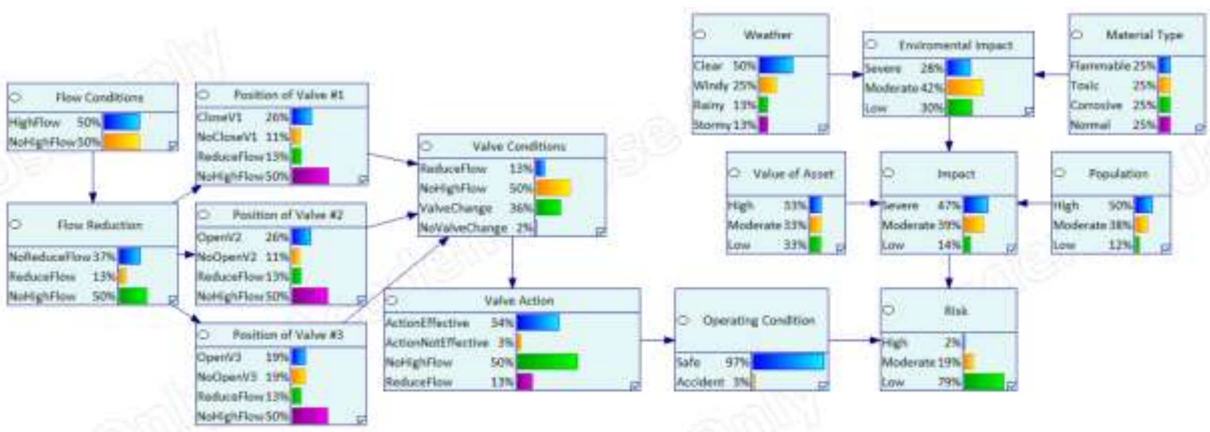

Figure 3-11: Bayesian Network for Tank with Bypass Valve

The original tank example was under manual operation only. To further improve safety and reliability and automatic control loop was added in place of the manual valves. It is thought by many that by automating a process system it can be made safer (Haight & Caringi, 2007).

The manual valves were replaced with an automatic control valve on V-2 with a level indicator and transmitter on the tank as shown in Figure 3-12.

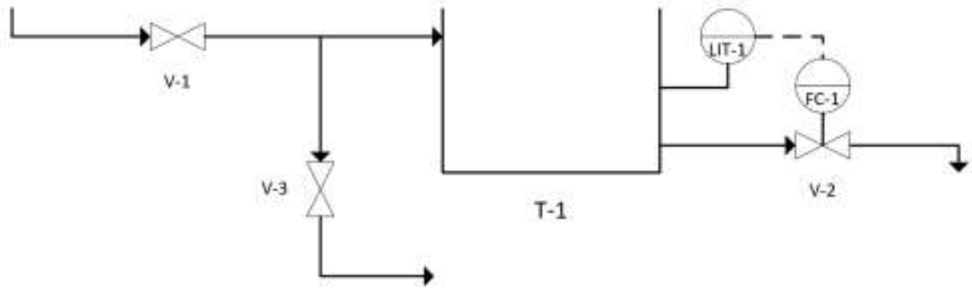

Figure 3-12: Tank Example with a Level Control Loop on Valve V-2

A new Bayesian network was created for the single automated control valve in Figure 3-13. This new network included the conditions of the level indicator and transmitter and the flow controller. With just the automatic valve V-2 the probability of an accident actually increased to 4.43% with the probability of safe operation decreasing to 95.57%. This result was not unexpected. This is now only one route of failure instead of three routes of failure with the valves. The high risk probability increased to 2.56%.

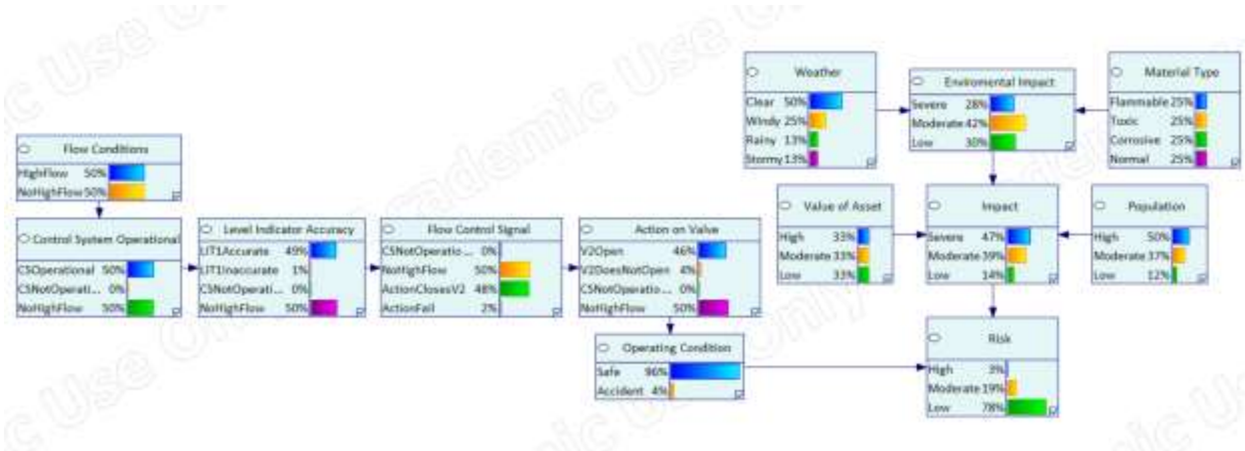

Figure 3-13: Bayesian Network for Automated Valve with Level Control Loop

To continue the trend of increasing the level of automation another control loop was added to the tank. A flow transmitter was added to the tank on the valve V-1 as shown in Figure 3-14.

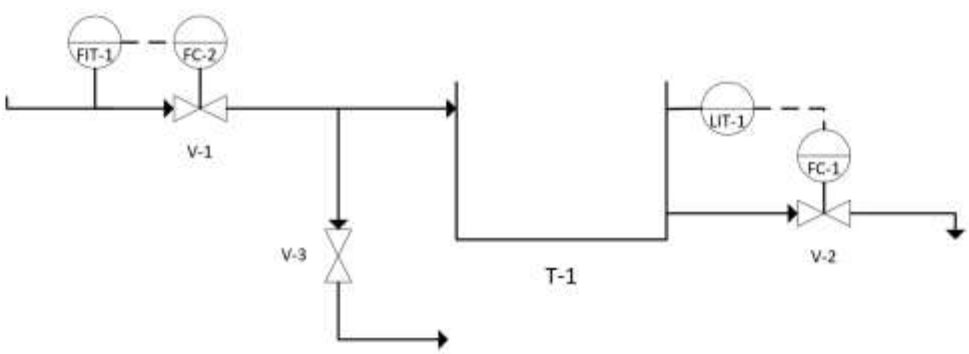

Figure 3-14: Tank with Flow and Level Control Loops

The Bayesian network of Figure 3-13 was updated and modified to include the new flow control loop on V-1 as shown in Figure 3-15. The addition of another control loop further increased the safety of the system to 98.77% and reduced the probability of accident to 1.23%. By adding control loops for a simple system and removing the manual operations, the operators talents and skills may be applied elsewhere (Haight & Caringi, 2007). The high risk probability decreased to 0.713%.

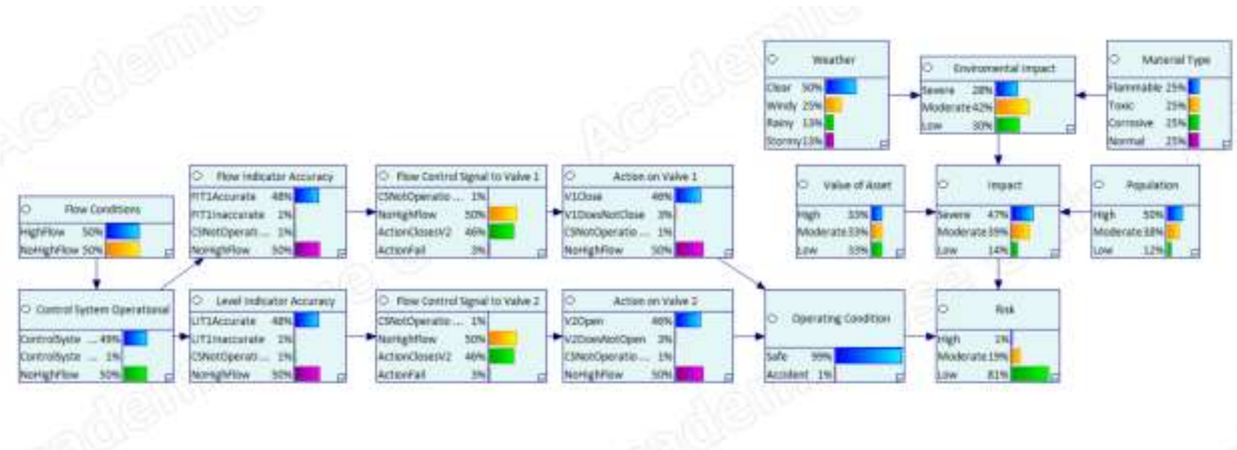

Figure 3-15: Bayesian Network for Two Control Loops

To further continue the trend of automation, all valves were made into control valves as seen in Figure 3-16. A flow transmitter was added to the line after the bypass line and set to control the bypass valve V-3 in the event that one or both of the other valves or control loops failed.

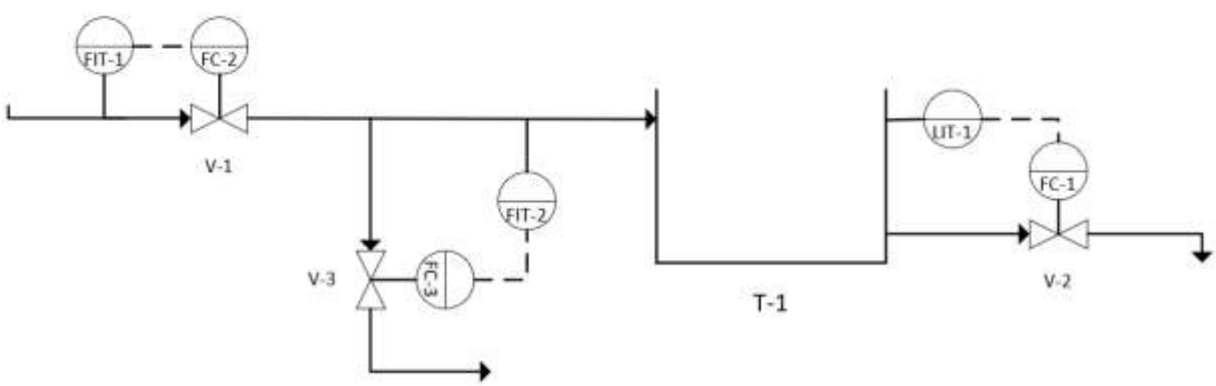

Figure 3-16: Tank with Two Flow Control Loops and Level Control Loop

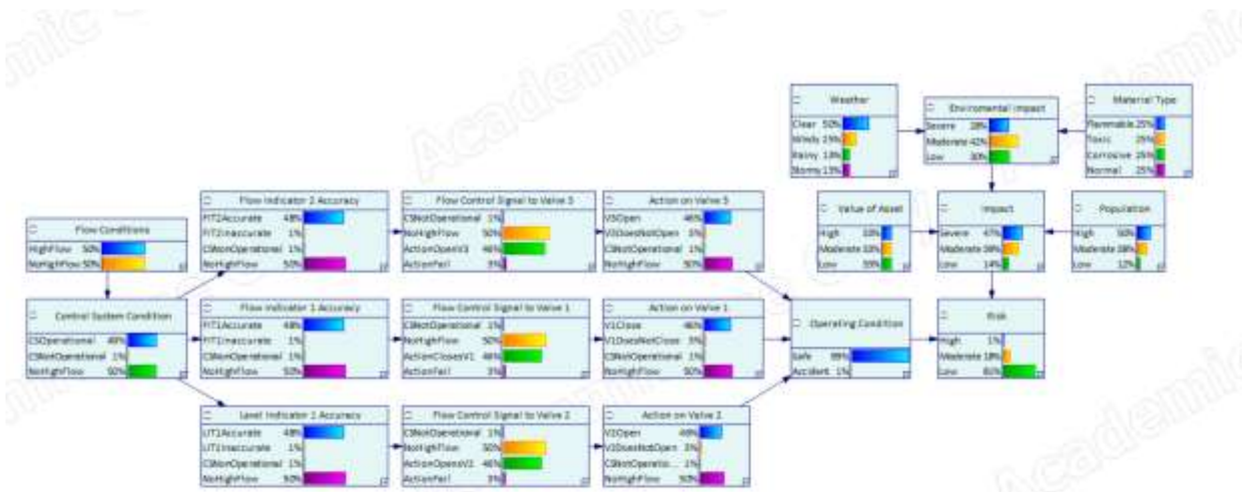

Figure 3-17: Bayesian Network with Two Flow Control Loops and Level Control Loop

The Bayesian network was modified again, Figure 3-17, to include the latest flow control loop and improve the tank system. The probability of an accident was reduced to 1.04% and the probability of safe operation was increased to 98.96%. The high risk probability was decreased further to 0.585%. The system is now completely automated. The system could be made even safer by implementing an additional safety system.

