The System Theoretic Accidental Analysis of A Crude Unit Refinery Fire Incident

by

Pitiporn Thammongkol

M. Eng., Chemical Engineering
Imperial College London (2003)

Submitted to the System Design and Management Program in Partial Fulfillment of the Requirements for the Degree of

Master of Science in Engineering and Management

at the

Massachusetts Institute of Technology
June 2014

Signature of Author Signature redacted

Pitiporn Thammongkol
System Design and Management Program

Certified by Signature redacted

Qi Hommes, Thesis Supervisor
Engineering Systems Division

Accepted by Signature redacted

Patrick Hale, Director
System Design and Management Program

Acknowledgements

I would like to express my sincere appreciation for my professor and thesis advisor, Dr. Qi Hommes, who has been a constant source of guidance and encouragement throughout my thesis work. Throughout my research, Dr. Hommes' assistance was critical in helping me understand the STAMP process, and apply STAMP methods prospectively in the accident analysis. Thank you for giving me an opportunity to work with you over this spring term under this limited time with your great patient and kind support.

I also wish to express my sincere thanks Professor Nancy Leveson. She has certainly inspired me into seeing safety from different perspectives. I have gained a lot of understanding of engineering system from her System Safety course and hopefully, I will be able to utilize this knowledge in my future works to reduce industrial accidents.

I would also like to thank John Edmed (my mentor at Chevron) who has inspired me with safety engineering. Working with him is one of the greatest experiences I ever had. Thank you for continuing to believe in me and always give me the opportunities and best supports whenever I need.

To my family, I hope that I can make them proud. Thank you for encouraging me throughout, for their immense support, and for the ever-lasting love. They have made me who I am today.

Lastly, I would like to thank to all my friends for their kinds of supports especially for this thesis and for great advises throughout my time here.

Abstract

Catastrophic chemical process accidents in the past such as Bhopal (India) and Flixborough (UK) have led to a major increase in societal concerns about the safety of these processing facilities. As the petrochemical industry has changed considerably over the past several decades due to changes in technology, automation control and greater integration of work services, this has led industry operations to become more advanced and complex. Therefore, when accidents occur, they usually have an involvement of multiple factors, which suggests that there are underlying complex systemic problems. Nevertheless, typical accident investigations often show that most accidents were preventable; identifying the cause of the accidents and monitoring warning signs are crucial to preventing the accidents.

The main objective of this thesis is to develop a better understanding of the missing causal identification from the use of traditional Swiss cheese base accidental model compared to a structured system-based method. This thesis applies Prof. Leveson's System Theoretic Accident Model and Processes, STAMP-CAST, on a case study of the August 2012 Richmond Refinery fire involving a crude unit. Then STAMP-STPA will be use in an example to develop warning signs to detect the deterioration of the Refinery's safety integrity. The analysis identified is complimentary to the refinery and regulatory controls that were not articulately expressed in the company's investigation report. These analyses are included in subsequent sections of this thesis to answer the research question "What could be done differently to understand the causes of accidents and prevent them?"

Table of Contents

Acronyms and Abbreviations

4-CU	Crude Unit (Distillation column) No.4
4-SC	Side Cut No.4 (piping branch of Crude Unit)
API	American Petroleum Institute
CalARP	California Accidental Release Prevention Program
CAL EMA	California Emergency Management Agency
CAST	Causal Analysis base on STAMP
CCC	Contra Costa County
CCHMP	Contra Costa Health Service's Hazard Material Program
CCHS	Contra Costa Health Service
CCPS	Center of Chemical Process Safety
CFD	Chevron Fire Department
CFR	Code of Federal Regulations
CML	Condition Monitoring Location
CSB	Chemical Safety Board
CUPA	Certified Unified Program Agency
CUSA	Chevron USA
CWS	Community Warning System
EPA	Environmental Protection Agency
EPCRA	Emergency Planning and Community Right-to-Know Act
ETC	Energy Technology Company
EWaSAP	Early Warning Sign Approach
HAZOP	Hazard and Operability
HC	Hydrocarbon
HSE	Health and Safety Executive
IPR	Intensive Process Review
KPI	Key Performance Indicator
ISO	Industrial Safety Ordinance
LOPA	Layer of Protection Analysis
MOC	Management of Change
OSHA	Occupational Safety and Health Administration
PHA	Process Hazard Analysis e.g. Hazop
PPE	Personal Protective Equipment
PSI	Process Safety Information
PSM	Process Safety Management
RC	Richmond City
RBI	Risk Base Inspection
RISO	Richmond Industrial Safety Ordinance
RMP	Risk Management Plan
ROI	Reliability Opportunity Identification
STAMP	Systems Theoretic Accidental Model and Processes
STPA	System Theoretic Process Analysis

Chapter 1 Introduction

The Problem

Catastrophic chemical process accidents in the past such as Bhopal (India) and Flixborough (UK) have led to a major increase in societal concerns about the safety of these processing facilities. Many regulations initially focused on preventing accidents through better technical control of the individual aspects of chemical processes. However, the continued occurrence of catastrophic process accidents led to a new industry paradigm regarding the causation of low probability – high consequence accidents.

Investigation of major accidents in the petrochemical industry and major hazard installations have shown that it is vital that chemical companies know that systems designed to control risks operate as intended. Therefore, the prevention of process accidents requires effective process safety management systems (PSM) on top of appropriate technical practices, as deficiencies in management systems are the underlying root cause of most chemical process. This current framework for thinking about process safety builds upon four different pillars:

- Commitment to process safety
- Understand hazards and evaluate risk
- Manage risk
- Learn from experiences.

As the petrochemical industry has changed considerably over the past several decades due to change in technology, automation control and greater integration of work services, this has led industry operations to become more advanced and complex. Therefore, when accidents occur, they usually have an involvement of multiple factors, which suggests that there are underlying complex systemic problems [23]. Typical accident investigations often show that most accidents were preventable; identifying the cause of the accidents and monitoring warning signs are crucial to preventing the accidents.

Research Question: What could be done differently to understand the causes of accidents and prevent them?

Having worked in the petrochemical industry and studied system based courses such as System Engineering, System Safety and System Dynamics at MIT, my curiosity arose on how much we may have missed in identifying real causes and factors involved in accidents in petrochemical industry. In most accident investigation models, the traditional causality model, often referred to as the 'Swiss Cheese' model, is usually used as a basis (reference upcoming definition on page 10). This means that accidents are considered to be caused by chains of failure events, each failure directly causing the next one in the chain [6]. However, in a complex system, which involves facility design, construction, operation and maintenance like in petrochemical industry, the causes of an accident may not entirely arise from individual phases or functions. Hence, the linear chain-of-events accident causality model may have a limitation to clearly identify those causes. Therefore, the objectives of this research thesis are as follows:

- To compare the effectiveness of Systems-Theoretic Accident Model and Processes[1] (STAMP) vs Swiss cheese model in identifying causes of process accidents
- To examine whether the organizational structure, management systems and safety culture in place actually prohibit incidents to occur or become part of the cause.
- To demonstrate an application of system theory model to assist the company with improvement to their existing management system such as Process Safety Management.

Research Approach

In order to meet the research objective, this research involves reviewing the literature and current industrial practices and looks from a systems approach for exploring means to improve on safety control structures as well as identifying warning indicators that can be

[1] STAMP is a new accident causality model based on systems theory and systems thinking described in Nancy Leveson's new book "Engineering a Safer World" [13]

integrated into the existing industrial framework such as PSM to maintain the integrity of the system throughout the life cycles. The following tools from system thinking approach will be used:

- STAMP - CAST[2] to identify accident causes and gap between existing tools use in the industry
- STPA[3] will be use to identify warning indicator
- A System Dynamics model will be use to illustrate factors involve in the accident

[2] CAST is the equivalent for accident/incident analysis base on STAMP which involve system theory and system thinking
3 STPA is a new hazard analysis technique based on STAMP

Chapter 2 Literature Review

Swiss Cheese Accidental Model Concept

James Reason proposed the image of "Swiss cheese" model to explain the occurrence of system failures or to model accident causality base on the concept of active and latent failures /condition. According to Reason, active failures are the actions or inactions of front line operators (e.g. control room crew, pilot) that are believed to cause the accident. Conversely, latent failures/conditions are errors that exist within the organization or elsewhere in the supervisory chain of command that affect the sequence of events ultimately resulting in an accident. A condition is not a cause, but it is necessary for a causal factor to have an impact [1]. The 'Swiss Cheese' model calls for accident investigation to look beyond active failures to examine latent failures and conditions to better understand causal and contributing factors in order to provide systems to prevent and mitigate impact from the accidents.

According to the Swiss cheese representation, in a complex system, hazards are prevented from causing losses by a series of barriers. Each barrier has unintended weaknesses, or holes which are open and close at random. When by chance all holes are aligned, the hazard reaches or accident occurs and causes harm as shown in Fig 2.1

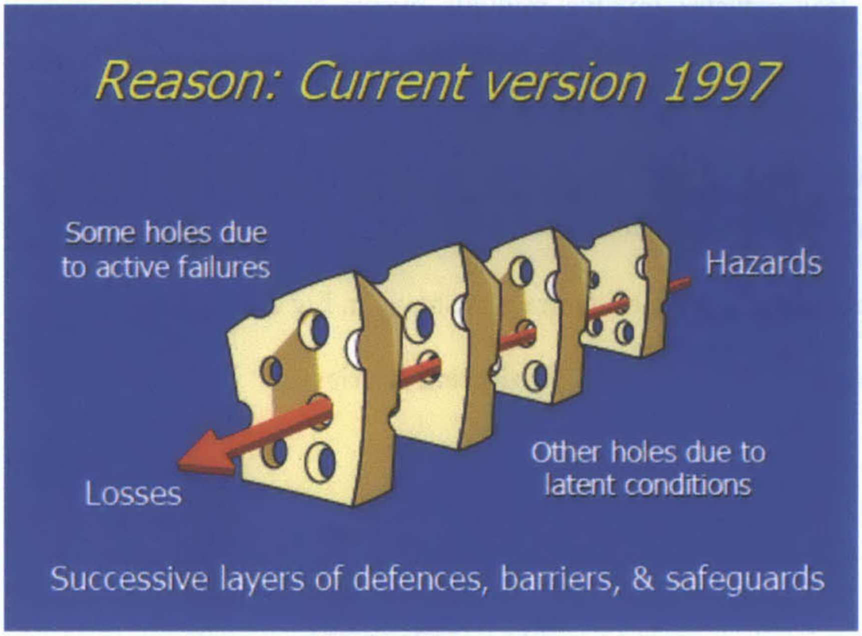

Figure 2.1 Swiss Cheese Model with layers of defenses [17]

With use over time, even the author has acknowledged this model's limitations and there was a significant change in 1997 Reason's book [17], [18]:

- The premise that any model of accident causation must have three basic elements: hazards, defenses and losses.
- The 'planes' are now represented as undisguised Swiss cheese slices and include all the many barriers, defences, safeguards and controls that any given system might possess.
- An explanation of how the holes, gaps or weaknesses arise. Short-term breaches may be created by the errors and violations of front-line operators. Longer-lasting and more dangerous gaps are created by the decisions of designers, builders, procedure writers, top-level managers and maintainers. These are now called latent conditions. A condition is not a cause, but it is necessary for a causal factor to have an impact. Oxygen is a necessary condition for fire; but its cause is a source of ignition.

Nevertheless the Swiss cheese model remains widely used and provides an application to model interactions and complexity in high consequence domains like in petrochemical industry.

Accidents in petrochemical industry involve multiple events occurring in the worst possible combination. The 'Swiss Cheese' model presents these as independent linearly treated events with low probability. Under this model, an accident would happen if all barriers fails at the same time, which imply the multiplication of these individual probabilities resulting in a very low probability for the overall risk.

One of an adoption is through a "Bow-Tie" diagram as shown in Fig 2.2.

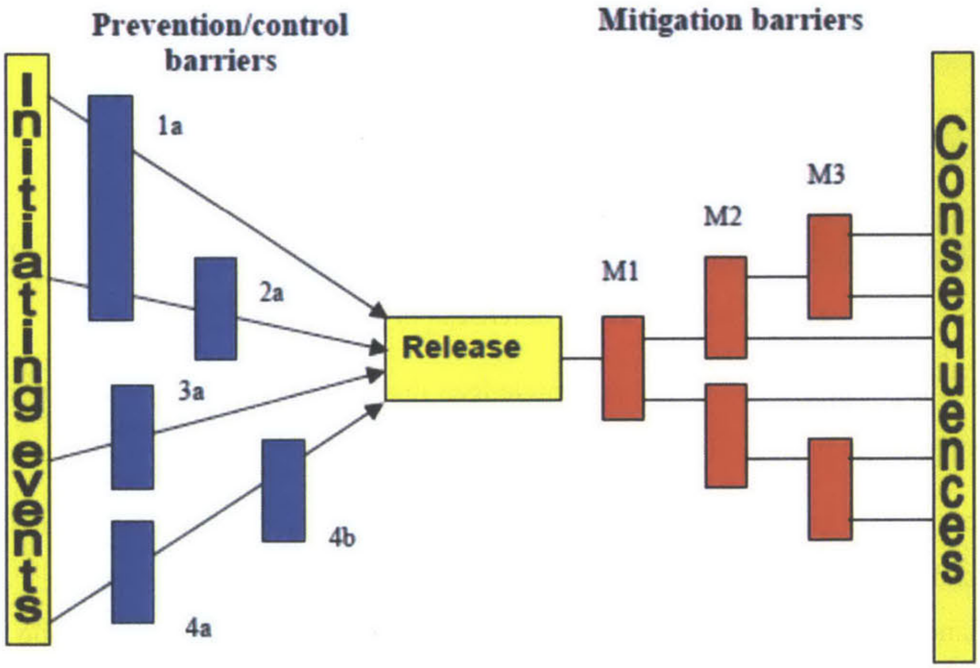

Figure 2.2 Example of Bow Tie diagram [2]

A bow-tie diagram is a representation of all the initiators and consequences of a particular scenario, together with the safety barriers that are in place to prevent, control or mitigate the event [2]. The barriers are usually referred to as lines of defense or layers of protection and hence other risk assessment method such as Layer Of Protection Analysis (LOPA) was developed to verify integrity of each barrier or safeguards. However, in reality, the events are dependent and likely related to common systemic factors that do not appear in the event chain. As such, the calculation involved in this type of assessment may not represent the real risk of the accident.

Process Safety Performance Indicator

Process safety is a framework for managing the integrity of operating system and the process handling hazardous substances. It is achieved by applying good design principles, engineering, and operating and maintenance practices [3]. For the petroleum industry, it is clear that the emphasis of process safety and asset integrity is to prevent an unplanned hydrocarbon (HC) release that could result in a major accident. In response to a number of major accidents in the industry, a significant effort from many entities have spent to develop guidelines on Key Performance Indicator (KPI) for companies to manage their process plant risk and inadvertent release of hazardous chemical. These guidelines include Healthy Safety Guide 254 - Developing process safety indicators [2], Offshore Petroleum Guide Report 456 - Recommended Practice for Key Performance Indicators. [3] and The American Petroleum Institute - Process Safety Performance Indicators for the Refining and Petrochemical Industries [19] , all of which look at how to detect integrity deterioration in each layer of the barriers in the similar view to the Swiss cheese model.

In each of these risk control systems, the leading indicator[4] identifies 'hole' or failing in vital aspects of the risk control system discovered during routine checks on the operation of a critical activity within the risk control system (e.g. Length of time plant is in production with items of safety critical plant or equipment in a failed state). Conversely, the lagging indicator[5] reveals failings or 'holes' in that barrier discovered following an incident or adverse event. The incident does not necessarily have to result in injury or environmental damage (e.g. Number of spill of chemical) and can be a near miss, precursor event or undesired outcome attributable to a failing in that risk control system [4] as shown in Figure 2.3.

---

[4] Leading indicators are a form of active monitoring focused on a few critical risk control systems in each barrier to ensure their continued effectiveness.
[5] Lagging indicators are a form of reactive monitoring requiring the reporting and investigation of specific incidents and events to discover weaknesses in that system.