The safety system proposed would be isolated from the main control loops and be there as a backup to operations. The safety system would have independent isolated sensors and controls signals on the valves in the event the control loops failed. The proposed safety system can be seen in Figure 2-18. The safety system transmitters and signals are highlighted in green.

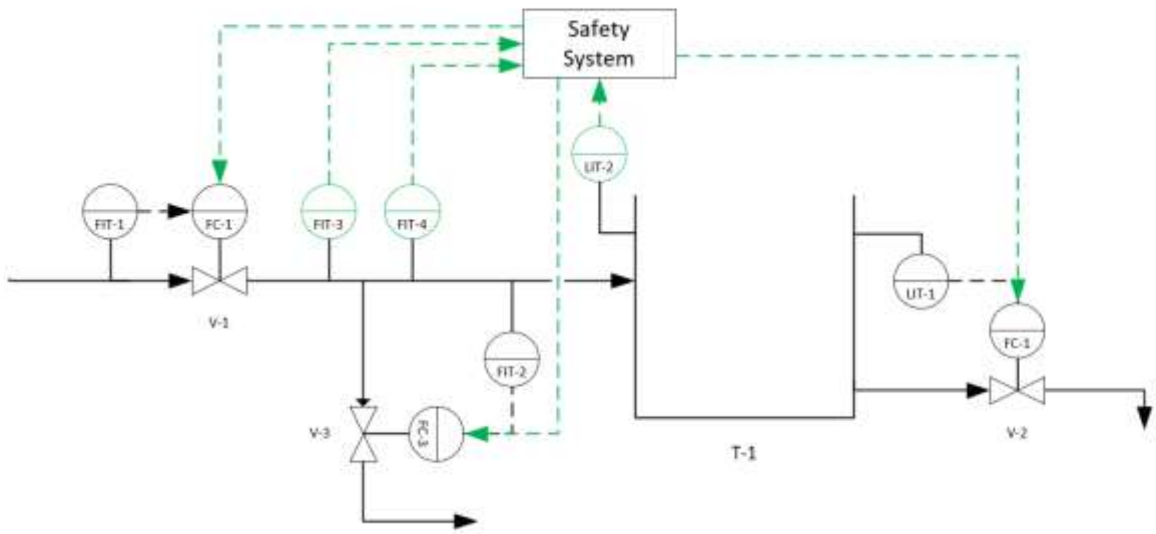

Figure 3-18: Tank Diagram with Safety System

The Bayesian network for the existing control loops was updated a final time to include the proposed safety system in Figure 3-18. The network is set up to include the condition that if the control systems as a whole or the existing control sensors fail the safety system would be activated in Figure 3-19. There are now six sensors, three for the original control system and three for the safety system. The safety system is responsible for the safe shutdown operation as a last resort to prevent an accident. With the safety system the probability of accident was reduced to 0.0105% and the probability of safe operation was increased to 99.9895%. The high risk probability was decreased to a final value of 0.00118%.

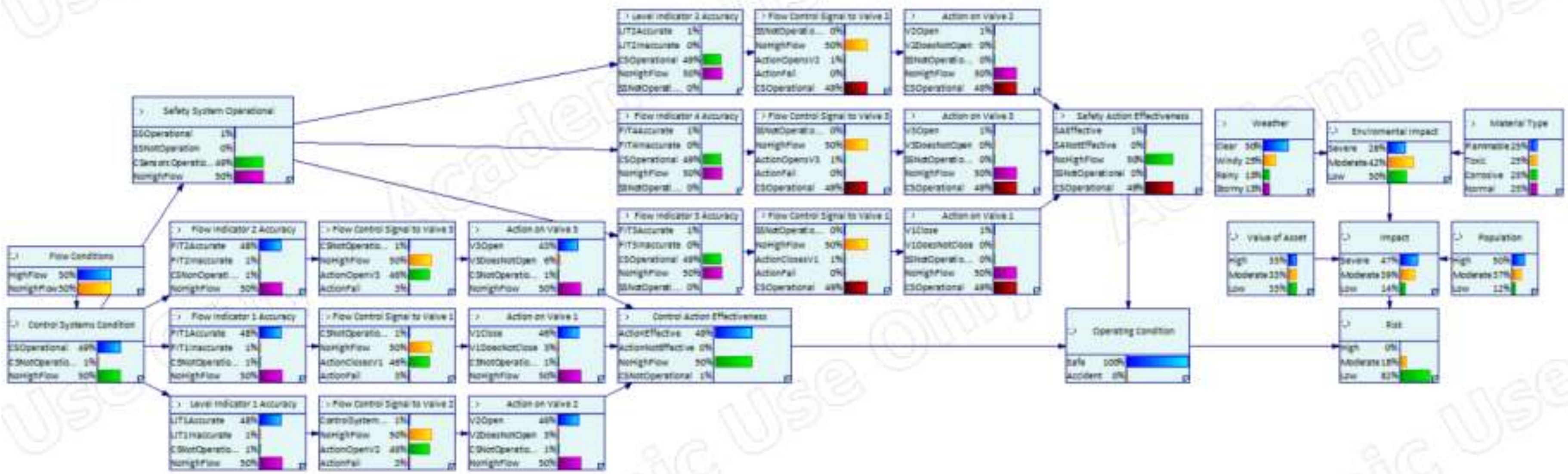

Figure 3-19: Bayesian Network for the Control and Safety System

A summary of all of the accident and Risk of failure is shown in Table 3-3 with a calculation to show the percent reduction from the original manual system.

Table 3-3: Summary of Accident and Risk of Failure for the Tank Systems

	Accident Probability	Change in Accident Probability	Risk of Failure	Change in the Risk
Manual Valve System	5.08%	--	2.94%	--
Manual System with Bypass Valves	3.48%	-31.5%	2.01%	-60.4%
Level Control System	4.43%	-12.8%	2.56%	-49.6%
Control System with Two Controls	1.23%	-75.8%	0.713%	-86.0%
Control System with Three Controls	1.02%	-79.9%	0.588%	-88.4%
Three Controls with Additional Safety System	0.0203%	-99.6%	0.0118%	-99.8%

The values of the high risk were plotted over time using random data for the instances of high flow rates for the tank systems. Table 3-4 shows the random data for each of the tank systems. Figure 3-20 shows the high risk value multiplied by the instances of high flow for each minute of operation. A threshold value of 0.001 or 0.1% was selected to show the minimally acceptable risk level.

The tank with the safety system is the only system to be below the threshold value based on the original Bayesian networks.

Table 3-4: High Risk Probabilities over Time for Each Tank System Using High Flow Data

Minutes	High flow readings in a minute taken each second	High flow readings in one minute	Manual Valves	Manual Valves with Bypass	Level Control System	Level and Flow Control System	Level and Two Flow Control Systems	Level and Two Flow Control and Safety System
0	0	0	0	0	0	0	0	0
1	16	0.267	0.00784	0.00536	0.00683	0.00190	0.00157	3.15E-05
2	16	0.267	0.00784	0.00536	0.00683	0.00190	0.00157	3.15E-05
3	15	0.250	0.00735	0.00503	0.00640	0.00178	0.00147	2.95E-05
4	15	0.250	0.00735	0.00503	0.00640	0.00178	0.00147	2.95E-05
5	15	0.250	0.00735	0.00503	0.00640	0.00178	0.00147	2.95E-05
6	15	0.250	0.00735	0.00503	0.00640	0.00178	0.00147	2.95E-05
7	15	0.250	0.00735	0.00503	0.00640	0.00178	0.00147	2.95E-05
8	15	0.250	0.00735	0.00503	0.00640	0.00178	0.00147	2.95E-05
9	16	0.267	0.00784	0.00536	0.00683	0.00190	0.00157	3.15E-05
10	16	0.267	0.00784	0.00536	0.00683	0.00190	0.00157	3.15E-05
11	16	0.267	0.00784	0.00536	0.00683	0.00190	0.00157	3.15E-05
12	16	0.267	0.00784	0.00536	0.00683	0.00190	0.00157	3.15E-05
13	16	0.267	0.00784	0.00536	0.00683	0.00190	0.00157	3.15E-05
14	16	0.267	0.00784	0.00536	0.00683	0.00190	0.00157	3.15E-05
15	15	0.250	0.00735	0.00503	0.00640	0.00178	0.00147	2.95E-05
16	15	0.250	0.00735	0.00503	0.00640	0.00178	0.00147	2.95E-05
17	15	0.250	0.00735	0.00503	0.00640	0.00178	0.00147	2.95E-05
18	15	0.250	0.00735	0.00503	0.00640	0.00178	0.00147	2.95E-05
19	16	0.267	0.00784	0.00536	0.00683	0.00190	0.00157	3.15E-05
20	15	0.250	0.00735	0.00503	0.00640	0.00178	0.00147	2.95E-05