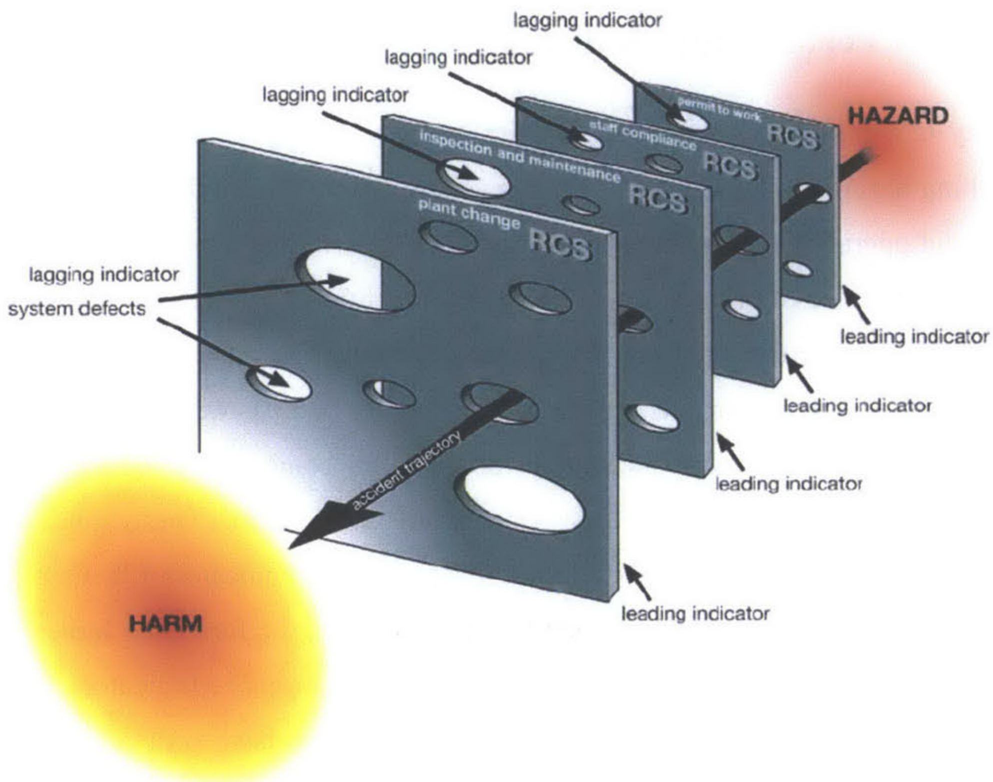

Figure 2.3 Leading and lagging indicators set to detect defects in important risk control systems [4]

System Theory and Accident

Systems approach focuses on the complete system and not the separate parts. It assumes that properties of the systems needs to be treated in its entirety, taken into account of all facets relating the social to technical aspects of the system [12]. These system properties derive from the relationships between components of the system. The foundation of system theory rests on two pairs of idea:

- Emergence and hierarchy
- Communication and control

Systems theory considers non-linear events and dynamics as well as feedback or feed-forward control. The concepts of systems theory and the implementation of systems engineering date from back to the mid-1900s. System theory considers accidents as arising from the interaction among system components in addition to component failures.

Systems theory usually does not specify single causal factor [13]. The application of system theory concept to understand the accident includes the following perspectives:

- Safety is an emergent property that arises when the system component interact within an environment.
- Emergent properties are controlled or enforced by a set of constraints.
- Accidents occur when component failures, external disturbances and/or dysfunctional interactions amongst system are not adequately controlled.

System Theoretic Accidental Model and Process (STAMP) Overview

Systems Theoretic Accident Model and Processes (STAMP) is a systemic accident model that addresses complex socio-technical systems problems [13]. STAMP treats safety as a control problem in which enforcement of system safety constraints involve physical, organizational, and/or social elements. Accident can be understood by identifying the safety constraints violated and determining why the controls were inadequate in enforcing them. This is unlike traditional accident models that address component failures and analyze accidents using the chain of events approach. STAMP allows more sophisticated analysis of failures and component failures accident [13]. For example, component failure may results from inadequate constraint from manufacturing process, engineering design or lack of correspondence between individual component including human capacity, physical degradation and so on.

By using STAMP, the higher-level control components are analyzed to determine how the lower component in the system controls might be violated. This will enable us to understand how each component is related, what is the control action and feedback comes in the form of communications with the higher levels of the hierarchy. The event of loss of containment in petroleum industry can be view as complex socio-technical system results from inadequate controls or lack of safety control enforcement. The typical control enforcement is shown in Figure 2.4.

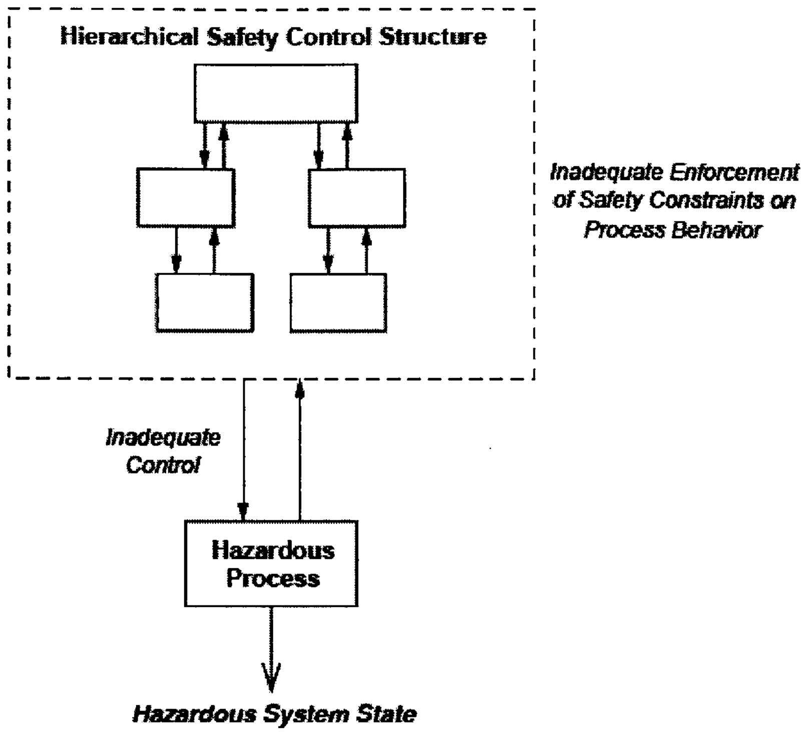

Figure 2.4 Control enforcement diagram [13]

A System Thinking Approach to Leading Indicators

There are always warning signs before a major accident occurs, but these signs or signals are often ignored or seen only as noise. There are tremendous efforts of work to identify leading indicators as mentioned in the previous section. This usually involves finding a set of general metrics or signals that presage an accident. Examples of such identified leading indicators are maintenance backlog, inspection overdue lists and minor incidents such as leaks or spills, equipment failure rates, and so on. While some general indicators may be useful, large amounts of effort over decades still fail to prevent major incidents. An alternative is to identify leading indicators or warning signs that are specific to the system being monitored [14].

Dokas, Feehan, and Imran look at the identification of early warning signs or signals that will indicate the presence of flaws and threats to a system in a timely manner. It is found that the structured identification and analysis of early warning signs is not readily available by the use of conventional hazard and risk analysis approaches [15]. Many approach on risk management were focusing on building safety into new system and mitigate potential hazard during development phase rather than attempting to safely operate an existing system. For example, the approach is capable of identifying leading safety indicators but it cannot provide those signs indicating the presences of flaws in the system during phase of operation [15]. Therefore, the STAMP Based Process Analysis (STPA) has been used to incorporate the identification of early warning signs by looking at where the inadequate control occurs that causes the violation in safety constraints of the system as shown Figure 2.6

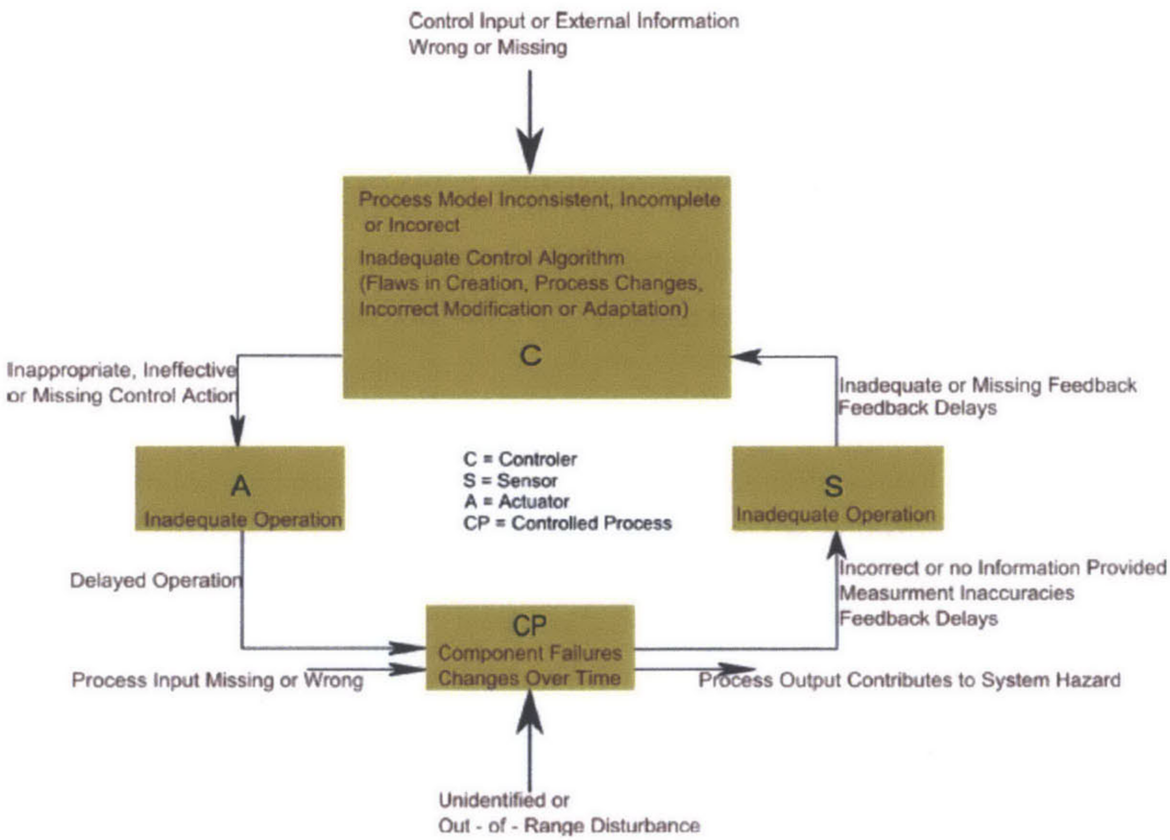

Figure 2.6 STPA guideword to identify flaws in the control process [13][15]

In order to provide a structure method for identifying warning sign, the Early Warning Sign Approach (EWaSAP) is developed with an extension from STPA model. Table 2.2 below shows the additional work of EWaSAP integrate into of STPA [21]:

STPA	EWaSAP
(1) Identify the hazard in system and top level safety constraint	Identify component/party involve in the notification loop.
(2) Create the control structure. ▪ Determine inadequate control actions ▪ Restate the inadequate control actions as safety constraints.	Identify sensory service outside of the system. ▪ Identify the signs, which indicate that the safety constraint has been violated. ▪ Find systems in the surrounding environment, which have sensors able of perceiving the signs, defined.
(3) Determine how the safety constraints determined in (2) could be violated. ▪ Create the process model for each controller ▪ Examine the parts of the process control loops to determine if they can contribute to or cause system level hazard	Enforce internal awareness actions for each flaw in the process control loop. ▪ Describe what needs to be monitored, and what type of features the sensor must have ▪ Define warning sign/ data indicating the occurrence of the flaw ▪ Update the process model of the appropriate controller(s). ▪ Define the Meta Data of the Early Warning Sign

Table 2.2 EWaSAP steps integrate into STPA

The application of STPA on to EWaSAP can be shown in the below control loop diagram in Figure 2.7.

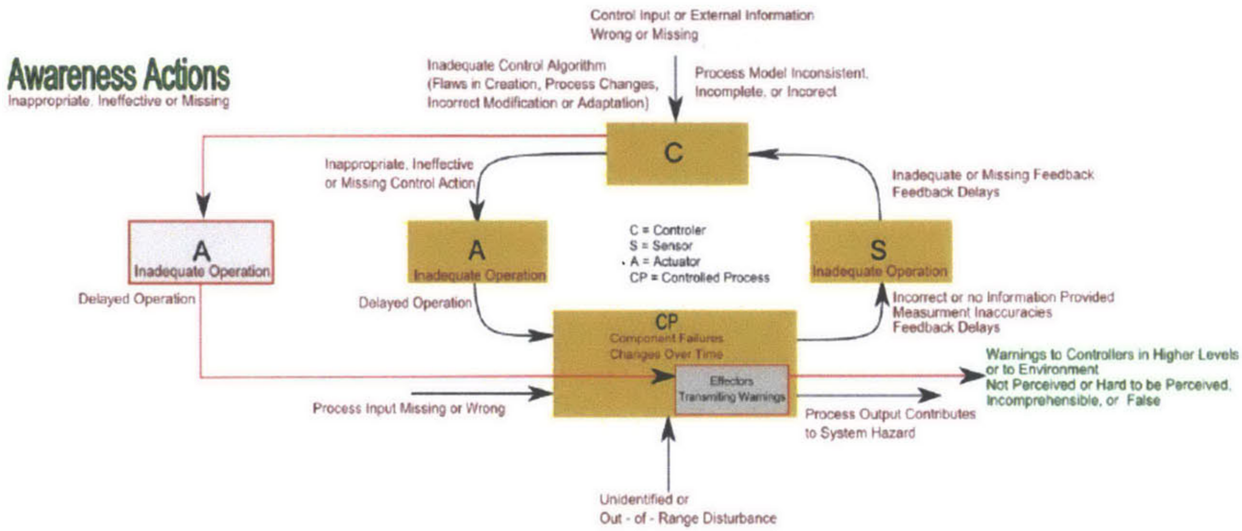

Figure 2.7 STPA control loop with EWaSAP integration [21]

While STPA aims at designing safe and resilient feedback control loops within a complex system, EWaSAP aims to enhance the awareness about the threats and vulnerabilities, which may be present in a system during its operations phase, via the systematic collection and analysis of their warning signs [15]. As result, EWaSAP is expected to help engineers to select and configure the appropriate sensors within the system and define appropriate reactive strategies into the process models of the controllers to detect the flaw under their control process, which in turn will prevent the accident.

Conclusion

The discussion of topics under this literature review highlights several important finding of the theoretical advantages of the system-based models like STAMP model (e.g., systems-based accident causality model) over the 'Swiss Cheese' approach to prevent industrial accidents. However, in order to answer the central research question of this thesis – *What could be done differently to understand the causes of accidents and prevent them?*

- an application of STAMP-CAST will be applied to a well known process accident to compare the finding results. Then STAMP-STPA will be use in an example to develop warning sign to detect the deterioration of safety integrity. These analyses are included in subsequent sections of this thesis.

Chapter 3 Case Study Incident Description and Proximate Event Chain

Background

Richmond Refinery is a 2,9000-acre petroleum refinery in Richmond, California on San Francisco Bay. It is owned and operated by Chevron Corporation (CUSA). The refinery has a capacity of approximately 240,000 barrels of crude oil per day into petroleum product such as gasoline, jet fuel, diesel fuel and lubricants. The refinery has more than 20 operating plants, where each plant consists of operating equipment units and piping connecting between them and to other plants.

Crude Unit no.4

The Crude Unit NO.4 (4CU) was put into service in 1976 to distill[6] crude oil to produce various product streams (sidecuts or SCs) as well as atmospheric overhead and vacuum residuum lines. The crude oil is heated, desalted and split into different product streams, which are then sent to intermediate storage tanks or downstream processing units as feed as shown in Figure 3.1. All crude oils processed in the Refinery pass through the 4CU, which consists of two distillation columns:

- the Atmospheric Distillation Column (C-1100) which is fed with heated crude oil
- the Vacuum Column, which is fed with the heated bottoms stream from the C-1100.

[6] Distillation separates mixture into categories of its components by heating the mixture in a distillation column where different product boils off and recovered at different temperature

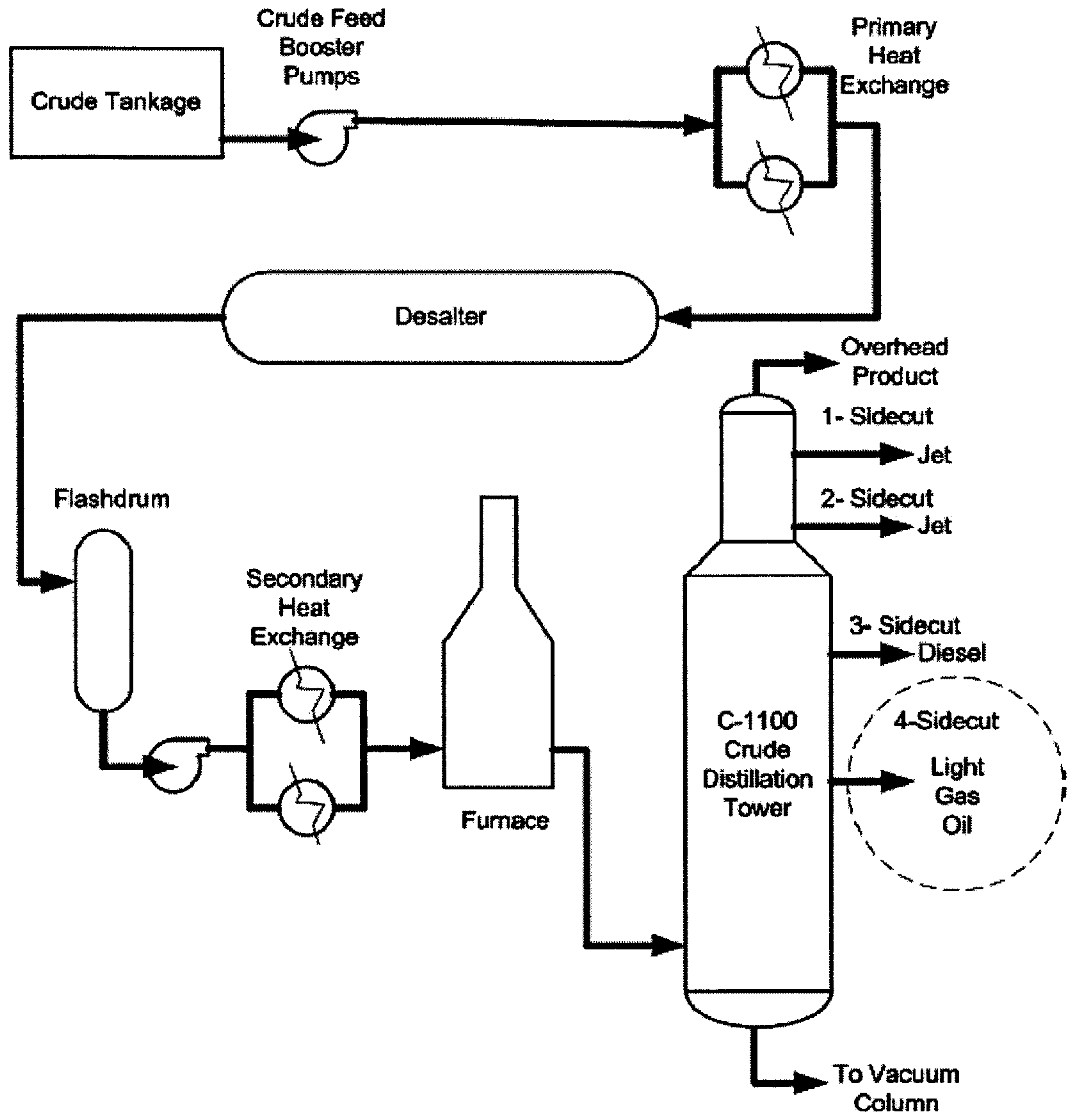

Figure 3.1 Simplified diagram showing C-1100 4CU Atmospheric Column and Upstream Process Equipment [7]

A post incident inspection showed that there were 67 components between the piping branch and the 4-SC stripper pump as shown in equipment arrangement in Figure 3.2.