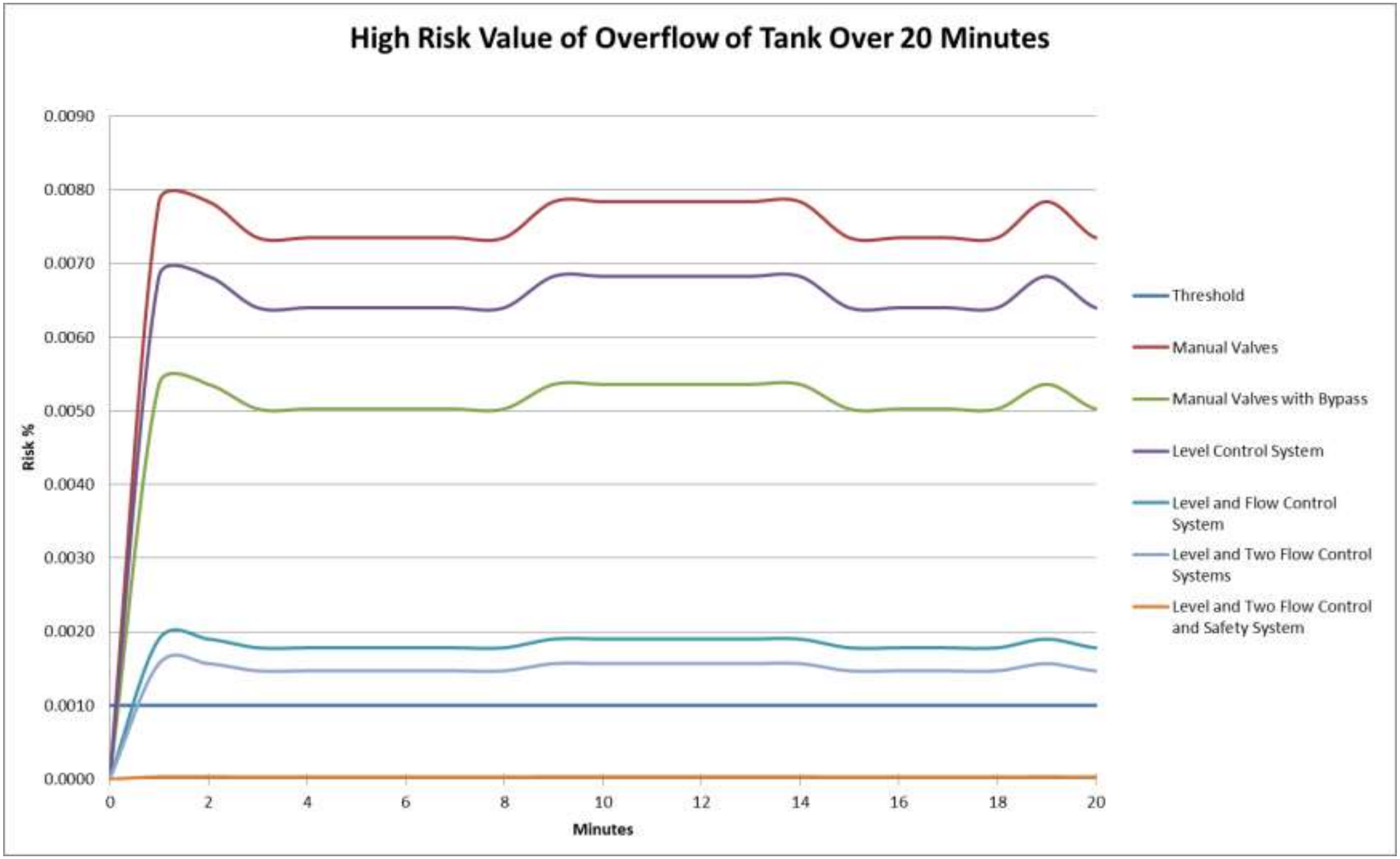

Figure 3-20: High Risk Probabilities Plotted over 20 Minutes for Each Tank System

As an example of how the high risk probability changes with different physical conditions a sample case was used. For this tank, the risk matrix was changed to show the value of the asset as moderate, the population as low, the weather as clear and the material was changed from normal to flammable as shown in Figure 3-21. The results of the high risk change when the material was switched from normal to flammable in shown in Table 3-5.

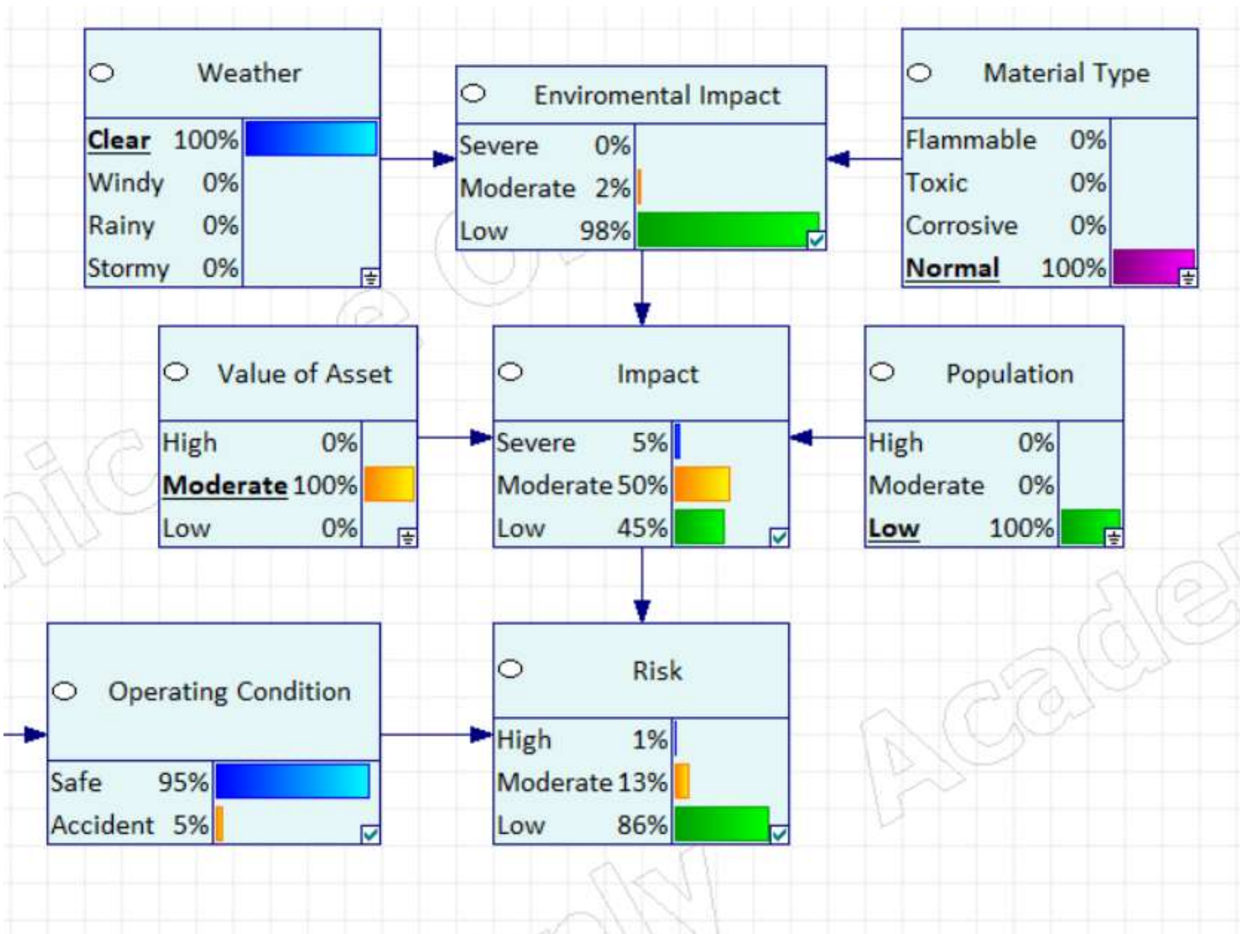

Figure 3-21: Risk Network with Evidence Selected for Case

Table 3-5: High Risk Probability of Tank Systems when Material is changed from Normal to Flammable

	High Risk for Normal Material	High Risk for Flammable Material
Manual Valve System	1.13%	2.14%
Manual System with Bypass Valves	0.771%	1.47%
Level Control System	0.981%	1.87%
Control System with Two Controls	0.273%	0.521%
Control System with Three Controls	0.225%	0.429%
Three Controls with Additional Safety System	0.00451%	0.00858%

Using the same random data given in Table 3-4, Table 3-6 was created to show the probability of an accident for each of the tiers of protection with flammable material. In this scenario, the high risk values for the tanks with two control loops, three control loops and three control loops with a safety system were below the acceptable levels of risk until the weather was changed from clear to windy at 10 minutes. Only the safety system was below the acceptable risk. Since the value is so small, it will be very unlikely that the risk level will ever be above the threshold.

Table 3-6: High Risk Values for all Tank Designs with Normal Material changed to Flammable Material

Minutes	High flow readings in a minute taken each second	High flow readings in one minute	Manual Valves	Manual Valves with Bypass	Level Control System	Level and Flow Control System	Level and Two Flow Control Systems	Level and Two Flow Control and Safety Systems
0	0	0	0	0	0	0	0	0
1	16	0.267	0.00301	0.00206	0.002616	0.000728	0.000600	1.20E-05
2	16	0.267	0.00301	0.00206	0.002616	0.000728	0.000600	1.20E-05
3	15	0.250	0.00283	0.00193	0.002453	0.000683	0.000563	1.13E-05
4	15	0.250	0.00283	0.00193	0.002453	0.000683	0.000563	1.13E-05
5	15	0.250	0.00283	0.00193	0.002453	0.000683	0.000563	1.13E-05
6	15	0.250	0.00283	0.00193	0.002453	0.000683	0.000563	1.13E-05
7	15	0.250	0.00283	0.00193	0.002453	0.000683	0.000563	1.13E-05
8	15	0.250	0.00283	0.00193	0.002453	0.000683	0.000563	1.13E-05
9	16	0.267	0.00301	0.00206	0.002616	0.000728	0.000600	1.20E-05
10	16	0.267	0.00571	0.00392	0.00499	0.00139	0.00114	2.29E-05
11	16	0.267	0.00571	0.00392	0.00499	0.00139	0.00114	2.29E-05
12	16	0.267	0.00571	0.00392	0.00499	0.00139	0.00114	2.29E-05
13	16	0.267	0.00571	0.00392	0.00499	0.00139	0.00114	2.29E-05
14	16	0.267	0.00571	0.00392	0.00499	0.00139	0.00114	2.29E-05
15	15	0.250	0.00535	0.00368	0.00468	0.00130	0.00107	2.15E-05
16	15	0.250	0.00535	0.00368	0.00468	0.00130	0.00107	2.15E-05
17	15	0.250	0.00535	0.00368	0.00468	0.00130	0.00107	2.15E-05
18	15	0.250	0.00535	0.00368	0.00468	0.00130	0.00107	2.15E-05
19	16	0.267	0.00571	0.00392	0.00499	0.00139	0.00114	2.29E-05
20	15	0.250	0.00535	0.00368	0.00468	0.00130	0.00107	2.15E-05

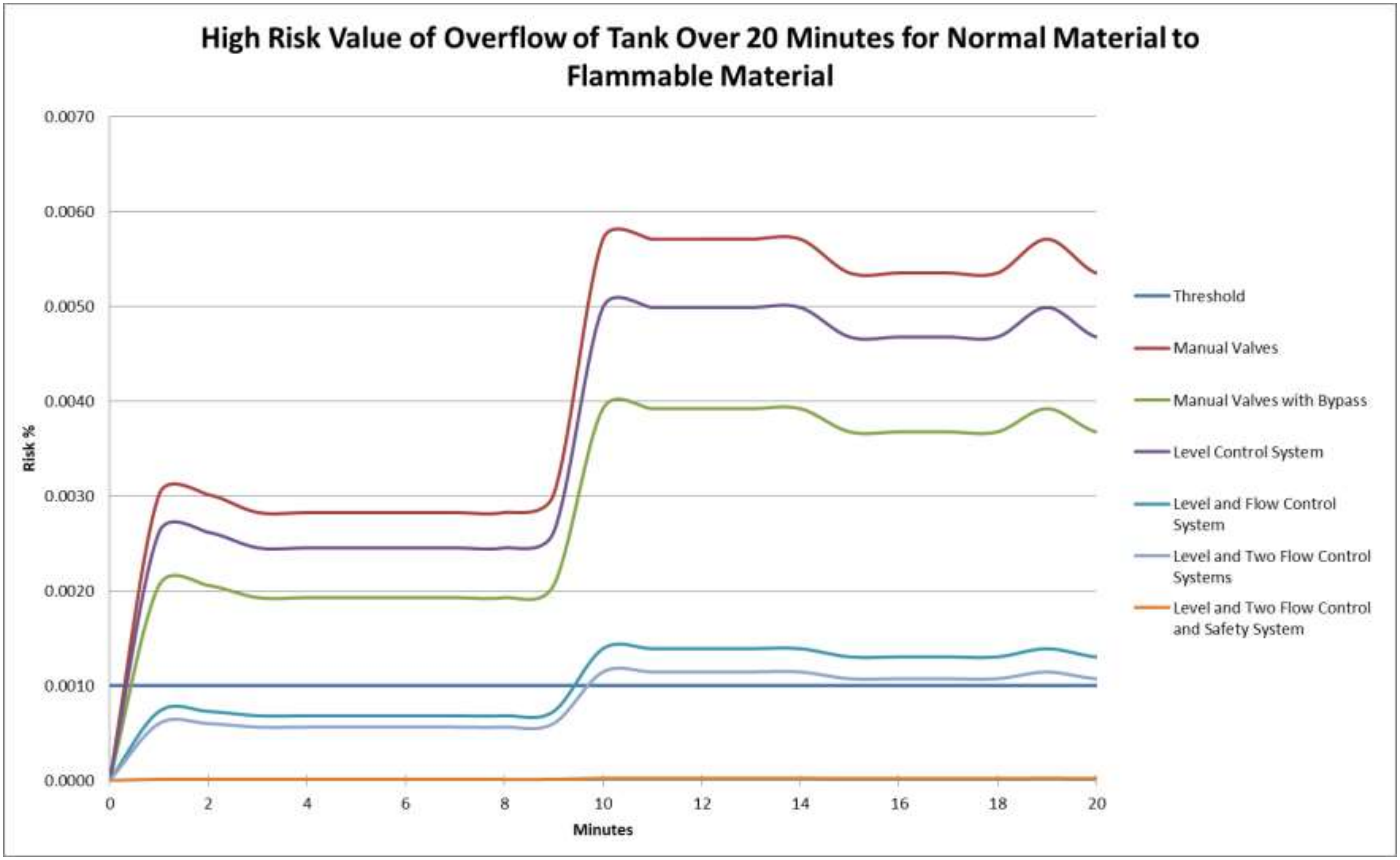

Figure 3-22: High Risk Probability for all Tank Systems for Normal Material changed to Flammable Material

3.5. Conclusion

The work outlined in this chapter proposes a dynamic risk monitoring system for process industries using a Bayesian network. By increasing the safety features, the overall risk to the process was reduced. This method allows for the risk of a process to be monitored in real time, and provides an opportunity for changes to be made to the process to minimize the risk. This method can be applied to other process systems to monitor risk in real time.

4. Chapter 4: Application of Risk Monitoring Methodology to the Williams Geismar Reboiler Rupture and Fire Accident

4.1. Overview

On June 13th, 2013 a reboiler on the propylene fractionator of the Williams Geismar Olefins Plant in Louisiana ruptured and caught fire. This accident killed two plant personal workers and injured 167 (CSB, Williams Geismar Olefins Plant Reboiler Rupture and Fire Geismar, Louisiana, 2016). The methodology presented in Chapter three was applied to this accident to demonstrate real world applications.

Two safety and risk Bayesian networks were created for this case study. The first network created is based on the original design of the reboiler and propylene system. The second network created was based on an updated design using the recommendations by an investigative organization and the additional safety system demonstrated in Chapter three.

The olefins plant operations and the accident are described in this chapter.

4.2. Case Study Background

Olefins, also known as alkenes, are a family of hydrocarbons that have one or more double carbon bonds. The Williams Geismar Olefins Plant produces propylene and ethylene from propane and ethane, respectively. The process for producing ethylene and propylene is shown in Figure 4-1 as a process flow diagram.

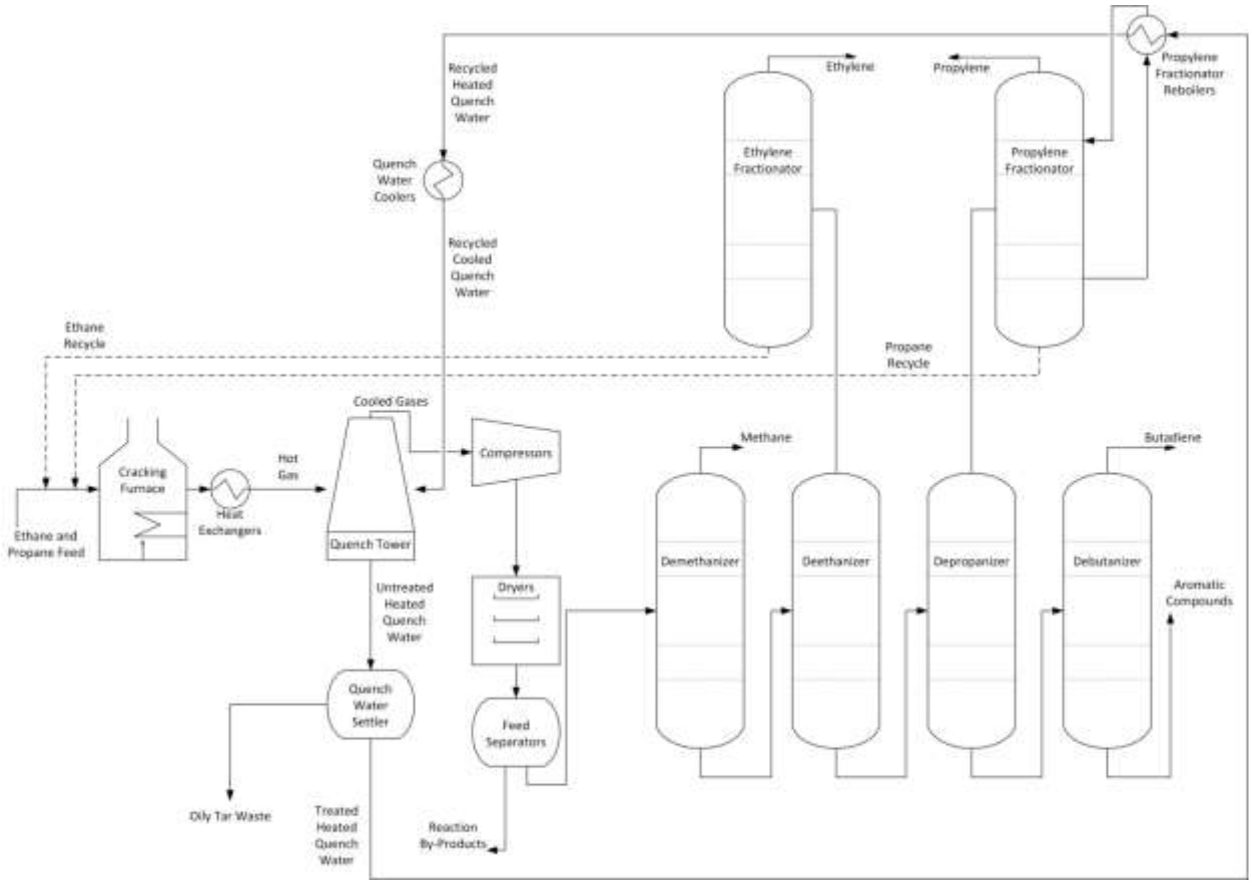

Figure 4-1: Process Flow Diagram of the Williams Geismar Plant

First, ethane and propane enter furnaces where they are converted or cracked into ethylene, propylene and by-products such as methane and butadiene. These gas products are first cooled by heat exchangers after leaving the furnaces. The gases are then further cooled in a quench tower. The cooled gases are then sent to different distillation columns for separation. The demethanizer column removes methane. The deethanizer removes the ethane and ethylene. The depropanizer removes propane and propylene. The remaining gases enter a debutanizer and are separated into butadiene and some other aromatic compounds such as toluene and benzene. The ethylene, propylene, butadiene and aromatic compounds are stored and transported. The ethane and ethylene of the deethanizer are sent to the ethylene fractionator which separates the ethane and ethylene. The ethane is recycled back to the beginning of the process. The propane and propylene from the depropanizer are sent to a propylene fractionator which separates the propane and propylene. The propane, like the ethane, is recycled to the beginning of the process.

In the quench tower, the gases are directly contacted with quench water which is sprayed down from the top. The quench water is heated by the gases and is used to provide heat in other areas of the plant. When the quench water is used for heating in areas of the plant it is cooled. The quench water is further cooled by a cooling system and then recycled back to the quench water tower in a closed system. Since the gas is in direct contact with the water, some gas products are condensed in the water as oily tar products (CSB, Williams Geismar Olefins Plant Reboiler Rupture and Fire Geismar, Louisiana, 2016). The oily products must be removed during a settling process before the water is used for heating. Unfortunately, some of the oily products are left in the quench water.

Each of the distillations columns requires reboilers. The reboilers are shell and tube heat exchangers. The heat for the reboilers is supplied by the treated quench water. The process streams are heated in the shell and the quench water is cooled in the tubes of the reboilers. The oily products in the water are known to build-up on the insides of equipment including heat exchanger tubes. This build-up is known as fouling. Fouling of the tubes reduces the heat transfer potential and decreases flow rates. When the fouling is severe, maintenance is required to remove the oily build up.

The schematic for the propylene fractionator prior to the accident is shown in Figure 4-2. Valves one and two on the tube side are ball valves. Valves three and four on the shell side are gate valves. There is a control valve on the quench water system.

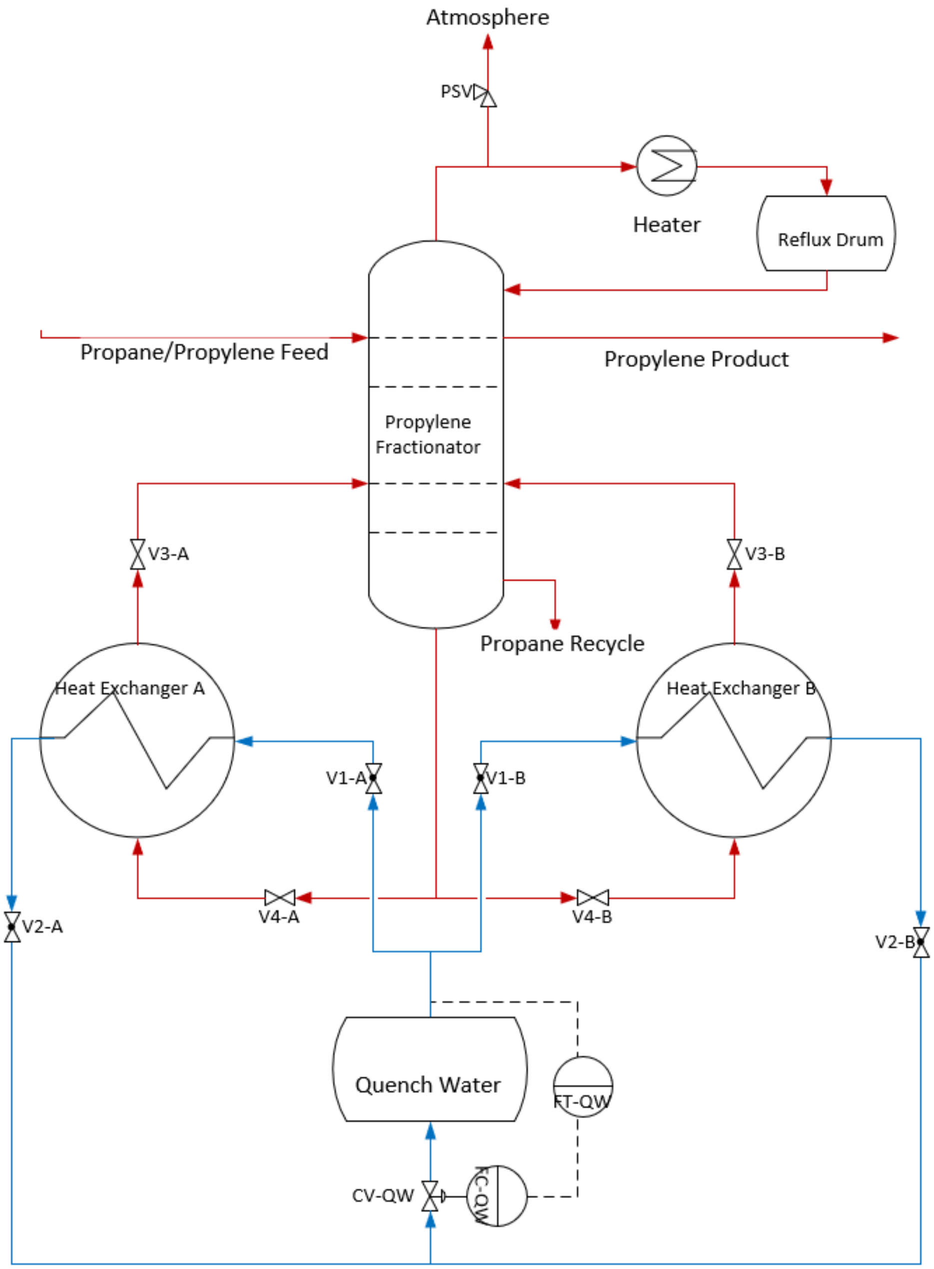

Figure 4-2: Propylene Fractionator Schematic for Williams Geismar Plant

The propylene fractionator had two reboilers, known as Reboiler A and Reboiler B. The reboiler that ruptures and caught on fire was reboiler B. The process fluid on the shell side contained a mixture of 95% propane with the balance propylene and four carbon hydrocarbons such as butane. This thesis with refer to the propane mixture as propane. The quench water entered the reboiler on the tube side to heat the propane on the shell side.