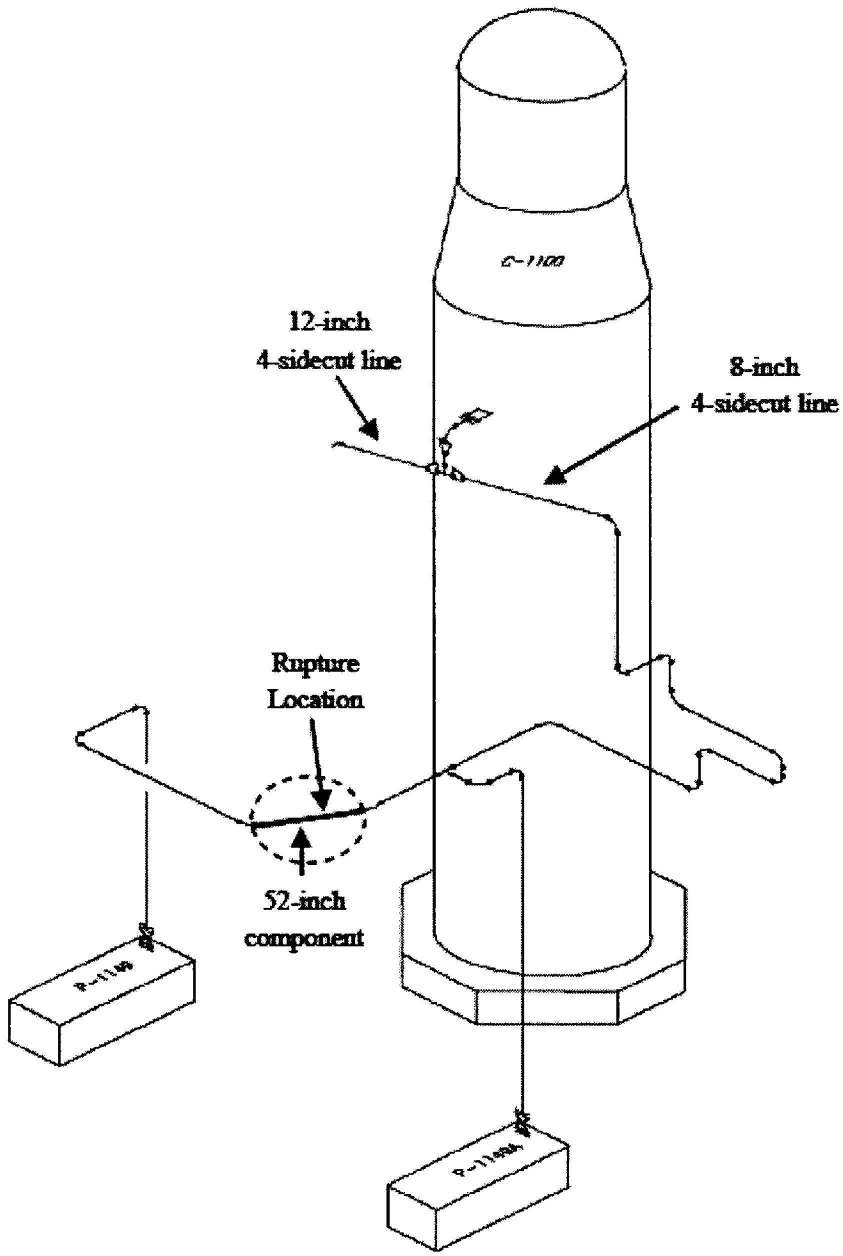

Figure 3.2 4-SC line configuration and rupture location [7]

All of the 4-SC piping was specified as carbon steel piping with schedule 40 thicknesses. Prior to 1980, when these piping were constructed, the industry followed carbon steel piping specification in ASTM 53, which did not include minimum silicon content [5].

Sulfidation Corrosion

Sulfidation corrosion is a damage mechanism that causes thinning in iron-containing materials such as steel due to the reaction between sulfur compounds and iron at temperature ranging from 450-800 degree Fahrenheit. This damage mechanism causes pipe wall to gradually thin over time. The basic fact about sulfidation corrosion in the refinery includes [7]:

- Sulfidation corrosion is common in crude oil distillation where sulfur can be found in crude feed such as hydrogen sulfide.
- Variable that affect corrosion rates include sulfur concentration in crude, flow conditions, and temperature of the system.
- Sulfidation corrosion rate is slower on stainless steel that contains high chromium percentage.
- Carbon steel experiences signification variation in corrosion rates due to variances in silicon content.
- Determining silicon content on existing carbon steel piping in field is a difficult task as 100% component inspection is required through either chemical analysis and pipe wall thickness measurement of every components.
- The thickness measurement on pipe wall is only useful if piping circuit has been exposed to sulfidation corrosion for a long enough time to detect variance in thickness and hence infer to corrosion rate.
- Chemical analysis of the steel piping to determine silicon content is the most accurate technique but it is a time consuming and costly under taking.

Proximal Event Chain

In the ten years prior to the incident, Company personnel with knowledge and understanding of sulfidation corrosion made many recommendations to reduce potential corrosion and monitor sulfidation corrosion condition of piping in the refinery as shows in Figure 3.3:

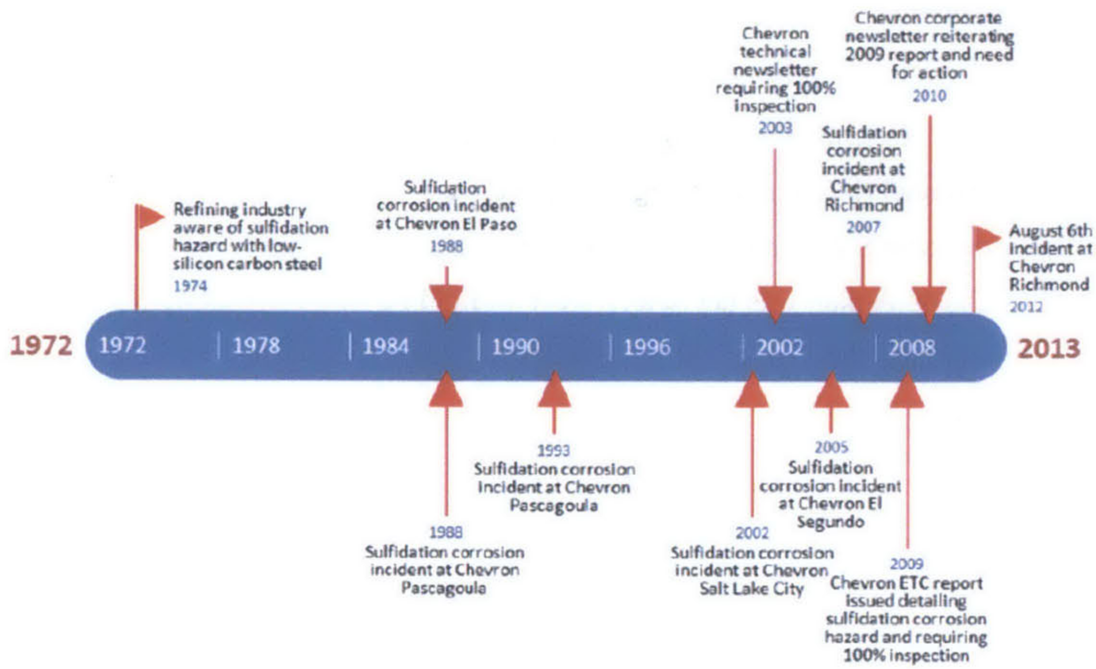

Figure 3.3 Richmond Refinery's key sulfidation event between 1974-2013 ([7], Page 24)

The accident took place on August 12, 2012 and involved a 4CU and its piping in the Refinery. A leak was discovered by an operator in an 8"diameter pipe carrying light gas oil in the 4CU. Later, the hydrocarbon release from the pipe resulted in the formation of a white could, a subsequent fire and a black plume. A shelter-in-place order was issued for cities of Richmond and nearby areas, which advised residents to remain indoors until the fire was controlled. Fire fighting teams brought fire under control and the shelter-in-place was lifted at late night. The proximal event chain is listed below [5][35]:

15.48: The refinery operator observed a leak on the 4-SC piping and notified the head operator and subsequently shift team leader went to the 4CU

16.02: The Chevron Fire Department was called and went to 4CU with two monitor trucks and engine foam fire suppression.

16.08: Fire fighting personnel performed gas testing and determined the atmosphere around leak was not flammable, based on 2% Lower Flammable Limit[7] reading.

[7] Lower Flammable Limit is the lowest concentration (percentage) of a gas or a vapor in air that capable of producing a flash of fire in presence of an ignition source (arc, flame, heat)

16.09: Control room operator began reducing oil feed to 4CU follow routine shutdown procedures.

16.20: Operation determined that the section of leaking pipe could not be isolated. Assembled personnel (inferred to be engineers, operation, fire department) concluded that the weather jacketing and piping insulation needed to be removed to allow visual assessment of leak. A plan was devised to erect scaffolding near the leaking pipe so that the insulation around the leak could be removed to determine whether an online repair was feasible.

~16.50: While the scaffolding was being erected (1 hour), a plan was developed for removing the weather jacketing and insulation from the leaking pipe, which entailed: two fire fighters using hand tools to remove jacketing and insulation from the leaking pipe.

~17.00: Operation and fire fighting personnel arriving for the night shift conducted field turnovers with the day shift.

18.10-18.21: Two fire fighters cut the bands on the piping and began to remove the weather jacketing.

18.22: A small flash fire[8] ignited when the second sheet of weather jacketing was removed. Two fire fighters quickly extinguished and two firefighters descended from the scaffolding and set up a fire monitor to provide additional firewater coverage on the leaking pipe. Fire fighter hose team briefly shut off the water to access the insulation removal, revealing an increase in volume of Hydrocarbon material from the leak. Around this time, the released material began to smoke.

18.27: The order for emergency shutdown of the 4CU was given, at which time supporting field personnel began to evacuate the area.

18.28: Refinery shift leader was informed that 4CU need emergency shutdown.

~18.29: The control room operator activated hand switches for emergency shutdown of 4CU.

[8] Flash fire is a sudden fire caused by ignition of a mixture of air and a mixture of flammable substance. It is characterized by high temperature and short duration.

~18.30: The leak was rapidly worsening. A large white cloud formed and enveloped the 4CU and downwind processing plants. Consequently, the fire fighting personnel withdrew from the area.

~18.32: The cloud ignited and black smoke plume formed

18.38: A shelter-in-place order was issued for the cities of Richmond, San Pabio, and North Richmond.

22.15: The Chevron fire department with assistance from Petrochemical Mutual Aid Organization and Municipal Mutual Aid brought the fire under control.

23.12: The shelter-in-place was lifted

In the weeks following the incident, nearby medical facilities received over 15,000 members of the public seeking treatment for ailments including breath problems, chest pain, and shortness of breath, sore throat and headache.

Chapter 4 Refinery Investigation and Findings

Following the Crude Unit No.4 fire accident at Richmond Refinery on August 6, 2012, in accordance with Contra Costa Health Service (CCHS) Hazardous Material Incident Notification Policy, Richmond Refinery (Chevron U.S.A. Inc) completed an analysis to investigate the causality of the accident [10]. This section of this thesis summarizes the findings of the Richmond Refinery incident investigation and report that Chevron submitted under 7th update to the 30-Day report for the CWS level 3 Event to CCHS [5].

4-CU Fire Incident Investigation Findings

The incident report concludes a failure occurred on a section of 8" carbon steel gas-oil pipeline from the atmospheric distillation tower (known as the 4-SC) in the crude unit resulting in a hydrocarbon leak. Subsequently, a fire erupted in the area of the failure. Consistent with the metallurgy evaluation report by Anamet [9], the investigation team conclude the five foot carbon steel component where the leak occur failed due to thinning caused by sulfidation corrosion which was accelerated by the low-silicon content. Individual carbon steel piping components with low-silicon was corroded at an accelerated rate and not readily detectable by multiple corrosion monitoring locations.

This investigation report identified four (4) main "causal factors" and that led to the crude unit fire accident. Each causal factor had related "pre-conditions" and "management/organizational issues" that contributed. Causal factors and associated contributing factors are detailed below.

Causal factor #1: The response and assessment after the discovery of the leak did not fully recognize the risk of piping rupture and the possibility of auto ignition –

The risk assessment performed was informal and under a perception of a small stable liquid leak. There was no meeting where all parties could collectively discuss the potential risk and outcome. In addition, not all-relevant information was included in the decision making process. Therefore, the following root causes were identified for this Causal factor:

- Misunderstood oral communication, No communication or untimely communication
- Standard, policies or administrative controls were confusing or incomplete or absence.

Causal factor #2: The documentation wall thickness information in Meridium limited the ability for future decision makers to utilized the data –

A measurement performed in 2002 showed one-third wall thickness loss in the failed pipe component but the data was entered as a comment. However, the Meridium[9] tool does not use information entered as text in a History Brief tab for computational, predictions or triggers. Therefore, investigation team identified the following root causes for this Causal factor:

- Standard, policies or administrative controls were confusing or incomplete
- Complex system – knowledge-base decision required
- Complex system – monitoring too many items

Causal factor #3: The Inspection during 2011 Turnaround[10] did not include every component in the 4SC piping –

The recommendations from guideline and internal analysis were not built into inspection plan for these piping circuits. In addition, no consideration of 100% component-by-component inspection was considered during 2011 Turnaround planning and hence the following root causes were identified:

- Continuing training needs improvement
- Work package/permit needs improvement
- Standard, policies or administrative controls need improvement

Causal factor #4: The 2009 Reliability Opportunity Identification (ROI) /Intensive Process Review (IPR) recommendations did not include a 100% component-by-component inspection –

---

[9] Meridium is an inspection management software tool that have a capability to store and perform calculation base on data entered

[10] Turnaround is a scheduled event wherein an entire process unit of a refinery or petrochemical plant is taken off-stream for an extended period for maintenance and/or renewal.

While documentation relate to the 2009 ROI/IPR references potential upgrade for some portions of 4-SC, it did not specify specific circuit. Although it suggested the need for additional information to evaluate potential upgrade recommendation, it did not include a recommendation for 100% component-by-component inspection. Hence, this information was not transferred to the refinery inspection management system. Investigation team identified two root causes for this Causal Factor:

- Corrective action needs improvement
- Standard, policies or administrative controls need improvement

Other Contributing Factors: The CUSA investigation report identified several contributing factors not necessarily associated with a single specific causal factor:

- The CFD did not complete a Hazard Material Data Sheet and position Engine Foam too close to the leak source when responding to the incident
- The leaking line could not be isolated on the upstream side to mitigate loss of containment.
- The ETC Sulfidation Inspection Guideline were not fully implemented and action items were not tracked to completion
- An engineer miss calculated minimum thickness for the 4SC spool piece where safety factor wasn't considered and hence this calculation results did not trigger a fitness for service analysis.
- 2012 4-SC inlet suction piping inspection results was not entered into the corrosion database (Condition Manager).
- 4 CU Process Hazard Analysis[11] (PHA) did not consider the potential for sulfidation corrosion

[11] PHA is a set of organized and systematic assessments of the potential hazard associated with an industrial plant such as HAZOP, What-if etc. A PHA is directed toward analyzing potential causes and consequences of fire, explosion, releases of toxic chemicals and major spills of hazardous chemicals. It focuses on equipment, instrumentation, utilities, human actions, and external factors that might impact the process.