Originally, both reboilers were operated continuously in series. When maintenance on one or both reboilers was required the system was shutdown. In 2001, the reboilers were reconfigured to operate in parallel so that one reboiler could operate when the other required maintenance. After this reconfiguration, the reboilers had additional valves installed so that it could be isolated from the system. The pressure relief devices of the reboilers were located on the top of the fractionator column. When reboiler was isolated from the process it was also isolated from the pressure relief devices. Reboiler B was isolated for 16 months using block valves on both the tube and shell sides (CSB, Williams Geismar Olefins Plant Reboiler Rupture and Fire Geismar, Louisiana, 2016). The block valves were leaking propane into the shell over the duration of the isolation. This leakage was unknown to the plant operators at the time. When a plant employee opened the gate valve on the tube side hot water inlet a Boiling Liquid Expanding Vapor Explosion (BLEVE) occurred. The hot water heated the propane in the shell and caused the liquid to boil and caused the emerging vapor to expand resulting in an explosion. The reboiler shell ruptured due to the increase in pressure and lack of pressure relief. Upon release, the propane mixture caught fire and burned for three and a half hours. (Center for Chemical Process Safety, 2010)

4.3. Methodology Application on Original Reboiler Design

The methodology of chapter two was applied to a real world case study to show the applications. The accident scenario considered for this application is the overpressure of a reboiler. The basis for calculations is the flow of propane entering the shell.

The schematic for the propylene fractionator prior to the accident is shown in Figure 4-2 was used to develop the Bayesian Network.

An overpressure accident scenario for the reboilers would be caused by the following actions: overheating caused by the tube side, isolation from the pressure relief devices and accumulation in the shell (Guo, Khan, & Imtiaz, 2019). An increase of tube side fluid temperature would increase the temperature of the shell side process fluid and subsequently increase the pressure. The tube side fluid heat potential can increase when the flow is increased or the temperature of the fluid increases. If the reboiler is isolated from the pressure relief device, a pressure increase beyond the threshold of the equipment material will result in a rupture.

A network based on the Olefins plant design prior to the accident is shown in Figure 4-3. The basis for the risk calculation is the flow rate of propane entering the reboiler. This network was not based on the templates of chapter three. In this network there are 21 nodes. Table 4-1 shows the characterization and relationships of the nodes within the network. Table 4-2 shows the states of each of the nodes. This model involves the three main events, stated above, that would cause an overpressure accident of the reboiler.

Table 4-1: Bayesian Network Node Characterization and Relationships for the Original Reboiler Design

Node	Node Name	Parent	Child	Characterization
1	Propane Feed Conditions	N/A	Operator Notices Flow Condition	Evidence
2	Operator Notices Flow Condition	Propane Feed Conditions	Tube Side: Inlet Valve; Tube Side: Outlet Valve; Shell Side: Inlet Valve; Shell Side: Outlet Valve	Intermediate
3	Tube Side: Inlet Valve	Operator Notices Flow Condition	Overheating of Heat Exchanger	Intermediate
4	Tube Side: Outlet Valve	Operator Notices Flow Condition	Overheating of Heat Exchanger	Intermediate
5	Shell Side: Inlet Valve	Operator Notices Flow Condition	Accumulation in Shell; Isolated from PSV?	Intermediate
6	Shell Side: Outlet Valve	Operator Notices Flow Condition	Accumulation in Shell; Isolated from PSV?	Intermediate
7	Isolated from PSV?	Shell Side: Inlet Valve; Shell Side: Outlet Valve	Operating Condition	Intermediate
8	Accumulation in Shell	Shell Side: Inlet Valve; Shell Side: Outlet Valve	Operating Condition	Intermediate
9	Flow Transmitter FT-QW Accuracy	N/A	Flow Control Signal to Valve CV-QW	Evidence
10	Flow Control Signal to Valve CV-QW	Flow Transmitter FT-QW Accuracy	Action on Valve CV-QW	Intermediate
11	Action on Valve CV-QW	Flow Control Signal to Valve CV-QW	Overheating of Heat Exchanger	Intermediate
12	Overheating of Heat Exchanger	Change in Quench Water Temperature; Action on Valve CV-QW	Operating Condition	Intermediate
13	Change in Quench Water Temperature	N/A	Overheating of Heat Exchanger	Evidence
14	Operation Condition	Overheating of Heat Exchanger;	Risk	Intermediate

Node	Node Name	Parent	Child	Characterization
		Accumulation in Shell; Isolated from PSV?		
15	Weather	N/A	Environmental impact	Evidence
16	Material type	N/A	Environmental impact	Evidence
17	Value of asset	N/A	Impact	Evidence
18	Population	N/A	Impact	Evidence
19	Environmental impact	Weather; Material type	Impact	Intermediate
20	Impact	Value of asset; Population; Environmental impact	Risk	Intermediate
21	Risk	Impact; Operation Condition	N/A	Query

Table 4-2: Bayesian Network Node States for the Original Design

Node	Node Name	States
1	Propane Feed Conditions	High Flow; No High Flow;
2	Operator Notices Flow Condition	Operator Notices High Flow; Operator Does Not Notice High Flow; No High Flow
3	Tube Side: Inlet Valve	Tube Inlet Open; Tube Inlet Close; No High Flow
4	Tube Side: Outlet Valve	Tube Outlet Open; Tube Outlet Close; No High Flow
5	Shell Side: Inlet Valve	Shell Inlet Open; Shell Inlet Close; No High Flow
6	Shell Side: Outlet Valve	Shell Outlet Open; Shell Outlet Close; No High Flow
7	Isolated from PSV?	Yes Isolated; No Isolated; No High Flow
8	Accumulation in Shell	Yes Accumulation; No Accumulation; No High Flow
9	Flow Transmitter FT-QW Accuracy	FTQW Accurate; FTQW Inaccurate
10	Flow Control Signal to Valve CV-QW	Action Open CV-QW; Action Fail
11	Action on Valve CV-QW	CVQW Open; CVQW Not Open
12	Overheating of Heat Exchanger	QW Temperature Increase; QW Temperature Does Not Increase
13	Change in Quench Water Temperature	Yes Overheating; No Overheating; No High Flow
14	Operation Condition	Safe; Accident
15	Weather	Clear; Windy; Rainy; Stormy
16	Material type	Normal; Flammable; Toxic; Corrosive
17	Value of asset	High; Moderate; Low
18	Population	High; Moderate; Low
19	Environmental impact	Severe; Moderate; Low
20	Impact	Severe; Moderate; Low
21	Risk	High; Moderate; Low

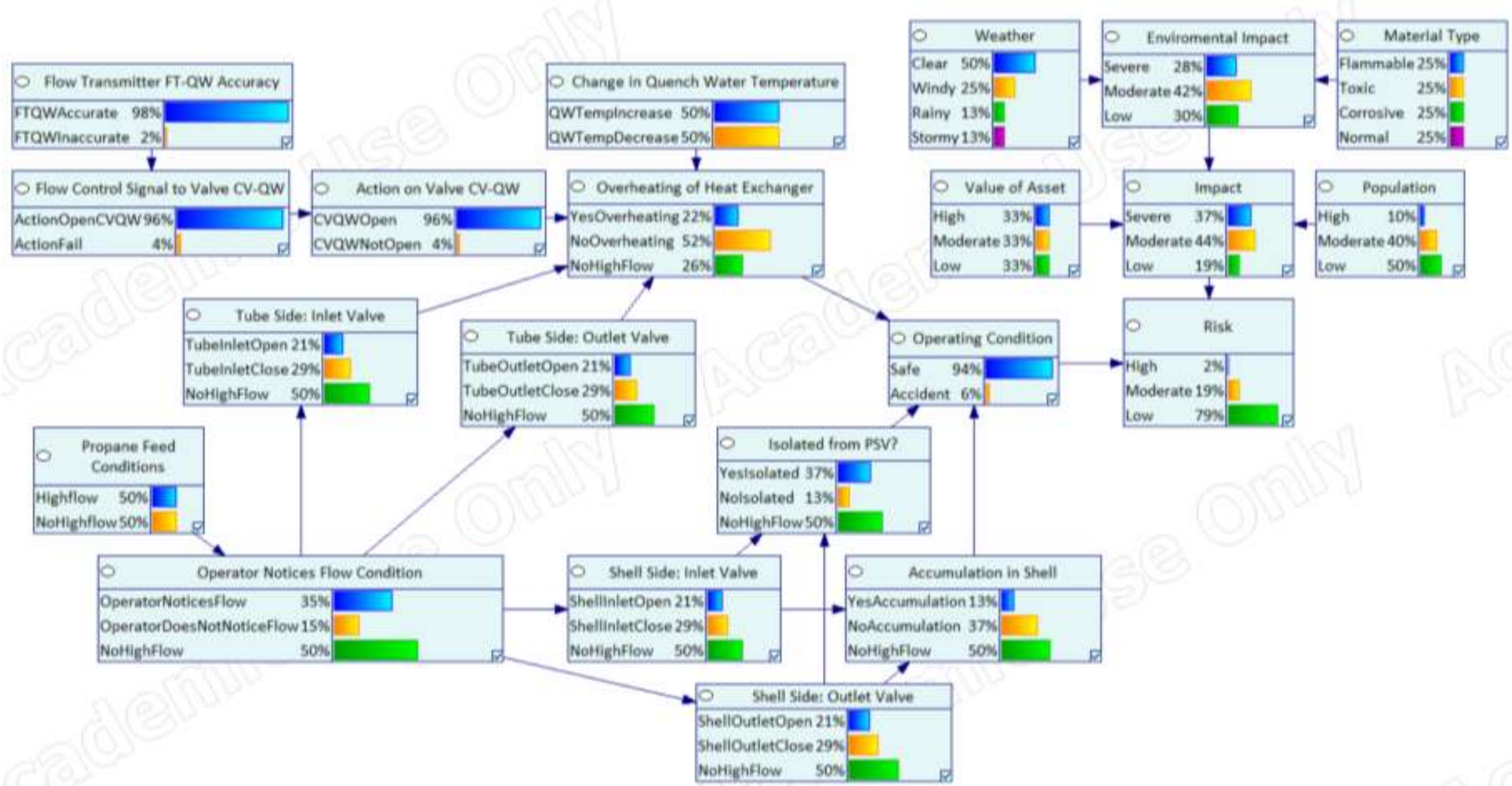

Figure 4-3: Bayesian Network for Original Design of Geismar Plant

Based on the subjective values used in this network, the probability of an accident was 5.60%. The probability of high risk, without any evidence selected, was 1.96%.