Investigation Recommendations

The 4CU fire documented several recommendations, listed below, to address the mentioned causal and contributing factors as followed:

- Revise Refinery policies and checklist to ensure appropriate information including process safety and inspection information is considered when evaluating leaks and addressing the issue of whether to shutdown or continue operation of equipment.
- Enhance the Refinery's mechanical integrity program to ensure the Refinery properly identifies and monitors piping circuits for appropriate damage mechanisms using a standardized methodology and documentation system.
- Review and enhance the requirements for inspector training and competency
- Develop and implement a process for additional oversight of mechanical integrity-related recommendation from industry alerts, ETC, and other subject-matter experts.
- Inspection 4CU piping that fall under ETC sulfidation corrosion guidelines criteria prior to restarting the 4CU.
- Implement the ETC Sulfidation Inspection Guideline for remainder of the Refinery.
- Ensure relevant technical studies and inspection data are considered for the Refinery's equipment reliability plans and incorporate the recommendations into the ROI/IPR process.
- Review company/industry loss history on large fractionating tower to determine if internal Engineering Standard adequately addresses mitigation of accidental releases from these systems. Revise the standard as warranted by the findings of this review.
- Ensure Refinery business plan provide the appropriate implementation of Process Safety recommendation (such as the ETC Sulfidation Inspection Guidelines).
- Consider additional training on expectation under the "Richmond Refinery Piping Maintenance Guideline" and internal reliability management system and guidelines.

- Review and modify the PHA procedures to ensure that teams consider known corrosion threats/mechanisms.
- Consider a project to evaluate the purpose and methods of various process safety management (PSM) reviews to determine if these activities can be combined or better sequenced to improve risk understanding across the various functions and promote better process safety outcome.

Chapter 5 CAST Analysis of No. 4 Crude Unit Fire Incident

In this Section, the Chevron Richmond Refinery Crude distillation column fire incident will be used to demonstrate how unsafe control actions and causal factors resulted in this accident. The data were obtained from the CSB and Chevron investigation reports [5][7][11]. Some of this information was limited so parts of the construction of safety control structure were assumed based on inferred information from investigation reports and the knowledge of process industry in general. However, for purposes of this demonstration, the available information is sufficient.

Step 1 –System Definition and System Hazards

System Definition:

The system being analyzed is the Richmond Refinery System. For the purposes of this analysis, the Richmond Refinery System is organized into two interfacing parts:

1. External Refinery System Management – responsible for enforcement of refinery and regulatory requirements, capabilities, work process, training, and procedures.
2. Richmond Refinery System Operation – responsible for conducting operation and maintenance of refining equipment and piping within Richmond Refinery.

System Hazards:

Based on the proximal event chain, the hazardous conditions that immediately yielded the catastrophic accident were initiated when there was a leak in the piping of 4CU. Once the piping leaked, actions were executed without awareness of the risk to further damage to the piping and hence pipe rupture occurred. The gas cloud released from the rupture section was ignited and put the refinery personnel in danger. Therefore, the system level hazards associated with this accident are:

- Uncontrolled release of Hydrocarbon vapor from crude unit piping
- Exposure to public of impact from refinery uncontrolled released

Step 2 – System Safety Constraints and System Requirements

System Safety Constraints:

The system level constraints required to prevent the hazard stated previously are:

- SC1. Hydrocarbon must be under positive control[12] at all time
- SC2. Measures must be taken to minimize exposure of refinery personnel if inadvertently releases do occur.
- SC3. Measures must be provided to minimize loss to the outside community
- SC4. Measures must be taken to minimize public exposure if inadvertently fire/ explosion occur

Table 5.1 provides a summary of design constraints associate to hazard identified earlier for the Refinery system.

System Requirements:

The system requirements necessary to prevent the mentioned hazard and enable the safe execution of roles and responsibilities are:

- SR1. Operation must control process parameters within design and operating limits.
- SR2. Operation and maintenance staff must maintain equipment and piping integrity within target.
- SR3. Safety device (e.g. flare and emergency shutdown system) must be operable and maintain when potentially hydrocarbon is being processed or stored.
- SR4. Safety critical equipment and refinery emergency response procedure must be provided to reduce exposure in the event of an inadvertent hydrocarbon release.
- SR5. All areas of the plant must be accessible to emergency personnel and equipment during emergencies.
- SR6. Refinery personnel must train to:

[12] Positive control means hydrocarbon is contained within the system and only release to the surrounding in a control manner i.e. majority of hydrocarbon will be vent through flare system and equipment can be open only when there is no pressure inside.

a. Perform their job safely and understand and use protective personal equipment (PPE) and safety equipment properly.
b. Understand their roles with regards to safety and the hazard relate to their job
c. Respond appropriately in an emergency

- SR7. Those responsible for safety in Richmond City and Contra Costa County must understand potential hazards from Richmond refinery and provided with information about how to respond appropriately
- SR8. Safety equipment and City/County emergency procedures including warning device must be provided to reduce exposure in the event of inadvertently hydrocarbon release

Hazard	**Safety Design Constraint**
(1) Uncontrolled release of Hydrocarbon vapor from crude unit piping	Hydrocarbon must be under positive control at all time and measures must be taken to minimize exposure should inadvertently release occur to inside refinery and outside community Integrity of equipment and piping must be maintained and sufficient means must be provided to detect uncontrolled release and mitigate its impact to surrounding
(2) Exposure of public to impact from refinery uncontrolled released	Measures must be taken to minimize public exposure if uncontrolled vapor ss inadvertently released or fire/explosion occurs. Sufficient report must be provided between refinery and county related personnel to provide warning alarm for community.

Table 5.1 Hazards and Safety Design Constraint of Richmond Refinery System

Step 3 - Hierarchical System Safety Control Structure

The hierarchical system safety control structure for Richmond Refinery Accident is split into two control structures where brief overview of system roles, responsibilities, and interfaces are displayed. Detailed descriptions of roles and responsibilities of each element within the system are provided later in the CAST analysis.

Overview of System Hierarchical Control Structure Roles, Responsibilities, and Interfaces:

Richmond Refinery System Operation – With regard to System Operation, the Richmond Refinery Management fulfills the roles of *Refinery General Manager* overseeing all internal activities to ensure that the business is ethically[13] conducted. In these capacities, the Refinery Manager manages all of the internal capabilities such as operation, maintenance, engineering, administration and departments as well as regulatory compliance and external communities. He supports the senior leadership team to build a stronger, more transparent safety culture throughout the refinery. Moreover, the refinery supports the community and City of Richmond by looking for opportunities to work with local businesses and contractors and showing transparency through engaging local community in various activities.

[13] Chevron and its employees have a worldwide reputation for conducting business with honesty and integrity and details are listed in http://www.chevron.com/investors/corporategovernance/businessconductethics/

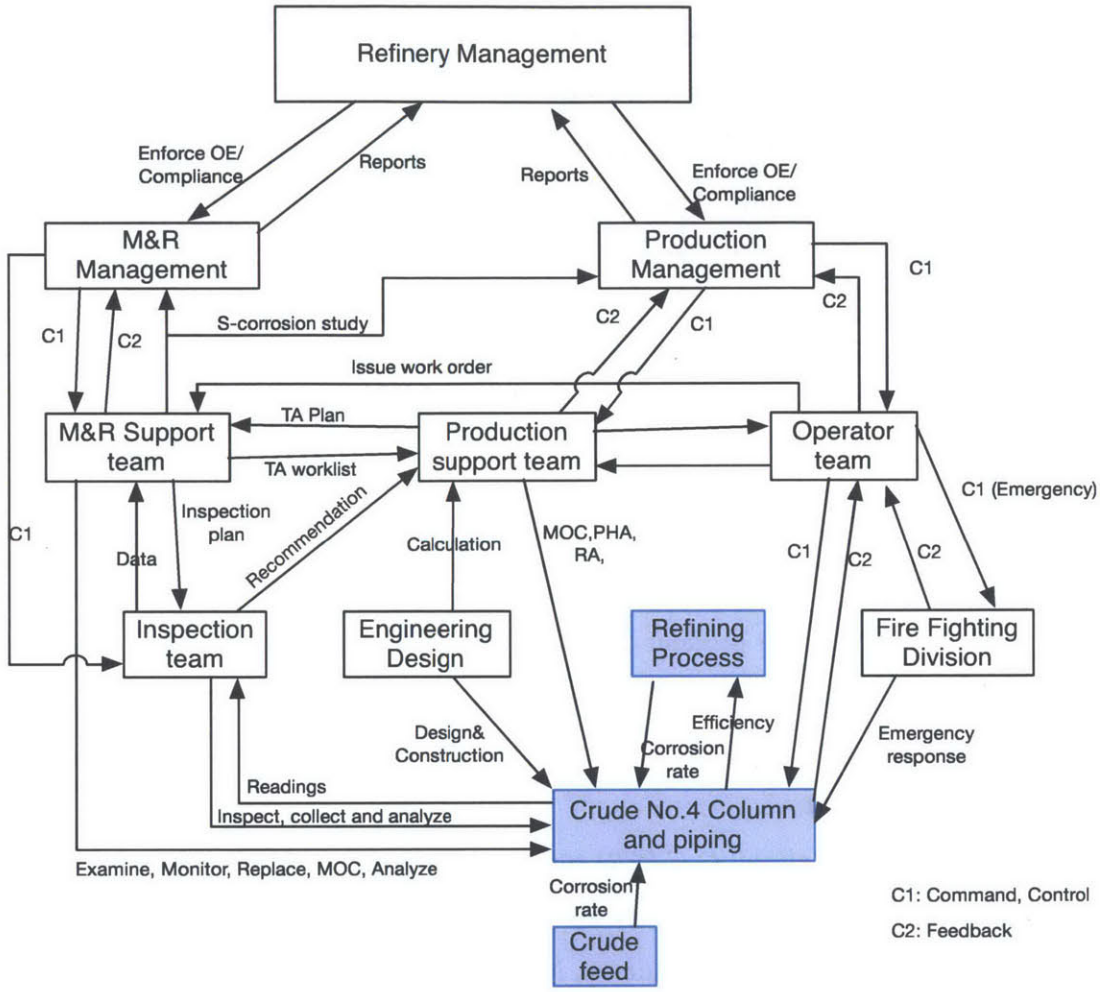

Figure 5.1 Refinery system operation control structure

Figure 5.1 shows the constructed safety control structure for Refinery system operation and below are the responsibilities of various functions under refinery operation management:

- *Operation management* is responsible for ensuring all 30 plants meeting production-planning target. Operation management enforces Operational Excellence management system[14], which is utilized by operator and production support teams.

[14] Systems that support a culture of safety and environmental stewardship that strives to achieve world-class performance and prevent all incidents.
http://www.chevron.com/about/operationalexcellence/

- *Production support team* mainly consists of plant engineers and/or supervisor who are involved in the day-to-day running of each plant. Production support team is responsible for ensuring production run smoothly by working with engineering, operator and maintenance teams. They provide technical expertise in troubleshooting the unit. They are also involved in decision-making, change management, planning turnaround and project works.
- *Operator team* consists of head operators, control room operators and field operators. They are the area owner of each plant, which they monitor and take actions, to ensure the units run continuously to deliver product and meeting specification requirements. They also provide operational feedback to various parties.
- *Maintenance & Reliability (M&R) management* is responsible for optimizing the plants' availability for production. Their subordinates include inspectors and the Maintenance & Reliability (M&R) support team. Maintenance management enforces Operational Excellence management system, which has the reliability as its key component.
- *Maintenance & Reliability (M&R) support team* consists of reliability, material and maintenance engineers. They are responsible for preventative maintenance and repair in the case of breakdown. M&R support team utilizes collected information of equipment to analyze and take actions to ensure equipment are fitted for service. The risk relates to compromising mechanical integrity is usually reviewed by engineering; production and reliability personnel to assign priorities and develop work plan to address them.
- *Inspector* collects and manages the equipment and piping inspection data. He is responsible for ensuring equipment and repairs meet engineering code and standards and statutory requirements. This is performed through providing recommendation to operation and M&R team and maintaining his expertise in damage mechanisms associated with processing unit.
- *Fire Fighting Division* is a department onsite within the Refinery, which includes state-certified fire fighters and emergency medical technicians. They maintain their competency in petroleum firefighting and emergency responses. They are

responsible for keeping site fire fighting equipment in good conditions and prepare to respond to site situation as defined in the Refinery emergency response plan. In addition, the Refinery maintains regular contact with state and local agencies and work with them to conduct large-scale emergency drills. Frequent drills are held in conjunction with local fire departments.

- *Engineering design* team designs the unit operation according to engineering codes and standards in the design phase. They are responsible for the design, installation and commission unit operations as well as providing additional engineering service to production team for capital project or on going operation upon requested.

External refinery system management – With regard to management system outside, the Richmond Refinery Management interacts with many parties as shown in Figure 5.2. The main interaction of the Refinery operation is with Chevron corporate management to strategically align with the business direction as well as various codes of conducts, procedures and work processes. Other components under social system operation includes:

- *Environmental Protection Agency (EPA)* has a main responsibility to ensure that environment is protected. This is performed through environmental licensing, enforcement of environmental law, environmental monitoring, analyzing, reporting and regulating, as well as waste management. Protecting the environment is a shared responsibility between government, industry, public and local communities.
- Occupational Safety and Health Administration (OSHA)/*Cal OSHA* has a responsibility to assure safe and healthful working conditions for workers. This is performed through setting and enforcing standards as well as providing training, outreach, education and assistance. OSHA enforces safety and health standards. An employer like Chevron Richmond Refinery has to comply with these standards and take appropriate actions to correct hazardous working conditions. OSHA body works with state or local compliance regulators to perform on-site inspections if there is a complaint or significant incident.

- *Chevron Energy Technology Company (ETC)* works in teams to develop technology products and technical services in reservoir management, earth science, drilling, production engineering, and facilities engineering. ETC follows the best practice, industrial codes and standard updates to revise Chevron's engineering codes and standards. In addition, ETC provides technical consultancy services to operating business unit upon request. They also design work process and guidelines to improve performance in areas related to facility operations.
- *Chevron Corporation (Chevron USA Inc.)* provides vision, values, and strategic plans to all subsidiary business units to support their business operation. This includes exploration, production and transporting crude oil and natural gas, refining, marketing and distributing transportation fuels and lubricants. Corporate is responsible for expanding management systems that support a culture of safety and environmental stewardship and strives to achieve world-class performance. Corporate believes in "zero accident is attainable" mission by providing policies, processes, tools and behavioral expectations to assist employees.
- *Contra Costa County (CCC), Richmond City (RC) and Contra Costa Health Service's Hazard Material Program (CCHMP)* are dedicated to providing public services, which improve the safety, health and prosperity of their residents and the economic viability of local businesses. Local officers work with industry to ensure compliance with state and federal regulatory laws and standards. In addition, they also provide services for the community including emergency preparedness.
- *Code and standards agencies* responsible for developing standards and codes to meet with change in technologies and product requirements. Companies and manufacturers are members of these agencies that utilize available standards or recommended practice and provide technical feedback for standards and code developments. An example of agency is American Petroleum Institute (API) who peaks for the oil and natural gas industry to the public, Congress and the Executive Branch, state governments and the media. In addition, API negotiates with regulatory agencies, represents the industry in legal proceedings, participates

in coalitions and works in partnership with other associations to achieve our members' public policy goals.

- *Bay Area Air Quality Management District (BAAQMD)* is the public agency entrusted with regulating stationary sources of air pollution in the nine counties that surround San Francisco Bay: Alameda, Contra Costa, Marin, Napa, San Francisco, San Mateo, Santa Clara, southwestern Solano, and southern Sonoma counties.

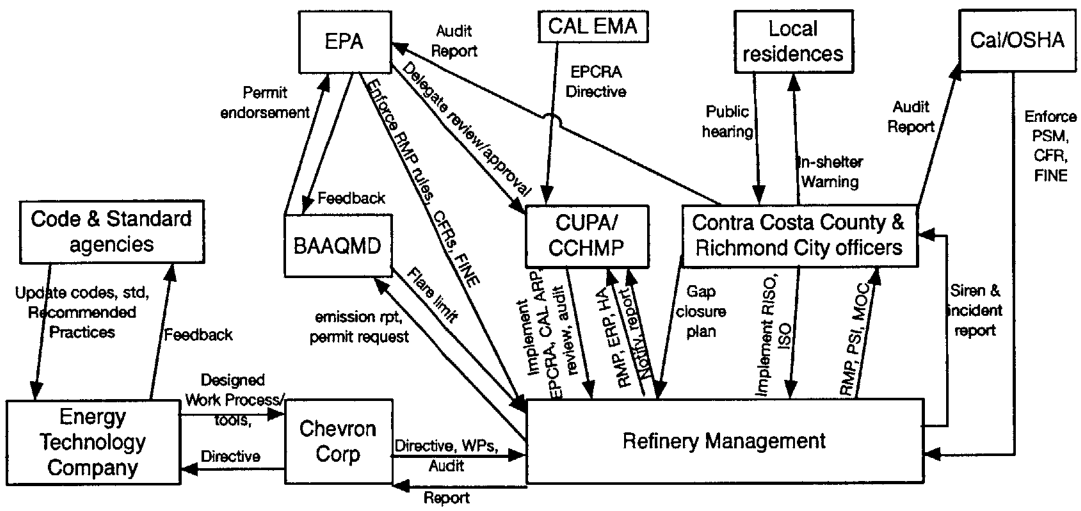

Figure 5.2 External refinery system management control structure

Refinery System Operations and External Refinery System Management Interactions –

As shown by the red arrows in Figure 5.3 there are eight major linkages across the two systems. Each are briefly described below:

- <u>Codes and standard agencies and Engineering Design</u>– From a social system perspective, agencies continually develop and update petroleum codes and standards that direct the design, development, and the procurement of material and equipment to improve product qualities and meeting operational requirements. From a system operation perspective, engineering design and development team utilizes piping codes and standards to design, verify and construct piping system for a crude distillation unit.