The probability of high risk changed to 1.76% when the appropriate evidence was selected. It was assumed that the weather was clear, the population was low, the material type was flammable, and the cost of the asset was moderate.

4.4. Methodology Application on Updated Safe Reboiler Design

The original design of the reboiler systems was poor. The CSB made recommendations for the plant after their investigation was concluded. Most of the recommendations made were based on the management of the plant. One of the recommendations made was that a pressure relief device should be installed on the reboiler shell and not on another piece of equipment. This recommendation was not unexpected. National Board of Boiler and Pressure Vessel Inspectors and National Board Inspection Code (NBIC) require that pressure relief devices are installed on all pressure vessels were the source of overpressure is internal to the vessel. At the time of the accident, Louisiana did not adopt this code (CSB, Williams Geismar Olefins Plant Reboiler Rupture and Fire Geismar, Louisiana, 2016).

As part of the methodology of chapter three, the reboiler system was redesigned with safety controls. Figure 4-4 shows the control systems of Heat Exchanger A. Since the reboilers are operated in parallel it was assumed that both reboilers would have the same separate control systems. In this system, there are three control loops for the tube inlet valve. The tube inlet flow can be based on the temperature of the shell outlet in a feedback loop, the flow of the inlet itself in a feedback loop and the temperature and flow of the shell inlet in a feedforward loop. The flows of the shell outlet, shell inlet and tube outlet are controlled by flow controllers. The quench water flow rate is controlled by the same flow control loop as before in Figure 4-4. A pressure relief device was installed on the shell of each reboiler.

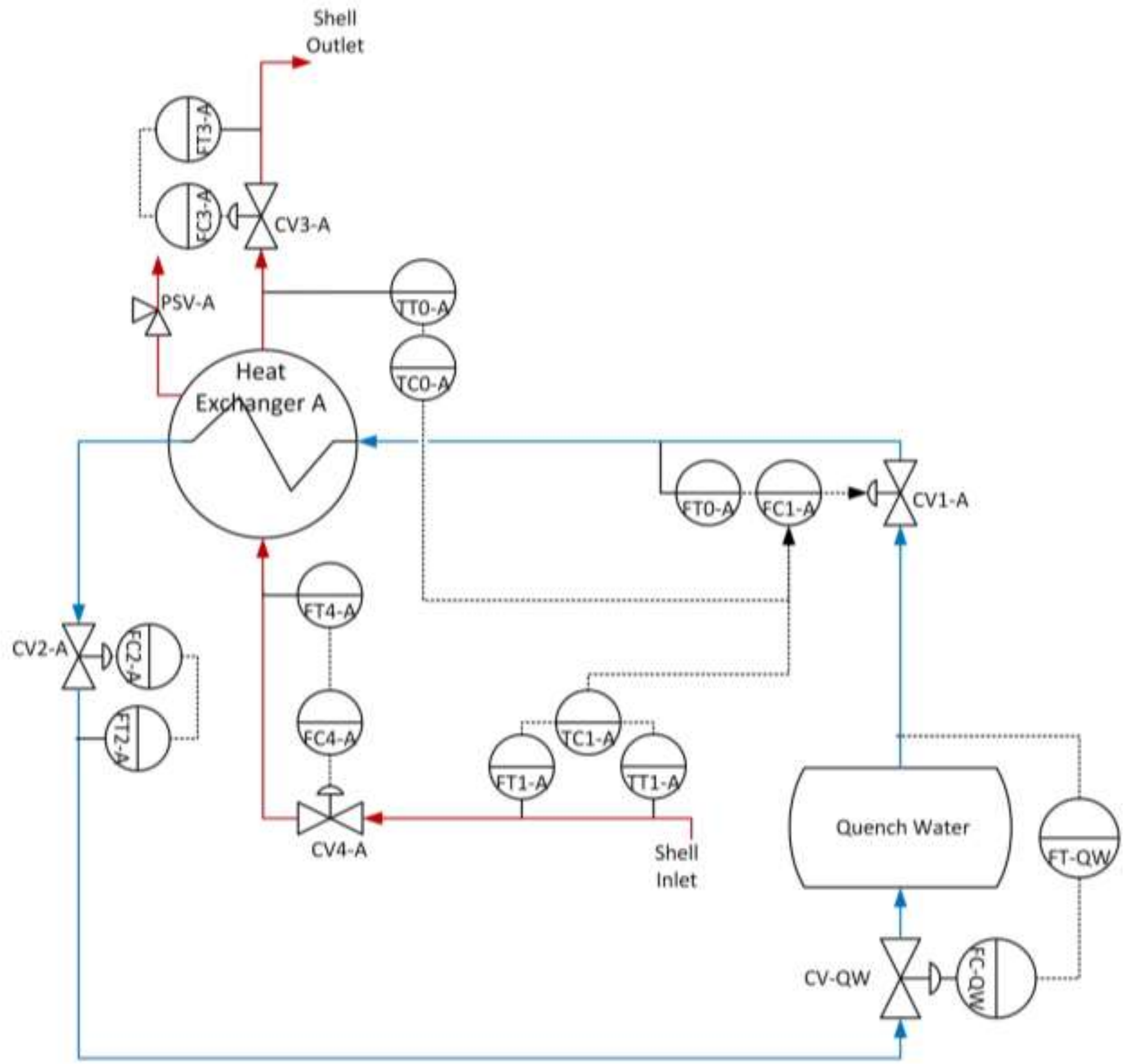

Figure 4-4: Schematic of Controls for Updated Reboiler Design

Similar to the final tank design of chapter three, an additional safety system was installed on the reboilers. For each control loops there are additional sensors and control signals separate from the operation in the case where a system shutdown is required. The control schematic for both heat exchangers is shown in Figure 4-5.

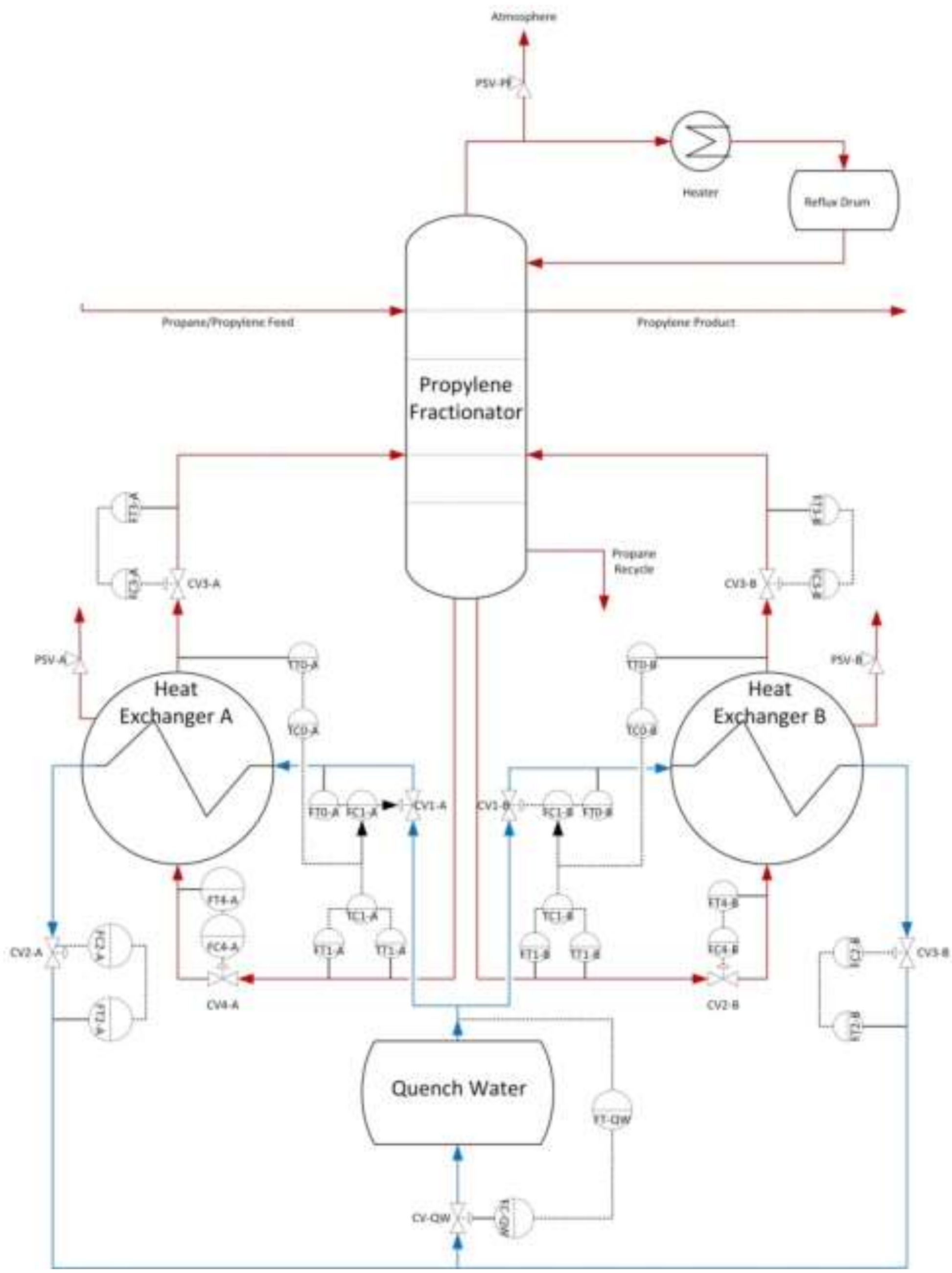

Figure 4-5: Schematic of the Reboiler Design with Two Reboilers

Another network was developed based on the updated safety design of the reboilers including the safety system. Table 3-3 outlines the node characterization and the relationships. There are a total of 49 nodes.

For each of the control loop transmitter nodes there are the following states: transmitter accurate, transmitter inaccurate, control system not operational and no high flow. For the safety control loop transmitters nodes there are the following states: transmitter accurate, transmitter inaccurate, control system not operational, control sensors operational and no high flow. For the control action nodes there are the following states: action success, action fail, control system not operation and no high flow. The safety control action nodes have the states: action success, action fail, control system operational, safety system not operational and no high flow. The nodes that are the same the original design network have the same states in this network.