- ETC and Refinery operation (functions under Production and Maintenance) – ETC continually updates company codes, standards and publishes them to all operational business units across Chevron subsidiaries. Sometimes ETC establishes a special recommendation report to a group of business units on specific issue; especially after an incident at one location and provides consultancy services to all operating business units upon request. From system operation perspective, once each operating business unit receives a recommendation report, a business unit needs to conduct gap analysis and prioritize appropriate actions.
- Chevron Corporation and Refinery operation (functions under Production and Maintenance as well as physical equipment) – from external refinery management system perspective, Corporation] conducts audit on their subsidiary operating facilities to check for their efficiency in policies, procedurals or work process implementation. Refinery system operation will prioritize pending actions and take appropriate steps to close those gaps.
- CCC and Refinery operation – from external refinery management system perspective CCC works with operation management to conduct audits to verify compliance of federal and state regulatory requirements. In addition, CCC also receives notification from refinery operation management upon incident occurrence at the refinery. In these cases, CCC sends out community warning signals, including siren, strobe lights, telephone, to protect community's population.

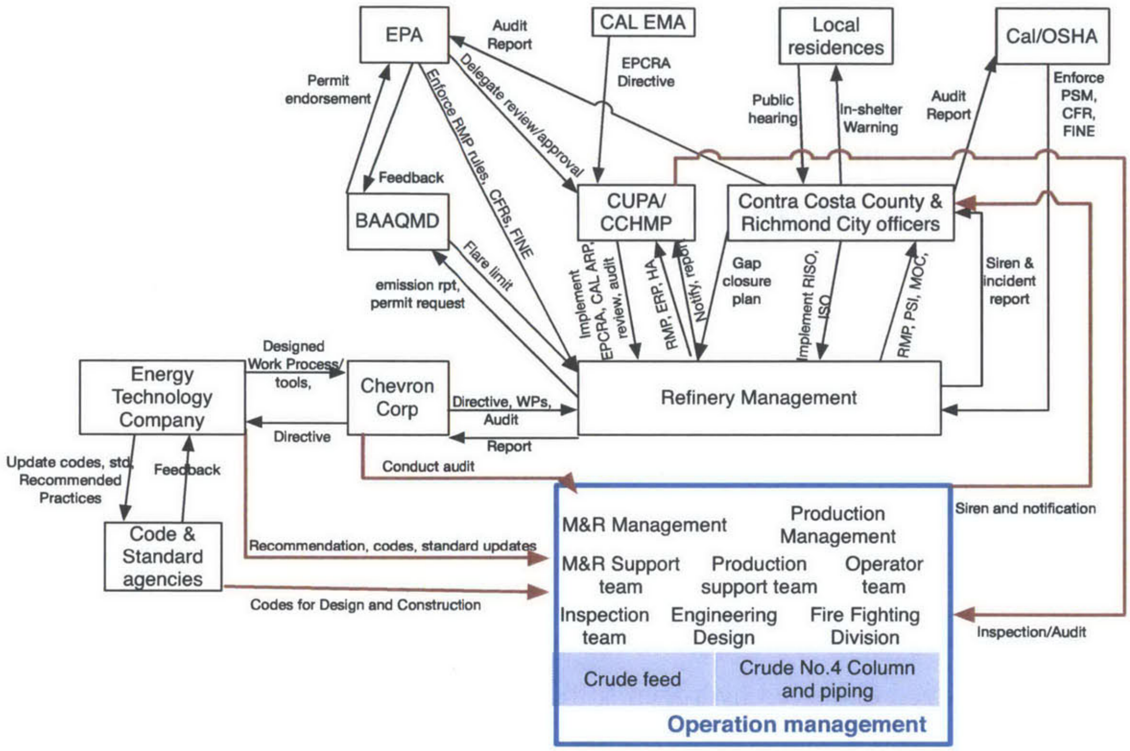

Figure 5.3 Linkage between Refinery system operation and External Refinery Management

Step 4 – Proximal Event Chain

The proximal event chain is contained in Chapter 3 of this thesis and is based on "the Refinery 4 Crude Unit Incident August 6, 2012 Report" on 4 Crude Unit leak and Fire provided by Chevron [5].

Step 5 – Analysis of Physical Process

Physical System (Distillation column, piping, refining process, crude feed) Safety Controls:

In this part of CAST, the physical system Crude No.4 distillation column sidecut no.4 (4-SC) piping, refining process and the crude oil feed are analyzed to identify physical failures, dysfunctional interactions and communication, or unhandled external disturbances that caused the adverse events. The goal is to determine why the physical controls in place during the time of the accident were ineffective in preventing the hazard. Figure 5.4 provides a summary of the safety requirements and constraints violated within the physical process, the emergency and safety equipment available to the refinery personnel, the physical failures and inadequate controls, and the physical contextual factors. Analysis of these actions results in the identification of the following control/feedback inadequacies at the physical system level:

Inadequate control/feedback – Material of construction was not designed to tolerate to higher crude sulfur content

The original design of this crude column was equipped with a sulfur removal unit that effectively removed dissolved hydrogen sulfide[15] from the 4CU. The sulfur removal unit allowed the 4-sidecut equipment and piping to be constructed of carbon steel. However, after 15 years of service, the sulfur removal unit was taken out of service without MOC or indicating in the documental record. The review to identify controls for mitigation of sulfidation corrosion post removal of this unit was thus not conducted, the vulnerability of sulfidation corrosion attack on the 4-SC piping increased.

Inadequate feedback – Did not provide means to detect sulfidation corrosion across all unit sections

There are sixty-seven (67) pieces of piping components assembled between Crude column and crude pumps [5]. However, piping components within a single circuit route consist of elbows, fittings, and straight pipe runs. Each component type contains different percentages of silicon concentration and hence, a large variation in sulfidation corrosion rates. In addition, there are only 19 permanent Condition Monitoring Locations (CMLs) or corrosion probes along the 4-SC piping. These CMLs are located on elbow components, which have relatively higher silicon content and hence did not show a high corrosion rate. In 2002, one part of this piping assembly--a 52-inch straight run piping

[15] Hydrogen sulfide is the most aggressive sulfur compound associate with sulfidation corrosion

component--was identified to have accelerated corrosion rate but no CML was added to ensure future monitoring and this component was not inspected again. Therefore, the refinery personnel relied on primarily inspection data from high silicon-containing components that did not reflect the high corrosion rate of the lower silicon-containing components of the 4-SC piping.

Inadequate control/ feedback – not designed for high corrosion rate from change in feed composition (higher Sulfur content %) and/or higher operating temperature

Crude oil feedstock used at the Richmond refinery is obtained from a variety of different sources[16]. In case of the Richmond refinery, the material of construction for 4-SC piping is carbon steel, which will not yield the original design life of the equipment when exposed to sour crude feed concentration and/or higher operating temperature. Although MOC process is used when the refinery introduces a new crude to evaluate the potential impact on the refinery, the MOC review considered general operational issues but did not analyze corrosion effects from sulfidation corrosion associated with increased sulfur content in the crude feed [7]. This might be because the MOC process relies on multidiscipline experienced reviewers to analyze impact from the propose scope of change. Therefore, if inaccurate or missing information reaches each reviewer, he or she could overlook or miss identifying impact of sulfidation corrosion and hence did not identify corrosion mitigation plan.

Inadequate control – can not be isolated from main 4CU

The 4CU was not designed with an isolation valve on 4-SC piping so inspection and isolation of this section can only be performed during 4CU and 4CU pumps shutdown. Although 4-SC contains relatively low hydrocarbon risk, combustible liquid similar to diesel, 4-CU contains a large inventory of multiple hydrocarbon components in the column. Hence the inability to isolate leak section imposes a risk to the refinery during

[16] These various crudes have different composition such as varying sulfur compounds and concentrations hence therefore different corrosion effects on process equipment and piping. There has been an increasing trend for refinery to process less expensive crudes which may contain high sulfur, naphthenic acid or very heavy hydrocarbon contents that a refinery may not have been originally designed to process.

process shutdown. As such 4-SC, did not provide adequate control for use by the emergency response team to mitigate pipe leak, rupture and escalation.

<u>Inadequate Control / Feedback - Process instruments were not able to detect process leakage and commence automatic shutdown during initial rupture</u>

There was no evidence of automatic action from low pressure or fire and gas shutdown system mentioned in any investigation reports. It is understandable that in general the pinhole pipe leakage goes undetected by the process instrument or gas detector and no automatic action taken. However, an automatic shutdown action should have been provided when flash fire occurs, as an alternative means to an operator initiated action.

Figure 5.4 is the summary of critical control/feedback inadequacies in the refinery physical system that must be addressed to remove hazards in the current control structure

Distillation column and 4SC

Safety Requirement & Constraints Violated:

- To protect against sulfidation corrosion
- To protect against inadvertent release of flammable hydrocarbon and explosion
- To provide operational flexibility with various crude feed concentration
- Isolate leak location to minimize potential uncontrolled release
- Provide means to shutdown and dispose associated hydrocarbon safely
- To provide sufficient safety factor to meet design life

Emergency and Safety Equipment (Controls):

- Level and Pressure alarm
- Liquid containment system
- Emergency shutdown system
- Flare system
- Fire detection
- Surveillance camera
- Fire water / fire fighting
- Refinery alarm system
- Emergency response system
- PPE
- Wind socks

Failure and inadequate controls:

- Material of construction was not design to tolerate to higher crude sulfur content
- Did not provide means to detect sulfidation corrosion across all unit sections
- Not designed for high corrosion rate from change in feed composition (higher Sulfur content %) and/or higher operating temperature
- Can not be isolated from main 4C
- Process instruments were not able to detect process leakage and commenced automatic shutdown during initial rupture

Physical contextual factors:

- Silicon content on piping and fitting are not uniformed from 1970+ manufacturers
- A lot of piping components, 4600+ components, in the refinery under are subject to corrosion and monitoring
- Small leak is undetectable from process parameter monitoring
- Unable to see piping condition due to presence of insulation and location of leak point.
- Presence of hot surface around distillation column
- Distillation column contains multiple components with different physical properties
- Large isolation boundary due to design practicality

Figure 5.4 Physical plant level analysis

Step 6 - Analyzing the Higher Levels of the Safety Control Structure

After the completion of the analysis of the physical plant equipment and identification of physical control inadequacies, the next step is to examine the higher levels of the hierarchical safety control structure in order to understand why those physical control inadequacies occurred. In order to perform this, this section of the thesis report analyzes each relevant component of the safety control structure, starting with the lowest physical controls and working upward to the higher level in refinery management and societal elements. By proceeding with the analysis, we will be able to develop an understanding of the reasons for the physical system inadequacies and why each component at the lower levels acted in the way they did.

The analysis will start at refinery system operation level, which is composed of working teams under supervision of maintenance and operations managements, refer to Figure 5.1.

Team of operators

Per the Safety Control Structure (Figure 5.1), the operators controlled the refining process by commanding and controlling via automation control system as well as taking actions in the field. The operators received feedback from the 4CU plant via various sensors/gauges and visual screen/auditory observation. During emergencies, they coordinated the emergency response with the firefighting team by using walkie-talkies.

Figure 5.5 summarizes the operators' safety related responsibilities, operational context, unsafe decisions and control actions, and process model flaws. As operators are the area owner of the 4CU plant, this is one of the components in the safety control structure with the most direct/proximate safety-related responsibilities during an emergency. Some of these key responsibilities include detecting unsafe operating conditions and preventing an escalation by shutdown of the crude unit. As listed in Figure 5.5, the operators took several unsafe control actions. Analysis of these actions identifies the following control/feedback inadequacies at the operator team level:

<u>Control/Feedback Inadequacies</u>

<u>Inadequate Control – Agreed to investigate the leak source on a non-isolated 4SC pipe during a normal crude column shutdown step</u>

Operators were aware that a safe investigation could not be performed unless the 4CU was completely shutdown and hence initiated the 4CU to be shutdown. However, the head of operator did not think the 4-SC liquid hydrocarbon leak was serious enough to warrant an emergency shutdown to stop production and hence allowed a leak investigation to occur in concurrent to the normal 4CU shutdown that was slowly taking place. This might be because they perceived it as a relatively low risk to handle the dripping 4SC liquid a hydrocarbon, which is a combustible liquid.

<u>Inadequate Control - Delayed to emergency shutdown of 4CU after initial flash fire</u>

Operators did not utilize an emergency shutdown function after the first two and half hours of leak discovery and even after an initial flash fire occurred. From chevron investigation report [5], it can be inferred that control room operator had to wait for shutdown command/approval from head operator at the scene as well as refinery shift leader. Therefore, the little time delay to activate a shutdown hand switch of seven minutes from initial flash fire. The inadequate control action from operators may occur from the combination of reasons such as difficult scene situation assessment, production pressure, unclear communication between emergency response team and did not want to cause a big flaring.

Inadequate Feedback - Delayed to encourage refinery personnel to move away from scene

Operators, as well as other teams onsite, did not anticipate the risk of pipe rupture and allowed 19 refinery personnel, including the emergency response team and non-essential personnel in the vicinity of the incident. These personnel evacuated from the scene five minutes after initial flash fire only when pipe rupture occurred.

Safety related responsibility

- Follow emergency response procedure
- Run the process within design limits
- Detect abnormal conditions and bring about the process safe condition
- Ensure all works in the 4CU area have undergone relevant safety reviews and execute resulting actions

Context

- Shift change: planning and executing teams were on different shifts
- Pressure under emergency condition
- Executing (On scene) team were not familiar with process equipment, nor were they aware of the risk of different forms of hydrocarbons.
- Leakage area contained combustible liquids similar to diesel (low flammability liquid)
- Slow crude unit shutdown under normal situation due to high temperature operating condition and complexity.
- Fine from flaring over the limit
- Bad perceptions from community on pollution and flaring
- Crude unit contained multi component hydrocarbons in the isolatable section.
- To minimize production disruption
- Refinery establishes an emergency response procedure

Unsafe Decision & control action

- Agreed to investigate the leak source on a non-isolated 4SC pipe during normal crude column shutdown step
- Delayed to emergency shutdown of the 4CU after initial flash fire
- Delayed to encourage refinery personnel to move away from scene

Process model flaw

- Believed that emergency response team would be able to bring process under control
- Believed that a leak section contains only combustible liquid similar to Diesel; not accounting for connections to other sections that contained gas and more volatile hydrocarbon.

Figure 5.5 – Operator level analysis

Fire fighting division

Per the Safety Control Structure (Figure 5.1), Fire fighting division provided control over crude unit by executing command and control in the form of leak intervention and oral communications. The fire division received feedback from 4CU via visual observation and auditory communications with the control room via walkie-talkies.

Figure 5.6 summarizes the fire division safety related responsibilities, operational context, unsafe decisions and control actions, and process model flaws. The fire fighter dealt directly with the leaking piping, which was the most direct/proximate safety-related responsibilities during emergency. Some of these key responsibilities include bringing unsafe condition back to normal the operating conditions. As listed in Figure 5.6, the fire fighters took some unsafe control actions. Analysis of these actions identifies the following control/feedback inadequacies at the fire fighting level:

<u>Control/Feedback Inadequacies</u>

<u>Inadequate control/feedback – Did not safely remove insulation, which resulted in pipe rupture</u>

Fire fighters used multiple methods to remove pipe insulation including pipe pike, hook and high pressure water jet which exerted forces on leak pipe as concluded in Anamet report [9]. They relied mainly on visual inspection to measure the degree of leakage from the 4-SC pipe. Although they previously used gas detectors to monitor the air in the area, it was not clear whether fire fighters used gas detectors to measure the flammability at the leak source or whether any other further action was taken.

<u>Inadequate control/feedback – Did not anticipate the risk of a gas leak and ignition or inadequate communication with the previous shift</u>

Fire fighters aware of potential flash fire resulting from exposing oil-soaked insulation to air and hence wore full PPE. However, CSB found that some fire fighters misunderstood the risk of dealing with 4-SC piping hydrocarbon content. They understood 4-SC hydrocarbon was at its flash point, that will ignite if there is an open flame, rater than at self-ignition temperature. However, the evening shift fire-fighting crews were mostly not involved in risk assessment and planning and hence there might be a gap in communication between shift changes.

Safety related responsibility

- Response to emergency to protect people and bring refinery to a safe state
- Follow Emergency procedure / Hazard check list
- Coordinate with operation and communicate effectively with associate parties
- Inspect fire-related equipment ready for use
- Authorize safe work permits for hot work and confined space entry, security, and a variety of other tasks related to fire prevention and emergency response
- Ensure that the ERP is implemented and followed in the preparation for and response to plant emergencies

Context

- Poor visibility and misty after applying fire water
- Shift change – different execution team
- Leak location is not accessible without scaffolding
- Insulation is firmly wrapped on pipe with strings
- Comprised of both full-time employees and trained employee volunteers
- Chevron Fire Department trains its personnel to handle any emergency that might occur including fires in process plants, building fires, storage tank fires, wild land fires, or fires related to transportation modes, including ships, barges, tank cars, and rail cars.
- Fire department personnel are trained in confined space, high angle, and heavy rescue procedures.
- All of the full-time members are certified Hazardous Material Technicians
- Volunteers consisting of employees from the Operations, Maintenance, and Technical Divisions. Each volunteer receives approximately 100 hours of training each year

Unsafe Decision & control action

- Did not safely remove insulation, which resulted in pipe rupture
- Did not anticipate risk of gas leaked and ignition or inadequate communication with the previous shift

Process model flaw

- Knowledge about Auto Ignition Temperature / Flash point
- Distillation and piping hydrocarbon content mixture led to wrong risk assessment

Figure 5.6 –Fire fighter level analysis

Operation support team

Per the Safety Control Structure Figure 5.1, operations support team controlled the refinery process by managing physical change to process equipment and piping via Process Hazard Analysis (PHA) and Management of Change (MOC) tools. The production support team received feedback by monitoring of automated control system and from operations team. Additionally, the operations support team worked with engineering and reliability team to ensure refinery process ran smoothly. The operations support team gathered data and technical information to make decisions and prioritizations and the work lists. In addition, they provided input to risk assessment and support operator to make appropriate decision and actions during emergencies.

Figure 5.7 summarizes the operations support team's safety related responsibilities, operational context, unsafe decisions and control actions, and process model flaws. As the operation support team involved in many changes of the crude distillation unit, this is an important component of the safety control structure with the proximate safety-related responsibilities during normal operation and turnaround. As listed in Figure 5.7, the operator support team took several unsafe control actions. Analysis of these actions identifies the following control/feedback inadequacies at the operation support team level:

<u>Control/Feedback Inadequacies</u>

<u>In adequate control – Did not provide sufficient input during leak investigation planning</u>

Production support team has technical process knowledge as well as understanding Chevron safe work practices such as isolation requirements. However, it was not mentioned whether the production support team was involved in any risk assessment that resulted in lived piping investigation in the presence of 19 plant personnel. It was not clear whether production support team viewed clamp[17] repairing work as a normal practice within the refinery or not.

[17] Clamp repair method - The simplest form of repair component is a metallic patch, which may be applied to cover a small, non-leaking defect. The repair involves the welding, by fillet welding to the pipe, of a suitably curved patch. [22]

Inadequate control/ feedback – Did not provide sufficient hazard reviews and change management associated with new operating condition and feed introduction

It can be inferred that a unit engineer plant, likely to be production support team, was responsible for managing the MOCs for change in crude feed and operating conditions. However, from CSB investigation [7], the managed MOCs only considered general operational issues but did not analyze corrosion effects from the increased in sulfur composition in crude feed. Hence, the production support team did not provide an update temperature and sulfur concentration to the inspector or reliability team to update their corrosion rate. Therefore, the inspector and reliability engineer had not used new corrosion rates to estimate the piping life and did not reduce the relevance of past inspection data when predicting future corrosion rates.

Inadequate control – Contributed to the 4-SC pipe replacement work scope reduction during the Turnaround Planning Process

If M&R team and inspectors provided too many work scopes during turnaround planning that imposes bottleneck in work sequencing or time constraint, turnaround work prioritization would occur. It seemed that production support team opposed to whole 4-SC pipe replacement scope that reliability engineer suggested because of limited corrosion data points available. Despite the fact that engineers made an engineering assumption on the uniformity of corrosion, they agreed that discharge piping exposed to a higher operating pressure and hence was more likely to fail.

Inadequate control - Rejected chrome pipe replacement plan on 4-sidcut during 2011 turnaround planning cycle

Based on the CSB investigation report turnaround core team, consists of production support team, inspectors and reliability engineers, rejected the 4-SC line replacement plan in 2011 turnaround due to lack of support data to confirm degree of severity of corrosion condition on 4-SC line.

Safety related responsibility

- Provide engineering support to relate safety analysis during the design and operation
- Follow Operational Excellence and Tenet of operation regimes
- Follow Emergency response procedure
- Plan Turnaround work list subject to improve reliability of equipment
- Ensure each change to process equipment and piping is reviewed comprehensively and execute correctly.

Context

- Refinery introduces new crude from various sources with different sulfur contents over operating lifetime.
- Refinery has been in operation for more than 40 years hence there are a lot of maintenance and repairing activity on going.
- There were many expansions, modifications on refinery equipment and piping from the past, which means a lot of projects, analysis and documentation.
- A lot of interfaces and interaction with all working groups such as operators, planning, reliability as well as upstream and downstream plant support teams.
- Corporate provides subsidiary companies with many work processes (MOC, PHA, RBI etc.) and documentation which imposes workload and time constraint to complete the process
- Refinery turnaround work planning is very intensive and interactive due to the scope and involvement of associate physical equipment.
- Management of Change work processes might not be strictly implemented in early refinery years
- The production team is subject to productivity, capital budgets and other goals imposed upon them
- Turnaround is very schedule driven and time constraining in nature

Unsafe Decision & control action

- Did not provide sufficient input during leak investigation planning
- Did not provide sufficient hazard review and change management associated with new operating condition, feed introduction
- Contributed to 4-SC pipe replacement work scope reduction during Turnaround planning process (2006)
- Rejected chrome pipe replacement plan on 4-sidcut during 2011 turnaround planning cycle

Process model flaw

- Engineer tends to make decision base on inspection data available without noticing bias or flaw
- Level of knowledge and understanding of Sulfidation corrosion varies between engineers
- 4-sidecut upstream and downstream piping experiences same level of corrosion (same operating temperature and composition) but put emphasis higher operating

Figure 5.7 – Operation support team level analysis

Maintenance & Reliability (M&R) support team

Assumption: M&R engineers owned the MOC scope for 4-sidecut piping replacement
Material engineer is part of M&R team

Per the Safety Control Structure (Figure 5.1), the M&R support team controlled the integrity of refinery equipment by driving preventive and corrective maintenance programs, replacing equipment and piping and providing input to other teams during PHA and MOC reviews. The M&R support team receives feedback from inspectors as well as fieldwork requests from the operator team. Additionally, M&R support team works with the engineering and production support teams to improve equipment reliability via the Risk Base Inspection (RBI) work process. M&R team gathers data from the Meridian database system as well as technical information to make decisions and prioritize the work lists. During emergency situations, the M&R team is involved in providing repair options and recommendations to operations to aid in making an appropriate decision and intervention.

Figure 5.8 summarizes the M&R support team's safety related responsibilities, operational context, unsafe decisions, control actions and process model flaws. As the M&R support team is involved in maintaining integrity of the crude distillation unit, it is an important component of the safety control structure with proximate safety-related responsibilities during normal operation, turnaround and emergency situations. As listed in Figure 5.8, the M&R support team took several unsafe control actions. Analysis of these actions identifies the following control/feedback inadequacies at the M&R support team level:

<u>Control/Feedback Inadequacies</u>

<u>Inadequate control - Revised scope of 4-SC pipe replacement instead of going for an inherently safe approach</u>

It seemed that when an M&R engineer got pushback on full 4-SC replacement, he revised the scope to partially upgrading 4-SC piping presumably based on an understanding of partial pressure[18] impact on corrosion. However, the M&R engineer was unaware that the relevancy of previous inspection data is reduced when production changed crude feedstock. In addition, the whole 4-SC pipe circuit is exposed to the same operating conditions, temperature and crude concentration, so M&R engineer could have convinced reviewers to approve for inherently safer solution under total replacement scope.

Inadequate control – Did not provide sufficient communication to higher-level management to push corrosion issue forward

When traced back to investigation reports, there were three occasions where 4-SC piping replacement scope were proposed to the turnaround planning process and were rejected. However, it seemed that M&R support team did not raise this issue to higher management level, this was probably because many sub teams under M&R conducted different corrosion studies or risk rankings with similar finding and recommendations. However, there were only two rounds of plant turnarounds, 2007 and 2011, where M&R could have replace the corroded piping. Hence, each engineer job owner who got refused from turnaround planning teams might not see a rejection as a big issue as the corrosion data still predicted a longer piping life and waited for the next round of turnaround. Therefore, the piping replacement issue was not raised up to M&R Management leading to not enough support for implementation even though sulfidation mitigation recommendations were published in chevron technical networks.

Inadequate control/ feedback – Did not follow up on 100% inspection using continuous monitoring technology during 2007 turnaround

From investigation report [7] the turnaround core team rejected replacement proposals based on existing corrosion data, which were in fact limited and inaccurately represented corrosion risk. However, there was no evidence that the M&R team who issued Corrosion Mitigation Plan for the crude unit followed up to verify continuous monitoring technology had been installed on all pipe components of 4-SC circuit. Hence, not all pipe components on 4-SC had been monitored leading to insufficient corrosion inspection data to confirm the need for 4-SC pipe replacement.

[18] Partial pressure is a function of substance concentration and system operating pressure. Partial pressure impact corrosion rate

Inadequate control / feedback – Did not provide a clear path forward during new guidelines presentation to refinery reliability steering team (2010)

The material engineer presented the new ETC guideline to the Refinery Steering Committee, which stated sufidation corrosion mitigation requirements. However, it seemed that there was no focal point to provide implementation plan, resources and drive this change and hence this issue was not put as high priority amongst various teams.

Inadequate control - Did not provide 100% inspection recommendation on 4-SC (2009)

The material group under the M&R department completed a risk ranking of the Crude unit's carbon steel piping which identified 4-SC piping as high-risk line per ETC ranking guidance. However, the material group did not provide any recommendation to complete 100% component inspection on 4-SC but instead recommended to replace corroded 4-SC piping with 9-Chrome material. Subsequently, the alternative 100% component inspection was not performed and when both the inspector and material group recommended the turnaround-planning team to replace 4-SC the planning team rejected this recommendation based on a lack of corrosion inspection data that would have showed the severity of corrosion on some of 4-SC pipe components.

Safety related responsibility

- Follow Operational Excellence and Tenet of operation regimes
- Follow Emergency response procedures
- Provide reliability input to process hazard analysis, MOC work processes
- Take appropriate action to improve equipment and piping reliability
- Competent and aware of current ongoing industrial issue relate to their working area e.g. sulfidation corrosion.

Context

- Refinery introduces new crude from various sources with different sulfur contents over operating lifetime.
- Refinery has been in operation for 40 years hence there are a lot of maintenance and repairing activity on going.
- The team has to interface with all working groups such as operator, reliability as well as upstream and downstream plant support teams so team has to work under some constraints and requirement imposed

- Corporate provides subsidiary companies with many work processes (e.g. RBI, ROI/IPR, Inspection guideline) and documentation which imposes workload and time constraint to complete the process
- Refinery turnaround work planning is very intensive and interactive in nature due to scope and associate physical equipment involved.
- Team is subject to reliability, capital budgets and other goals imposes
- Turnaround is very schedule driven and time constraint in nature
- Complex data tracking system

Unsafe Decision & control action

- Revised scope of 4-SC pipe replacement instead of going for inherently safe approach
- Did not provide sufficient communication to higher-level management to push corrosion issue forward
- Did not follow up on 100% inspection using continuous monitoring technology during 2007 turnaround
- Did not provide a clear path forward during new guidelines presentation to refinery reliability steering team (2010)
- Did not provide 100% inspection recommendation on 4-SC (2009)

Process model flaw

- Engineer tends to make decision base on inspection data available without noticing bias or flaw.
- Level of knowledge and understanding of Sulfidation corrosion varied between engineers
- 4-sidecut upstream and downstream piping experiences same level of corrosion (same operating temperature and composition) but put emphasizes on higher operating pressure service rather drive for inherent design approach

Figure 5.8 – M&R Support team level analysis

Inspector

Per the Safety Control Structure (Figure 5.1), the inspector controlled the integrity of refinery equipment by performing inspections, collecting and analyzing corrosion monitoring data, and providing recommendations to the M&R support team and production team via inspection reports. The inspector received feedback from ETC, M&R support and production team via email, minutes of meeting or verbal communication. The inspector collects data from CML sensors and updates these into the meridian database system.

Figure 5.9 summarizes the inspector safety related responsibilities, operational context, unsafe decisions and control actions, and process model flaws. As an inspector is involved in re-validating the integrity of the crude distillation unit, he/she is an important component of the safety control structure with the proximate safety-related responsibilities during normal operation and turnaround. As listed in Figure 5.9, the inspector took several unsafe control actions. Analysis of these actions identifies the following control/feedback inadequacies at the inspector level:

Control/Feedback Inadequacies

Inadequate control/feedback – Did not correctly enter inspection (Radiographic testing) data into condition manager section of the software (2002)

A 4-CU inspector entered 30% loss in thickness of the 4-SC spool that failed in the history description section rather than in the condition manager database section, where the program in that section to calculate corrosion rates and predicting future thickness would have used these CML data. Therefore, entering data in the wrong location limited the ability for the 2007 turnaround core team to utilize data in making its decisions.

Inadequate control - Did not install that the CML probes at the right locations

4 CU inspectors were not aware that current monitoring locations mainly on the fittings of 4-SC piping components did not reflect the severity of the sulfidation corrosion. In general, CMLs are most frequently placed on elbows and fittings as these locations consist of welding and change in flow directions, which make them more susceptible to corrosion. However, the risk of sulfidation corrosion was also high at straight pipe components because the silicon content of the carbon steel was lower - the carbon steel pipe manufacturing process had preemptively provided fittings and elbows with higher silicon content than straight pipe components. Therefore, the installed CMLs did not reflect severity of corrosion condition of 4-SC.

Inadequate control – Did not install sufficient number of continuous monitoring instruments for 100% inspection per Corrosion Mitigations Plan (2007)

Based on the CSB investigation report [7], 4-SC piping has 67 components but only had 16 Guided Wave Ultrasonic Testing (UT) sensors installed. The investigation report [5] did not explained why 100% monitoring was not provided but it may have been due to budget constraints and/or the confidence in the accuracy of readings obtained from UT sensors - in 2009, the inspectors concluded that these UT sensors were unreliable and continued to rely on the traditional wall thickness measurement techniques.

Inadequate control – Did not implement 100% inspection per ETC guideline (2011)

The turnaround core team agreed to inspect 4-SC piping during the 2011 turnaround but there was no indication that the ETC guideline that recommended conducting 100% component-by-component inspection was considered or documented in the planning. Thus, the inspector installed additional CMLs on 4-SC straight pipe components leading to a total of 19 CMLs across 67-pipe components. However, it was not clear why he did not cover all components as per the ETC recommendation and therefore, 100% high priority pipe inspection was not performed. This led to wrong understanding of sulfidation corrosion status indicators and allowed the turnaround core team to believe that 4-sidecut piping would last until next turnaround in 2015-2016.

Inadequate control/feedback – Did not conduct Fit for Service on pipe section that was deferred for replacement (2011)

The inspector did not evaluate for 'fitness for service' on the 4-SC pipe spool that he aware it had a marginal thickness remaining compare to design criteria. Hence, when this pipe spool piece was deferred for replacement by turnaround planning team, its integrity was unknown and therefore, no information to feedback on the urgent need to replacement this 4-SC pipe.

Inadequate control / feedback – Did not repeat the measurements on out-of-tolerance CML readings and did not enter these measurement data into conditional manager database (2012)

According to Chevron's investigation report [5], per the Refinery Piping Inspection Guideline, out-of-tolerance readings have to be repeated. The inspector did not repeat the out-of-tolerance measurements resulting in inaccurate data collection. Besides, the data were not entered into the conditional manager database and hence no one else could detect the flaw in the data. Thus, this piping inspection data could not be tracked for its latest status and did not reflect the risk of piping integrity.

Safety related responsibility

- Follow Operational Excellence and Tenet of operation regimes
- Determine integrity of equipment and piping on fitness for service
- Manage inspection data in compliance to company's process safety management policy
- Train and Certify by industrial agencies (API, stage, National Boiler Inspection Code) to perform inspection and develop appropriate inspection plan for their units

Context

- Refinery has been in operation for 40 years hence there are a lot of maintenance and repairing activity on going for 1000+ equipment and miles of piping.
- Refinery turnaround work planning is very intensive and interactive in nature due to scope and associate physical equipment involved.
- Team is subject to reliability, capital budgets and other goals imposes
- Turnaround is very schedule driven and time constraint in nature due to its infrequent occurring (once every 4-5 years)
- Complex data tracking system (Meridian system is used in storing, predicting, computation of inspection data and triggering inspection or replacement activities)
- Crude unit no.4 associate piping contains more than 8800 CMLs where each CML involves four or more thickness measurements.
- Utilize unreliable sensor technology, Ultrasonic Testing, to monitor 4SC piping
- Silicon concentration is higher in fitting component and straight piping
- Require destructive testing to measure silicon concentration for detecting risk of sulfidation

Unsafe Decision & control action

- Did not correctly enter inspection (Radiographic testing) data into condition manager section of the software (2002)
- Did not install that the CML probes at the right locations
- Did not install sufficient number of continuous monitoring instruments for 100% inspection per Corrosion Mitigations Plan (2007)
- Did not implement 100% inspection per ETC guideline (2011)
- Did not conduct Fit for Service on pipe section that was deferred for replacement (2011)
- Did not repeat the measurements on out-of-tolerance CML readings and not entered these measurement data into conditional manager database

Process model flaw

- Believe in flaw calculation from other function relate to hoop stress and safety factor thickness estimation.
- Not aware that straight run piping is at higher risk than fitting due to non uniform silicon distribution from manufacturer
- Locate corrosion coupons on fittings where other type of corrosion normally takes places.

Figure 5.9 – Inspector level analysis

Maintenance and Reliability (M&R) management

Per the Safety Control Structure (Figure 5.1), Maintenance and Reliability management are responsible for ensuring work process and tools are in placed to control the refinery equipment reliability performance. M&R management supervises inspector and M&R support team as well as setting and monitoring department performance indicators. The M&R management receive feedback from their direct subordinates, ETC and operation management via report, email, minutes of meetings or verbal communication as well as Chevron's technical community update/ bulletins.