Table 4-3: Bayesian Network Node Characterization and Relationships for Safe Design

Node	Node Name	Parent	Child	Characterization
1	Flow Conditions	N/A	Control system Condition; Safety System Operational	Evidence
2	Control system Condition	Flow Conditions	Safety System Operational; Flow Transmitter 0 Accuracy; Flow Transmitter 1 Accuracy; Flow Transmitter 2 Accuracy; Flow Transmitter 3 Accuracy; Flow Transmitter 4 Accuracy; Temperature Transmitter 0 Accuracy; Temperature Transmitter 1 Accuracy	Intermediate
3	Flow Transmitter 0 Accuracy (Tube Inlet)	Control system Condition	Flow Control 0 Signal	Intermediate
4	Flow Transmitter 1 Accuracy (Tube Inlet)	Control system Condition	Flow Control 1 Signal	Intermediate
5	Flow Transmitter 2 Accuracy (Tube Outlet)	Control system Condition	Flow Control 2 Signal	Intermediate
6	Flow Transmitter 3 Accuracy (Shell Outlet)	Control system Condition	Flow Control 3 Signal	Intermediate
7	Flow Transmitter 4 Accuracy (Shell Inlet)	Control system Condition	Flow Control 4 Signal	Intermediate
8	Temperature Transmitter 0 Accuracy (Tube Inlet)	Control system Condition	Temperature Control Signal 0	Intermediate
9	Temperature Transmitter 1 Accuracy (Tube Inlet)	Control system Condition	Temperature Control Signal 1	Intermediate
10	Temperature Control Signal 0 (Tube Inlet)	Temperature Transmitter 0 Accuracy	Control Action Effectiveness (Tube Side)	Intermediate
11	Temperature Control Signal 1 (Tube Inlet)	Temperature Transmitter 1 Accuracy	Control Action Effectiveness (Tube Side)	Intermediate

Node	Node Name	Parent	Child	Characterization
12	Flow Control 0 Signal (Tube Inlet)	Flow Transmitter 0 Accuracy	Control Action Effectiveness (Tube Side)	Intermediate
13	Flow Control 1 Signal (Tube Inlet)	Flow Transmitter 1 Accuracy	Control Action Effectiveness (Tube Side)	Intermediate
14	Flow Control 2 Signal (Tube Outlet)	Flow Transmitter 2 Accuracy	Control Action Effectiveness (Tube Side)	Intermediate
15	Flow Control 3 Signal (Shell Outlet)	Flow Transmitter 3 Accuracy	Control Action Effectiveness (Shell Side)	Intermediate
16	Flow Control 4 Signal (Shell Inlet)	Flow Transmitter 4 Accuracy	Control Action Effectiveness (Shell Side)	Intermediate
17	Control Action Effectiveness (Shell Side)	Flow Control 3 Signal (Shell Outlet); Flow Control 4 Signal (Shell Inlet);	Accumulation in Shell	Intermediate
18	Control Action Effectiveness (Tube Side)	Flow Control 0 Signal (Tube Inlet); Flow Control 1 Signal (Tube Inlet); Flow Control 2 Signal (Tube Outlet); Temperature Control 0 Signal (Tube Inlet); Temperature Control 1 Signal (Tube Inlet)	Overheating on Tube Side	Intermediate
19	Safety System Operational	Control system Condition	Safety Flow Transmitter 0 Accuracy; Safety Flow Transmitter 1 Accuracy; Safety Flow Transmitter 2 Accuracy; Safety Flow Transmitter 3 Accuracy; Safety Flow Transmitter 4 Accuracy; Safety Temperature Transmitter 0 Accuracy; Safety Temperature Transmitter 1 Accuracy	Intermediate
20	Safety Flow Transmitter 0 Accuracy	Safety System Operational	Safety Flow Control 0 Signal	Intermediate
21	Safety Flow Transmitter 1 Accuracy	Safety System Operational	Safety Flow Control 1 Signal	Intermediate

Node	Node Name	Parent	Child	Characterization
22	Safety Flow Transmitter 2 Accuracy	Safety System Operational	Safety Flow Control 2 Signal	Intermediate
23	Safety Flow Transmitter 3 Accuracy	Safety System Operational	Safety Flow Control 3 Signal	Intermediate
24	Safety Flow Transmitter 4 Accuracy	Safety System Operational	Safety Flow Control 4 Signal	Intermediate
25	Safety Temperature Transmitter 0 Accuracy	Safety System Operational	Safety Temperature Control Signal 0	Intermediate
26	Safety Temperature Transmitter 1 Accuracy	Safety System Operational	Safety Temperature Control Signal 1	Intermediate
27	Safety Temperature Control Signal 0	Safety System Operational	Safety Action Effectiveness (Tube Side)	Intermediate
28	Safety Temperature Control Signal 1	Safety System Operational	Safety Action Effectiveness (Tube Side)	Intermediate
29	Safety Flow Control 0 Signal	Safety Flow Transmitter 0 Accuracy	Safety Action Effectiveness (Tube Side)	Intermediate
30	Safety Flow Control 1 Signal	Safety Flow Transmitter 1 Accuracy	Safety Action Effectiveness (Tube Side)	Intermediate
31	Safety Flow Control 2 Signal	Safety Flow Transmitter 2 Accuracy	Safety Action Effectiveness (Tube Side)	Intermediate
32	Safety Flow Control 3 Signal	Safety Flow Transmitter 3 Accuracy	Safety Action Effectiveness (Shell Side)	Intermediate
33	Safety Flow Control 4 Signal	Safety Flow Transmitter 4 Accuracy	Safety Action Effectiveness (Shell Side)	Intermediate
34	Safety Action Effectiveness (Tube Side)	Safety Flow Control 0 Signal; Safety Flow Control 1 Signal; Safety Flow Control 2 Signal; Safety Temperature Control 0 Signal; Safety Temperature Control 1 Signal	Overheating on Tube Side	Intermediate
35	Safety Action Effectiveness (Shell Side)	Safety Flow Control 3 Signal; Safety Flow Control 4 Signal;	Accumulation in Shell	Intermediate

Node	Node Name	Parent	Child	Characterization
36	Flow Control Action on CV-QW	FT-QW Accuracy	Overheating on Tube Side	Intermediate
37	FT-QW Accuracy	N/A	Flow Control Action on CV-QW	Evidence
38	Quench Water Temperature Increase	N/A	Overheating on Tube Side	Evidence
39	Accumulation in Shell	Safety Action Effectiveness (Shell Side); Control Action Effectiveness (Shell Side)	Operating Condition	Intermediate
40	Overheating on Tube Side	Safety Action Effectiveness (Tube Side); Control Action Effectiveness (Tube Side); Quench Water Temperature Increase; Flow Control Action on CV-QW	Operating Condition	Intermediate
41	Is PSV Operational?	N/A	Operating Condition	Evidence
42	Operating Condition	Accumulation in Shell; Overheating on Tube Side; Is PSV Operational?	Risk	Intermediate
43	Weather	N/A	Environmental impact	Evidence
44	Material type	N/A	Environmental impact	Evidence
45	Value of asset	N/A	Impact	Evidence
46	Population	N/A	Impact	Evidence
47	Environmental impact	Weather; Material type	Impact	Intermediate
48	Impact	Value of asset; Population; Environmental impact	Risk	Intermediate
49	Risk	Impact; Operation Condition	N/A	Query

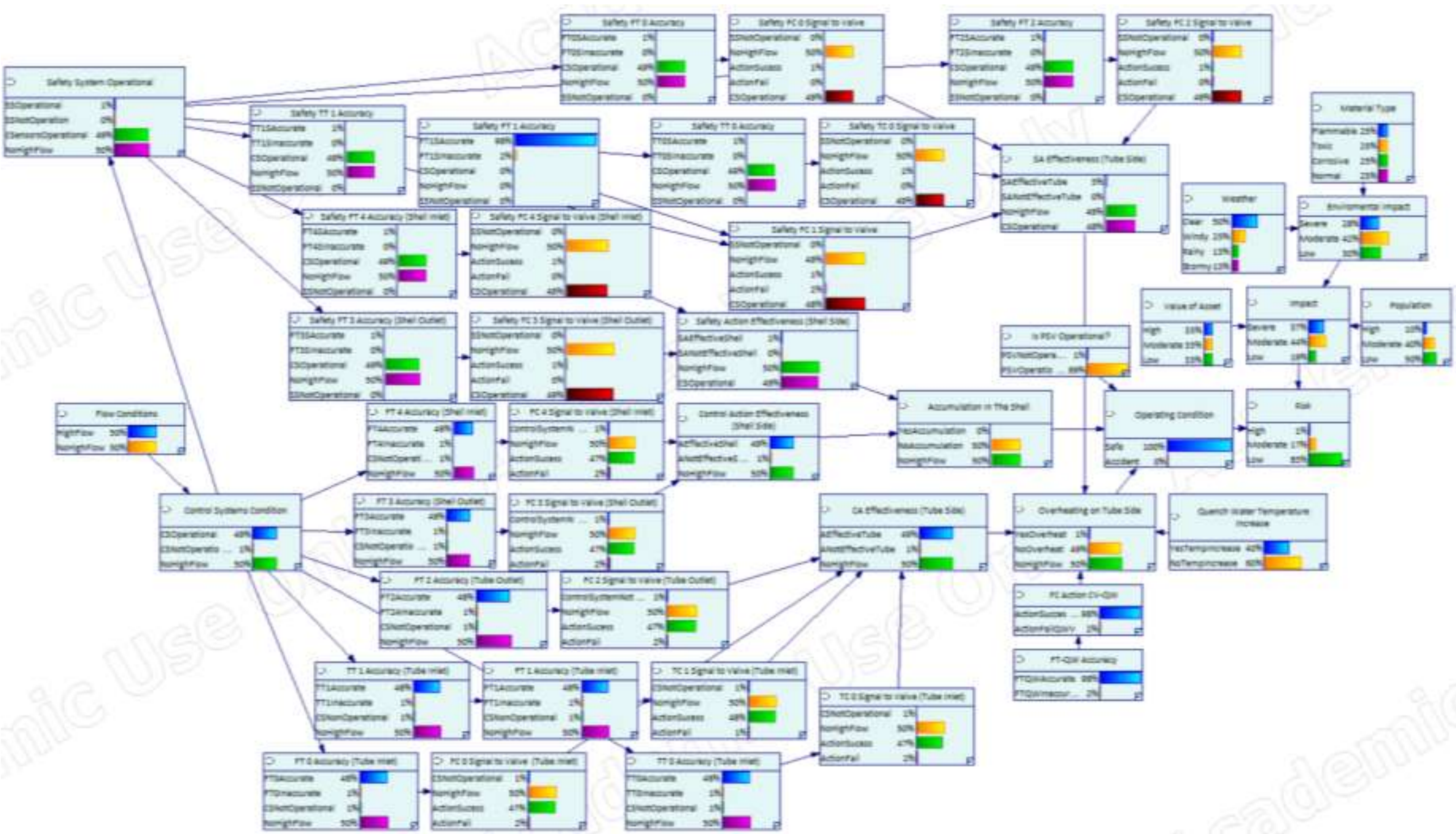

Figure 4-6: Bayesian Network of the Updated Reboiler Design

The network for the safe design is shown in Figure 4-6. The probability of accident was decreased to 0.249% from 5.60% and the probability of high risk was decreased to 0.501% from 1.96%. With the same evidence selected for the original design, the high risk probability was decreased 0.407% from 1.76%. The probability for an overpressure accident was decreased by 95.6% and the high risk probability was decreased 76.9% by with these additional safety measures.

4.5. Risk of Reboiler Rupture Monitored Over Time

The risk and flow rate of propane entering the shell was plotted over time in Figure 4-7. Table 4-4 shows the data used to plot the risk over time.