Figure 5.10 summarizes the M&R management's safety related responsibilities, context, unsafe decisions and control actions, and process model flaws. As listed in Figure 5.10, the M&R management took some unsafe control actions. Analysis of these actions results in the identification of the following control/feedback inadequacies at the M&R management level:

Control/Feedback Inadequacies

Inadequate feedback – did not take action on the sulfidation corrosion issues at executional level

It appeared that maintenance management did not take action on the issues that their M&R subordinates were facing. When production rejected 4-SC replacement three times there was no evidence in the investigation reports that maintenance management provided support to inspectors or the M&R team to drive 4-SC piping replacement. M&R management was directly involved in the communication loop from ETC regarding the implementation of 100% inspection on high priority piping, P1, but failed to follow up and provide an interface with the production manager who could enforce the replacement recommendation.

Inadequate control – did not fully optimize the use of available resources

From the investigation report [7], it appeared that the M&R support team and inspectors had utilized many work process tools and initiated studies, which were redundant. There is no evidence to indicate any attempt by the M&R management to consolidate or link the data obtained from various inspections and studies into one tracking process or system. This resulted in each sub team only using the limited data that was available to them. It also did not seem that M&R management utilized many expertise from Corporate or ETC teams to support driving the change in piping material for 4-SC.

Safety related responsibility

- Follow Operational Excellence and Tenet of operation regimes
- Follow Refinery emergency response procedure
- Drive ETC recommendations to improve safety/reliability performances
- Ensure compliance to company code/standard requirements
- Maintain refinery equipment and piping to ensure they meet integrity requirements
- Ensure effectiveness of cooperate safety related work process utilization

Context

- Work pressure not to disrupt on ongoing production
- Budget planning is set once a year
- Many areas to be focused to meet budget, reliability and safety goals
- Corporate initiatives can give some redundancy in work scope or information
- Many sub division/teams under supervisions
- Only have refinery turnaround every 4-5 years

Unsafe Decision & control action

- Did not take action on the sulfidation corrosion issues at executional level
- Did not fully optimize the use of available resources

Process model flaw

- Underestimate effort of implementing sulfidation corrosion mitigation action
- Subordinates are familiar and working effectively with existing tools and work process
- Inadequate communication and means to detect issues at execution level

Figure 5.10 – M&R management level analysis

Operation management

Per the Safety Control Structure (Figure 5.1), operation management enforced work process and corporate tools to control the refinery equipment productivity performance. This is performed through supervising production support team and operation team, enforcing work process, setting and monitoring department performance indicator. The operation management received feedback from their subordinates via reports, email, minutes of meetings or verbal communication, Maintenance management and ETC via email, verbal communication, or technical communities update/ bulletins.

Figure 5.11 summarizes the operation management safety related responsibilities, context, unsafe decisions and control actions, and process model flaws. As listed in

Figure 5.11, the operation management took unsafe control actions. Analysis of these actions results in the identification of the following control/feedback inadequacies at the operation management level:

Control/Feedback Inadequacies

Inadequate control – Did not enforced safety culture to operation working teams adequately

There were many lessons to be learnt from previous industrial accidents due to sulfidation corrosion as well as training provided to refinery engineers by corrosion expert personnel. However, it seemed that the production team did not rate process safety related decisions as a high priority. When they faced with conflicting decision e.g. from risk assessment and MOC reviews, they did not give sufficient priority to the piping integrity issue. This may be because production management did not provide sufficient process safety enforcement to the production support team, which resulted in the previously mentioned decisions and outcomes.

Inadequate feedback - Not abled to detect socio and regulatory pressure impact relate to flaring

By receiving pressures from other division such as perhaps commercial and the community, production management team did not detect or anticipate the impact these have on their workers' decision that resulted in escalated fire of the crude unit.

Safety related responsibility

- Follow Operational Excellence and Tenet of operation regimes
- Follow Refinery emergency response procedure
- Drive ETC recommendations to improve safety/productivity performances
- Ensure compliance to company code/standard requirements
- Ensure compliance to federal, state, city and local regulatory requirements
- Ensure effectiveness of cooperate safety related work process utilization
- Provide training to personnel
- Ensure accurate record of equipment and piping information are maintained

Context

- Commercial pressure not to disrupt on ongoing production
- Many areas to be focus to meet budget, productivity and safety goals
- Corporate initiatives can give some redundancy in work scope or information
- Many plants/teams under supervisions
- Various drives on work process and studies from various groups with similar recommendations
- Many actions generate from various audits at various quality
- Only have refinery turnaround every 4-5 years

Unsafe decision & control action

- Did not enforced safety culture to operation working teams adequately
- Not abled to detect socio and regulatory pressure impact of flaring

Process model flaw

- Emphasize on compliance to demonstrate good operational discipline
- Subordinates are familiar and working effectively with existing tools and work process
- Inadequate communication and means to detect problem at execution level
- Prioritize high priority on data driven over industrial lesson learns and recommendation from experts in decision making

Figure 5.11 – Operation management level analysis

Refinery Manager

The Refinery Manager is the center of gravity of the External Richmond Refinery management system with control and feedback linkages to multiple entities on both the Richmond Refinery System Operation and External Refinery System management of the hierarchical system Safety Control Structure. The Refinery Manager's roles and responsibilities include providing operation and maintenance management with capabilities in the form of resources, procedures, work processes, oversight, and training programs to support safe and effective execution of the refinery missions. In addition, he also needs to manage expectations of the communities around the refinery through ensuring good socially responsible care and transparency and demonstrating regulatory compliance. From a Refinery system operation perspective (Figure 5.1), as Refinery Manager, the management maintains the following control/feedback linkages:

- Operation and Maintenance (O&M) management – The Office of Refinery Management provides O&M management with goals, policies and capabilities to meet the mission needs. The O&M management provides feedback to the Office of Refinery Management in the form of performance reports.
- Chevron Corporate - The Office of Refinery Management provides Chevron Corporation with performance reports to meet defined goals and objectives. Chevron Corporate provides directive and requirement to the Office of Refinery Management in the form of policies, processes, management system, tools and behavioral expectations and facility auditing.
- EPA - The Office of Refinery Management provides EPA with risk management plans and payments upon regulatory violations from previous incidents. The EPA provides regulatory requirement and subsequent notification to the Office of Refinery Management in the form of CFR (Code of Federal Regulations), letter or notification and endorsement on district works.
- Cal/OSHA – The Office of Refinery Management provides OSHA/Cal OSHA with fine payment upon regulatory violations from previous incidents. The Cal/OSHA provides regulatory requirement and notification to the Office of Refinery Management in the form of CFR, letter or notification and facility audit.
- Contra Costa County (CCC) and Richmond City - The Office of Refinery Management demonstrates refinery compliance to CFR by providing CCC and Richmond city with incident report, Hazard analysis, emergency response and gap closure plans. The CCC and Richmond city provide Richmond Refinery Management Office with audit/inspection reports.
- Bay Area Air Quality Management District - The Office of Refinery Management provides BAAQMD with emission permit request for approval and emission reports. BAAQMD enforces pollution control by requesting a flare minimization

plan, providing feedback on emission reports and stipulating terms of permit approval.

Based on the above interaction, the following inadequacies regarding control/feedback within the Refinery Management system and specifically the Office of Refinery management are identified:

Control/Feedback Inadequacies

Inadequate Control/Feedback – Insufficient Review/Enforcement of Corporate auditing recommendation

There was no evidence in the investigation report [7] describing how the Refinery manager cascaded or enforced actions resulting from corporate audit regarding sulfidation corrosion down to operation management level. Therefore, it is unclear whether the Refinery manager provided resources to track and take actions to improve pipe integrity as a result from audit finding.

Inadequate Feedback – Insufficient monitoring of effectiveness and quality of work processes implementation

There is no record of Refinery management providing audit regarding implemented work processes. For example, MOC process should have communicated the change from production to maintenance so that related maintenance information could have been updated but it did not. If a refinery management only looks at the tracking MOC performance results it is unlikely that management will know of any issues on use of tools at operation level.

Inadequate Feedback/Control – Not provide sufficient emergency guidelines for operation personnel to make decision and failure to detect the dynamic changes, which shifted the operators' safety priority

Productivity, cost and environmental enforcements are likely to impact refinery personnel during their decision-making process. Refinery management has to provide adequate guidelines to enable decision makers to make quick, safe, and decisive choices. For example, operation often needs to decide whether they should shutdown or continue the operation of equipment when evaluating leaks. It was not certain whether the guidelines only contained high-level emergency management information and hence resulted in ambiguity regarding which level of leak severity triggers the use of emergency shutdown.

Inadequate Feedback/Control – Failure to integrate various safety related reviews/ tools to improve risk understanding across functions and reduce redundancy work process

Various chevron employees (Refinery and ETC) participate in a number of process safety management review sessions such as PHA, ROI/IPR, RBI which provide significant input to the analysis. However, these activities are sometimes redundant or do not have full involvement from other functions which could result in underestimation of the risk and a gap in communication. If Refinery management could provide a combined review or better work sequences (informational flow) between the individual reviews so that a better understanding across various functions was established this would lead to better process safety outcome.

Inadequate Control/detection – Did not provide adequate emphasis on equipment mechanical integrity management

As identified in CSB report [7] the refinery has more than 100 clamps installed in processing units. According to the Cal/OSHA citation some of these clamps did not get replaced on time during turnaround. This indicates a mechanical integrity management issue inside the refinery.

Inadequate Control - Failed to promptly report the release of toxic material into the air

Refinery management did not alert Contra Costa County immediately during the initial white cloud leak. The approximately 10-minute delay resulted in people who lived in the nearby area being exposed to particulates from smoke and subsequently hospitalized.

Figures 5.12 summarize the safety related responsibilities, context, unsafe decisions and control actions, and process model flaws of the Refinery Managers.

Safety related responsibility

- Ensure compliance to Federal, State, City and country Risk and Process safety requirements.
- Ensure compliance to corporate codes/standard requirements
- Ensure effectiveness of corporate safety related work process utilization
- Delivery of appropriate HES processes including process safety and workforce behavior
- Accountable for all aspect of refinery's performance including commercial, public affair, safety environmental and human resources.
- Commitment and responsibility to public to operating safely protecting people and the environment

Context

- Increasingly stringent state and federal policies that called for the refinery to reduce air emission and waste, treat water, and prevent oil spill (1980)
- Growing needs of California electric utility companies and shift in the availability of quality crudes, presented challenges to manufacturing operations (early 1980)
- Refinery need to meet its production target (largest crude base producer)
- Between 1989 and 1995, there were 304 accidents at the Chevron refinery including fires, spills, leaks, flaring and toxic gas releases.
- From 2009 to 2011, Chevron and the City of Richmond were entangled in a legal battle over Chevron compliance with environmental regulations related to an upgrade of the aging refinery
- Refining environment, marked by tight margins and mounting regulatory challenges, the ability to process high-sulfur crude is increasingly important.
- Local greenhouse gas-mitigation measures and several council members have already signaled they want to see emission reductions at the refinery
- Refinery consists of 30 integrative operating plants (2002)
- An explosion and fire at the refinery spread noxious fumes and sent hundreds of Richmond residents to hospitals (1999) causes bad perception to community and more forces from environmentalist
- Community concern over some visible flaring that occurs at the Richmond Refinery

Unsafe Decision & control action

- Not provide sufficient review/ Enforcement of Corporate auditing recommendation
- Not provide sufficient monitoring of effectiveness and quality of work process implementation

- Not provide sufficient emergency guidelines for operation personnel to make decision and failure to detect the dynamic changes, which shifted the operators' safety priority
- Failure to integrate various safety related reviews/ tools to improve risk understanding across functions and reduce redundancy work process
- Did not provide adequate emphasis on equipment mechanical integrity management
- Failed to promptly report the release of toxic material into the air

Process model flaw

- Current work process and software are sufficient to ensure safe operation and meet regulatory compliances.
- Not aware of safety state of the refinery

Figure 5.12 Refinery management level analysis

Energy Technology Company (ETC)

The ETC controls the feedback linkages to multiple entities on both the Internal Refinery System Operation and External Refinery System management of the hierarchical system Safety Control Structure. The ETC's roles and responsibilities include providing operation and maintenance managements with capabilities in the form of tools, guidelines, standards, advice and training programs to support safe and effective usage of those capabilities.

Figure 5.13 summarizes the ETC related responsibilities, context, unsafe decisions and control actions, and process model flaws. As listed in Figure 5.13, the ETC performed some unsafe control actions. Analysis of these actions resulted in the identification of the following control/feedback inadequacies at the ETC level:

<u>Control/Feedback Inadequacies</u>

<u>Inadequate Control - Did not appear to deliver a clear path forward for new guideline implementation</u>

There was no evidence in the investigation reports [5],[7] that it is the ETC's responsibility to monitor or track the extent which the operating business unit acted upon their advice. It is inferred that the ETC is only responsible for generating suitable guideline currently and only provides one-way communication. However, it was not clear whether the ETC establishes a timeline for completing the piping prioritization analysis or whether they define the completion timeline for a 100% baseline inspection in the guideline. Therefore, in 2010 when a material engineer presented the new sulfidation corrosion protection guideline, which helps to prioritize high risk piping sections to refinery personnel, the refinery personnel did not understand the way forward or the urgency of the action was required.

Inadequate Control / Feedback – Did not provide official guideline to assess the adequacy of isolation valves on old distillation units

It was not clearly indicated within –the investigation reports [5][7] whether the missing isolation valve on crude no.4 unit, which was based on the old design, required upgrades. This is a similar issue to the carbon steel piping code revision. The installed 4-SC piping did not comply with current standard. The policy implemented by the Refinery or ETC on how to address existing design gaps compared to the current industrial standards is not known. Perhaps if the ETC provided a Loss Prevention audit checklist or conducted an audit of the business unit, it may help in the detection of issues for further review.

Inadequate Control – Did not provide reflections of lesson learnt from incidents into PHA guideword/ checklist

From the CSB's investigation report, it seemed that sulfidation corrosion was not documented in the PHA session. If the ETC had integrated this item into the PHA checklist, then the question or concern could have been raised in the HAZOP/ What-if? sessions and documented in due process.

Safety related responsibility

- Keep up with industrial updates to maintain technical expertise in the fields
- Provides technical expertise for Chevron operations worldwide to improve reliability and safety performance.
- Invents proprietary technologies designed to find and produce energy reserves safely and protecting the environment and supporting local communities
- Revise company code and standards to reflect changes in technologies and industrial lessons learns

Context

- Many technologies and industrial updates while facilities were built to comply to old codes
- Knowledge and manufacturing specifications of equipment and piping were not as stringent in the past as today.
- ETC has to service hydrocarbon processing facilities around the world. Those facilities were built differently and hence it is difficult to provide perfect solution to address gaps that occur.
- Distillation column has many off-take piping hence it is difficult to define practical isolation location.

Unsafe Decision & control action

- Did not appear to deliver a clear path forward for new guideline implementation
- Did not provide official guideline to assess the adequacy of isolation valves on distillation units.
- Did not provide reflections of lesson learnt from incidents to PHA checklist/ guideword

Process model flaw

-

Figure 5.13 ETC level analysis

Chevron Corporate Management

The Corporate Management controls linkages to multiple entities mainly in the External Refinery System management of the hierarchical system Safety Control Structure. The Corporate Management roles and responsibilities were mentioned earlier in Refinery management sections. Corporate Management also conducts audits of business unit operation at the management level and provides feedback to management to address their findings. At the same time, the Corporate Management directs the ETC to design solutions to common issues that business units face in order to improve operational excellence. Corporate Management also interfaces with EPA and OSHA upon associated legal actions.

Figure 5.14 summarizes the Corporate Management related responsibilities, context, unsafe decisions and control actions, and process model flaws. As listed in Figure 5.14, the Corporate Management performed some unsafe control actions. Analysis of these actions resulted in the identification of the following control/feedback inadequacies at the corporate level:

Control/Feedback Inadequacies

Inadequate control and feedback – Did not provide adequate audit and follow up on findings from the audit

From the CSB investigation report, the corporate audited Richmond Refinery in March 2012 and detected issues on corrosion risk management. However, the issues had first risen in 2002 indicating there may not be sufficient audits provided to the site previously to detect chronic problems such as in this case. In addition, there was no evidence on how the Corporate Management tracked the 2012 findings in the system and followed up on the issues.

Inadequate control and feedback – Did not provide adequate oversight and enforcement of the ETC recommendation and work processes related to safety

There was no evidence that corporate found any deficiency in PHA reports or MOC items during their work process audits. In addition, Corporate Management did not provide adequate enforcement of ETC sulfidation corrosion recommendations, which may have resulted in the operations developing a different prioritization scheme for taking corrective action.

Inadequate feedback – Did not provide adequate oversight related to human factors which resulted in certain safety deficiencies

Corporate Management was not aware of any shift in safety culture or contextual factors that had the potential to alter refinery employee behavior. (See a discussion in Step 6 – Operation Management that that discussed about factors affecting shutdown decision)

Safety related responsibility

- Commitment and responsibility to public to operating safely, protecting worker, public and the environment
- Provide global business strategy to operate where it can legally and profitably conduct its business
- Provide management system, work process, procedure, guideline and resources to business units to support their regional operation effectively

Context

- Greater challenge to explore and produce crude oil and natural gas in lead to a greater demand to run to run business flexibly.
- Global warming, green house gases and pollution have become the world's concern.
- Impact of politic, economic and geographical constraints on price and quality of raw material e.g. crude oil

Unsafe Decision & control action

- Did not provide adequate audit and following up on finding actions from the audit
- Did not provide adequate oversight and enforcement of ETC recommendation and work processes related to safety
- Did provide adequate oversight related to human factors which resulted in certain safety deficiencies

Process model flaw

- Believe that tools and system in place are effective to prevent losses to the company
- Believed the Richmond Refinery fully comply to regulations
- Believed that Operational Excellence, Tenet of Operation etc. in place were sufficient to prevent process incidents

Figure 5.14 – Corporate level analysis

Bay Area Air Quality Management District (BAAQMD)

BAAQMD agency has used its expertise to diminish air pollution levels throughout the Bay Area and mainly interacts with the EPA and the refinery as shown in hierarchical system Safety Control Structure shown in Figure 5.2.