Table 4-4: Sample Data for Plotting Risk of Original and Updated Design over Time

Minutes	High flow readings in a minute taken each second	High flow readings in one minute	Reboiler Safety Re-Design	Original Reboiler Design of 2001
1	3	0.0500	0.000204	0.000880
2	3	0.0500	0.000204	0.000880
3	3	0.0500	0.000204	0.000880
4	3	0.0500	0.000204	0.000880
5	4	0.0670	0.000271	0.00117
6	4	0.0670	0.000271	0.00117
7	4	0.0670	0.000271	0.00117
8	4	0.0670	0.000271	0.00117
9	6	0.100	0.000407	0.00176
10	6	0.100	0.000407	0.00176
11	6	0.100	0.000407	0.00176
12	6	0.100	0.000407	0.00176
13	6	0.100	0.000407	0.00176
14	6	0.100	0.000407	0.00176
15	5	0.0830	0.000339	0.00147
16	5	0.0830	0.000339	0.00147
17	5	0.0830	0.000339	0.00147
18	5	0.0830	0.000339	0.00147
19	5	0.0830	0.000339	0.00147
20	5	0.0830	0.000339	0.00147
21	5	0.0830	0.000339	0.00147
22	5	0.0830	0.000339	0.00147
23	5	0.0830	0.000339	0.00147
24	5	0.0830	0.000339	0.00147
25	4	0.0670	0.000271	0.00117
26	4	0.0670	0.000271	0.00117
27	4	0.0670	0.000271	0.00117
28	4	0.0670	0.000271	0.00117
29	4	0.0670	0.000271	0.00117
30	4	0.0670	0.000271	0.00117

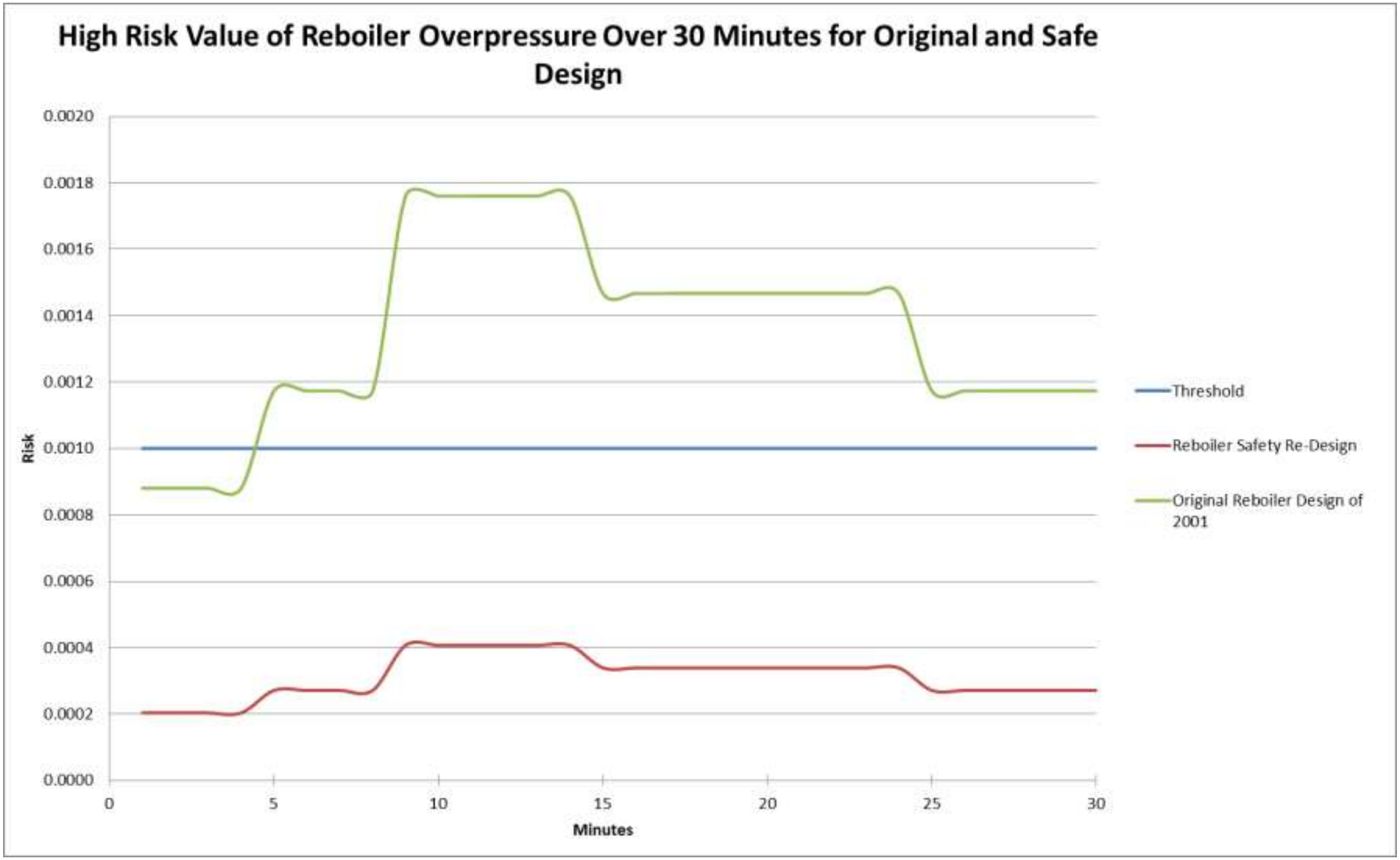

Figure 4-7: Plot of Risk over Time for both Original and Updated Reboiler Design

As shown in Figure 4-7, the risk level for the reboiler with the new design is much less risky as it is below the threshold. Since there are two reboilers, the data for the second could be used with the same matrix and its different conditions. Both reboiler overpressure risks could be plotted on the same graph.

4.6. Conclusion

For the Williams Geismar plant, the design was highly risky. It required significant revision to be a safer design. Analyzing the accident using the proposed methodology it is observed that if a monitoring system had been put in place, an accident may not have occurred. This risk monitoring system only considered the event of an over pressured reboiler and does not consider other accident scenarios. Incorporating different accident scenarios into a single matric is part of further work.

5. Chapter 5: Conclusion and Future Work

5.1. Conclusions

In conclusion, risk can be monitored in a process system over time. While event trees are commonly used in risk assessments, this thesis describes how event trees can be modified into Bayesian networks. Event trees are static and lack flexibility for accurately determining risk in a process system. Bayesian networks are beneficial for risk prediction as they are dynamic and can change in real time to more accurately reflect process operations. The risk values produced by these networks can be used with process data to monitor process risk in real time. A summary of each chapter is as follows.

Chapter one introduces safety and risk monitoring in process systems. The research motivation, objectives and outline were described in this chapter.

Chapter two describes a literature review completed on process safety and risk, monitoring and modelling. Different process accidents were described, as well as different accident modelling techniques. The risk assessment method that is becoming more popular in literature and industry was used in the development of the methodology in chapter three. The factors influence safety

Chapter three proposes a methodology for developing a risk monitoring model using event tree and Bayesian networks. These networks can be used to monitor risk in real time. Bayesian network uses and applications were described. A simple example of an overflowing tank is used as basis for the network model. The design of the tank was improved upon in six steps to show how the improvements in safety reduce the overall risk of the process. The risk of the overflowing tank was plotted over time. The Bayesian network is dynamic and is used to show how changing conditions improve or worsen the risk. It was shown how the Bayesian network can improve the prediction of an accident over the event tree as independent factors that could lead to an accident could be captured. This methodology created a framework for future studies and the ability to apply it to cases as seen in chapter four.

Chapter four applies the methodology developed in chapter three to a real work case. The reboiler rupture and fire at the Williams Geismar Olefins Plant was used a case study. The accident of an over pressured reboiler was used for the network. A network was created based on the original design of the reboilers. A second network was created after safety based design features were implemented on the original set up. The risk values of the original and updated networks were plotted over time. The conditional probabilities for the final operating conditions were the same for both the original and safe designs. By updating the design of the reboiler to include safety features and controls the accident probability was decreased by 96% and the high risk probability was decreased 76.9%. By plotting the risk overtime, future projections of risk for the plant can be predicted and action can be taken to prevent accidents before they could occur.

5.2. Future Work

The methodology presented in this thesis can be improved upon by considering multivariate parameters. The developed methodology also needs to be tested using experimental data. As the values used in the Bayesian networks are subjective, the accuracy of the networks can be improved upon by the use of credible objective data. The methodology presented here shows the creation of a network based on a single accident type. In the future, the networks may be updated to include multiple different hazards of a process instead of a single event. The methodology will need to be applied to more complex case studies and if possible through lab and field experiments to check its applicability and usefulness.

References

Abbassi, R., Garaniya, V., & Khan, F. (2016). An Application of BN to Envisage Potential Accidents in FLNG Facility. *ISOPE Pacific/Asia Offshore Mechanics Symposium* . Queensland.

Al-shanini, A., Ahmad, A., & Khan, F. (2014). Accident modelling and analysis in process industries. *Journal of Loss Prevention in the Process Industries*, 319-334.

Al-shanini, A., Ahmad, A., & Khan, F. (2014). Accident modelling and analysis in process industries. *Journal of Loss Prevention in the Process Industries*, 319-344.

CCPS. (2001). *Layer of Protection Analysis: Simplified Process Risk Assessment.* New York : American Institute of Chemical Engineers .

Center for Chemical Process Safety. (2010). *Guidelines for Vapor Cloud Explosion, Pressure Vessel Burst, BLEVE, and Flash Fire Hazards.* Hoboken: John Wiley & Sons, Inc.

Chakraborty, S. P.-R. (2003). Risk-based Safety Performance Indicators for Nuclear Power Plants. *17th International Conference on Structural Mechanics in Reactor Technology*. Prague.

Crowl, D., & Louvar, J. (2011). *Chemical Process Safety: Fundamentals with Applications.* Boston: Pearson Education Inc.

CSB. (2014). *Metal Dust Explosion and Fire* . Washington: CSB.

CSB. (2016). *Investigation Report: Drilling Rig Explosion and Fire at the Macondo Well.* Washington: Chemical Safety Board.

CSB. (2016). *Tesoro Martinez Refinery: Process Safety Culture Case Study* . Washington: CSB.

CSB. (2016). *Williams Geismar Olefins Plant Reboiler Rupture and Fire Geismar, Louisiana.* Washington: U.S. Chemical Safety and Hazard Investigation Board.

CSB. (2018). *Key Lessons for Preventing Inadvertent Mixing During Chemical Unloading Operations.* Washington: CSB.

CSB. (2018). *Organic Peroxide Decomposition, Release, and Fire at Arkema Crosby Following Hurricane Harvey Flooding.* Washington: CSB.

Dan, S., Lee, C. J., Park, J., Shin, D., & Yoon, E. S. (2014). Quantitative risk analysis of fire and explosion on the top-side LNG-liquefaction process of LNG-FPSO. *Process Safety and Environmental Protection, 92*, 430-441.

Darwiche, A. (2009). *Modeling and Reasoning with Bayesian Networks.* Cambridge University Press.

Guo, C., Khan, F., & Imtiaz, S. (2019). Copula-based Bayesian network model for process system risk assessment. *Process Safety and Environmental Protection*, 317-326.

Haight, J., & Caringi, R. G. (2007). Automation vs. human intervention: What is the best mix for optimum system performance? A case study. *International Journal of Risk Assessment and Management*, 708-721.

IADC. (2015). *Health, Safety and Environment Case Guidelines for Mobile Offshore Drilling Units - 4. Risk Management.* IADC.

Ibe, O. C. (2011). *Fundamentals of Stochastic Networks.* Hoboken: John Wiley & Sons, Inc.

Khan, F., Abunada, H., John, D., & Benmosbah, T. (2009). Development of Risk-Based Process Safety Indicators. *Process Safety Progress*, 133-143.

Kujath, M., Amyotte, P., & Khan, F. (2010). A conceptual offshore oil and gas process accident model. *Journal of Loss Prevention in the Process Industries*, 323-330.

Marsh, D., & Bearfield, G. (2008). Generalizing event trees using Bayesian networks. *Journal of Risk and Reliability,, 222*(O2), 104-114.

Samith, R., Khan, F., & Amyotte, P. (2011). SHIPP methodology: Predictive accident modeling approach. Part I: Methodology and model description. *Process Safety and Environmental Protection*, 151-164.

Shahri, H. R., MahdaviNejad, R. A., & AmirKabir, S. A. (2016). A Review of Recent Safety Research Activities on LNG Operation. *SPE Asia Pacific Oil & Gas Conference and Exhibition.* Perth.

Unnikrishnan, G., Shrihari, & Siddiqui, N. A. (2014). APPLICATION OF BAYESIAN METHODS TO EVENT TREES WITH CASE STUDIES. *Reliability: Theory & Applications*, 32-45.

You, X., & Tonon, F. (2012). Event-Tree Analysis with Imprecise Probabilities. *Risk Analysis*, 330-344.