Figure 5.15 summarizes the BAAQMD related responsibilities, context, unsafe decisions and control actions, and process model flaws. As listed in Figure 5.15, the BAAQMD performed some unsafe control actions. Analysis of these actions has resulted in the identification of the following control/feedback inadequacies at the BAAQMD level:

Control/Feedback Inadequacies

Ineffective control - Stringent flaring allowance guidelines have inadvertent side effects on operator decisions

As there are many processing facilities that emit pollutants or toxic substances under the area of responsibility of BAAQMD, BAAQMD only grants stringent flaring allowances to ensure each facility minimizes the practice. However, flaring is a safety critical element of a refinery processing facility to quickly release hydrocarbon out of the systems safely under emergency. The penalties imposed by BAAQMD for exceeding its allowances might provide another variable for consideration by the operation team such that they delay the use of the Emergency Shutdown Button during initial the leak discovery and prior to rupture. Therefore, clear unambiguous guidelines should be put in place.

Safety related responsibility

- Reduce and ultimately eliminate health disparities due to air pollution.
- Achieve and maintain air quality standards for all criteria pollutants, utilizing the expertise and innovation of the Air District and its partner agencies.
- Implement exemplary regulatory programs and ensure compliance with applicable Federal, State and Air District regulations.
- Enforce "Clean Air Act"
- Ensure EPA concerns are addressed in industrial flare permit

Context

- The 9 counties of the San Francisco Bay Area form a regional air basin, sharing common geographical features and weather patterns, and therefore similar air pollution burdens, which cannot be addressed by counties acting on their own
- Significant increases in traffic and population in the region
- The continual evolution of industrial technologies
- Health-protective air quality standards that are periodically strengthened by the state and federal governments.
- The Bay Area Air Quality Management District receives approximately 3,000 air pollution complaints every year from members of the public.
- Many hydrocarbon / chemical flaring incidents or release accidents from refineries, chemical plants within the areas

Unsafe Decision & control action

- Stringent flaring allowance guidelines have inadvertent side effects on operator decisions.

Process model flaw

- BAAQMD requires that refineries within the District have flare minimization plans in place to prevent and reduce the number of flaring incidents. However, flaring is one of a means for refinery to safely operate within design limit so this impacted operator decision during emergency
- Casual of complaints can come from various sources, not only refinery and chemical plants

Figure 5.15 BAAQMD system level analysis

Cal/OSHA

The Cal/OSHA controls linkages to multiple entities in both the Refinery system operation and the External Refinery System management of the hierarchical system Safety Control Structure. As mentioned earlier, the Cal/OSHA roles and responsibilities include assuring safe and healthy working conditions for workers by maintain and revising CFRs and standards including PSM. Cal/OSHA works with local agencies in the CCC and the City of Richmond to audit workplaces to ensure enforcement of regulation and to impose citation penalties upon violations by the companies.

Figure 5.16 summarizes the Cal/OSHA related responsibilities, context, unsafe decisions and control actions, and process model flaws. As listed in Figure 5.16, the Cal/OSHA performed some unsafe control actions. Analysis of these actions resulted in the identification of the following control/feedback inadequacies at the Cal/OSHA level:

Control/Feedback Inadequacies

Inadequate control/feedback – Did not provide adequate review of a company's PHA to identify quality of hazard analysis works

OSHA enforced PSM standard in which one of fourteen components under PSM requires company to conduct PHA and revalidate it every five years. However, Cal/OSHA does not typically review a company's PHA [7] as part of its routine oversight of process safety management unless there is a specific complaint. Therefore, Cal/OSHA will not be able to detect the missing risk identifications or review a quality of safeguards that a company claims to have put in place. This lack of review results in reactive safety management, which is inadequate for reducing risk and preventing complex accidents from occurring.

Inadequate feedback – Did not have the means to detect the state of the process safety situation of each facility

OSHA PSM District office only conducted three planned inspections with only 150 inspector hours of effort. These inspections did not result in any citations or fines whereas the other federal NEP refinery inspection programs spent 1000 inspector hours and resulted in average of 11.2 violation [7] finding. Besides, as Chevron voluntarily utilizes both leading and lagging indicators in their US refineries. OSHA did not request Chevron to report the status of its indicators to the California regulator. Therefore, OSHA does not have the sufficient means to detect the state of the process safety situation of each facility to drive for continuous safety performance improvement.

Inadequate control / feedback – Did not improve regulation requirements to match the lessons learnt from incidents or audit findings

OSHA takes a long time to revise its CFR and other regulatory requirements owing to policies and procedures of its own. This results in codes, which are not up to date for the local inspector and auditors. Many potential process accidents in the chemical and refinery industries in the USA may be able to be averted with a more frequent revision of the regulations.

Inadequate control– Did not provide adequate review of recommended best practices

OSHA did not consolidate the recommended best practices for the industry to follow as compared to other regulatory agencies in other region. In addition, OSHA did not analyze recommended practice such as API RP 939-C [7] to determine whether its provisions are sufficient to reduce risks and manage hazard relate to sulfidation corrosion. API RP 939-C does not use the word "shall" which means no requirements are imposed on the petroleum industry. However, OSHA used this voluntary practice to issue a citation to Chevron instead of challenging the requirements of the RP to drive continuous improvement and risk reduction.

Safety related responsibility

- Manage safety requirements in workplace
- Revise code, standards, technology and lessons learnt to improve safety performance
- To ensure workers in process facilities are thoroughly trained and adequate PSM practices are implemented.
- To ensure employers in California provide effective written injury and illness prevention program for workers
- Enforce process safety regulation
- Provide guidance to state, regional and area offices and agencies for inspecting petroleum-processing facilities to reduce or eliminate workplace hazard.

Context

- Lengthy standard setting process due to complicated impact evaluation leading to a decade long of static regulations
- Industry standards, technologies and practice continue to change and advance
- New chemicals and discoveries continue to be developed and produced but the list of hazardous chemicals have not been updated since 1990
- Great number of petroleum refinery incidents occur each year (125 cases in 2012) which intensifies OSHA's workload
- Regulatory regime in USA does not focus on management of change, which is usually one of the accidents causal.

Unsafe Decision & control action

- Did not provide adequate review of company's PHA to identify quality of hazard analysis works
- Did not have the means to detect the state of the process safety situation of each facility.
- Did not improve regulation requirements to match with lesson learns from incidents and audit findings
- Did not provide adequate review of recommended best practices

Process model flaw

- Belief that the activity based model will be sufficient to manage risk in the industry
- Have not used the ability to address urgent hazards by issuing emergency temporary standards
- Belief that all facilities are only required demonstrating their performance within the set requirement instead of reducing risk down to reasonably practical level.

Figure 5.16 Cal/OSHA system level analysis

Contra Costa County (CCC) / City of Richmond officers

The CCC and the City of Richmond controls linkages to multiple entities in both Refinery system operation management and External Refinery System management of the hierarchical system Safety Control Structure. As mentioned earlier, the CCC's and the City of Richmond's roles and responsibilities include assuring safe and healthy working conditions for workers and the surrounding communities. They do so by working with various government agencies to implement programs such as RISO and ISO to ensure processing facilities in the area conduct their business in an ethical manner as well as protecting their workers, communities and the surrounding environment.

From the External Refinery System Management perspective (Figure 5.17), as the CCC and the City of Richmond maintain the following control/feedback linkages:

- Richmond refinery - The local officers provide Richmond refinery management and operations with regulatory program enforcement in the form of regulatory requirements, audit and report and document reviews. Richmond refinery submits RMP, Process Safety Information, and Emergency Response Plan per regulatory requirements as well as provides a proposed gap closure plan for findings from the facility audit.

- Local communities – The CCC and the City of Richmond provide emergency warning systems in the form of SMS and audio alarm as well as air quality monitoring systems. In addition, the officers present the facility audit report to the public for comments. The local communities provide feedback to the CCC and the City of Richmond in the form of written communication, attending public hearing etc.

Figure 5.17 summarizes the CCC and the City of Richmond officers' related responsibilities, context, unsafe decisions and control actions, and process model flaws. As listed in Figure 5.17, the CCC and the City of Richmond officers' performed some unsafe control actions. Analysis of these actions resulted in the identification of the following control/feedback inadequacies at the CCC and the City of Richmond officers' level:

<u>Control/Feedback Inadequacies</u>

<u>Inadequate control - Did not provide an effective emergency warning system to communities</u>

It is found that in some areas community members did not know about "shelter in place" warnings because of the delay in messages of up to 3 hours. This resulted in the residents' exposure to contaminated air. The computer system could only make 500 to 1,000 calls at a time and some callers were blocked, so at the end of the day the warning calls reached only a fraction of the residents who were put at risk by the fire.

<u>Inadequate control - did not establish a joint information center to coordinate public communication</u>

During the Chevron incident, the local agencies did not establish a joint operation center leading to poor public coordination, which resulted in conflicting statements and confusion among members of the public and local health care providers.

Inadequate control - Did not provide requirement of inherent safer system to existing construction, repair or corrective actions

Under ISO, the refinery is only required to implement inherently safer system during PHA and for new construction. The ISO that local agency develop does not require the refinery to provide supporting documentation to show that any selected system is inherently safer which made it impossible for agencies to verify the claim.

Safety related responsibility

- Protect local community from hazard
- Ensure compliance to state and federal regulation
- Implement additional requirements for Risk and Process safety management at county and city level
- Improve industrial safety by improving review, inspection, and audit
- Generate more stringent safety requirements.
- Activate the county's Community Warning System in the event of an immediate threat to life, health, or safety of the community

Context

- Rejected refinery renovation project due to insufficient environmental impact quantification

Unsafe Decision & control action

- Did not provide an effective emergency warning system to communities
- Did not establish a joint information center to coordinate public communication
- Did not provide requirement of inherent safer system to existing construction and repair

Process model flaw

- Audit based on current regulations – without any comparison with world wide industrial best practice
- Belief that the warning system was effective.

Figure 5.17 CCC and City of Richmond level analysis

CUPA / CCHMP

The CUPA/CCHMP controls linkages to multiple entities in both Refinery system operation management and External Refinery System management of the hierarchical system Safety Control Structure. The CUPA's roles and responsibilities include enforcement through various federal and state programs such as Cal ARP, RMP, Unified

Program and EPCRA and to protect public and the environment and the surrounding communities.

From the External Refinery System Management perspective (Figure 5.2), as the CCC and the City of Richmond maintain the following control/feedback linkages:

- Richmond refinery - The local officers provide Richmond refinery management and operations with regulatory program enforcement in the form of regulatory requirements, audit and report and document reviews. Richmond refinery submits RMP, Process Safety Information, and Emergency Response Plan per regulatory requirements as well as provides a proposed gap closure plan for findings from the facility audit.
- EPA - The local officers provide EPA with regulatory compliance updates in the form of facility audit reports while EPA provides codes, standards and guideline to local regulators to perform their enforcement job adequately.
- RC /CCC – The CCC / City of Richmond officers provide RISO, ISO requirements for CCHMP to conduct audit at local facilities
- Cal/OSHA – The local officers provide Cal/OSHA with regulatory compliance updates in the form of facility audit reports while Cal/OSHA provides city and county regulators with requirements in the form of CFRs, Process safety guideline etc.

Figure 5.18 summarizes the CUPA related responsibilities, context, unsafe decisions and control actions, and process model flaws. As listed in Figure 5.18, the CUPA officers' performed some unsafe control actions. Analysis of these actions resulted in the identification of the following control/feedback inadequacies at the CUPA/CCHMP officers' level:

Control/Feedback Inadequacies

Inadequate control/ feedback - Utilized inadequate regulatory checklists in facility audit

CCHMP engineers used existing regulations and regulatory program requirements; including Cal/OSHA PSM standards, EPA RMP rule, Cal ARP Program and RISO, as their basis in the facilities audit. As some of these regulations have not been regularly updated since 2000 [11], this has resulted in insufficient risk identifications. In addition, it can be inferred that CCHMP did not receive their feedback on the quality of their audit report from EPA and OSHA agencies and hence they did not receive the verification from code owners but only received an area of focus for the next audit.

Inadequate control/ feedback – Did not provide quality resource to enforce appropriate safety control action

From the latest audit at the Richmond Refinery, CCHMP engineers either gave "ensure" or "consider" findings. They did not encourage Richmond Refinery to follow an inherently safer system approach to provide safeguards for their crude unit in their PHA to reduce their risk further. The types of action items issued are dependent upon the knowledge and experience of the engineer conducting an audit. With budget constraints, the CCC and the City of Richmond did not have adequate staff to frequently audit each facility and provide good detection of flaws in each facility's operating and management system.

Safety related responsibility

- Implementing additional requirements of Risk and Process safety management at county and city level
- Report audit results to EPA and OSHA
- Improve industrial safety by proving review, inspection, audit

Context

- Cal ARP regulation is duplicative to EPA risk management plan with a few exceptions`
- Type of actions from audit depend on engineer's level of experience
- Experience budget reduction in millions

Unsafe Decision & control action

- Utilized inadequate regulatory checklists in facility audit.
- Did not provide quality resource to enforce appropriate safety control action

Process model flaw

- Audit base on current regulatory without comparing with industrial best practice elsewhere in the world
- Believed that the warning system was effective.

Figure 5.18 CUPA/ CCHMP level analysis

EPA

The EPA controls linkages to multiple entities in both the Refinery system operation management and External Refinery System management of the hierarchical system Safety Control Structure. As mentioned earlier, the EPA's roles and responsibilities include assuring safe environmental conditions for the workers and the public by maintaining and revising CFRs and standards. The EPA works with division and local agencies to enforce regulatory compliance, controlling air emission limit via citation penalties, emissions permit approval/endorsement and the review of audit reports.

Figure 5.19 summarizes the EPA related responsibilities, context, unsafe decisions and control actions, and process model flaws. As listed in Figure 5.19, the EPA performed some unsafe control actions. Analysis of these actions resulted in the identification of the following control/feedback inadequacies at the EPA level:

Control/Feedback Inadequacies

Inadequate control – Did not implement recommendations and learning from CSB from past industrial incidents

The CSB has made a number of recommendations to the EPA to revise the PSM and RMP regulations. However, the EPA has failed to implement these recommendations resulting in not updated regulations for the auditors.

Inadequate control/ feedback – Did not provide sufficient on-site inspection or audit

In 2009 the Office of Inspector General concluded that 65% of active RMP facilities (including high-risk facilities) had not received an on-site inspection or audit. This means that the EPA does not have sufficient data feedback. Additionally they cannot verify whether a facility has implemented what it has stated in its RMP.

Inadequate control – Did not provide sufficient requirement and oversight of RMP to reduce risk at facilities

EPA prescribes the Refinery to develop and submit a RMP and high level information of Hazard Analysis reports. However, the RMP rule does not require facilities to include the detailed PHA report, which indicates that detailed control and mitigation has been put in place. Hence, the EPA or its delegate does not drive the refinery to demonstrate and verify safety controls and mitigations. Additionally, the EPA RMP inspection team does not have the enough resources to conduct rigorous audits and does not require facilities to reduce risk to a 'As Low As Reasonably Practical' level. Therefore, the EPA does not provide an effective RMP program to comprehensively enforce control over major accident hazards and reduce risks. This only makes it activity-based requirement.

Safety related responsibility

- Enforcing environmental law regulatory requirements
- Monitoring, analyzing and reporting on the environment trends and work with organizations to carry out specific environmental function
- Regulating greenhouse gas emissions
- Ensuring industry to carry out appropriate actions for waste management
- Implementing Risk Management program
- Demand a report the release of toxic material into the air from operating chemical facility and others
- Cite facilities for failure to comply with Recognized and Generally Accepted Good Engineering Practice or CFRs.

Context

- Lengthy rule making process due to various impact assessments leading to static regulations for decades
- Industry standards, technologies and practice continue to chance and advancement.
- New chemical and discovery come into operation / production but list of hazardous chemicals have not been updated since 1990
- Similar requirement of Risk Management Program to OSHA Process Safety Management standard

Unsafe Decision & control action

- Did not implement recommendations and learning from CSB from past industrial incidents
- Did not provide sufficient on-site inspection or audit
- Did not provide sufficient requirement and oversight of RMP to reduce risk at facilities

Process model flaw

- Believe in activity base model will be sufficient to manage risk for refinery and chemical industries
- Not keep up with new risks generated from new technologies and chemicals.
- EPA only stay focuses on incidents under the scope of responsibility PSM and RMP to re-evaluate their safety rules. However, similar type of incident from different sources could reflect gaps in safety rule for further improvement too.

Figure 5.19 EPA system level analysis

Code and standard agencies

Code and standard agencies are responsible for providing companies and manufacturers with available standards or recommended practice. Companies will then provide technical feedback for standards and code developments.

Figure 5.20 summarizes the Code and standard agencies related responsibilities, context, unsafe decisions and control actions, and process model flaws. As listed in Figure 5.20, the Code and standard agencies performed some unsafe control actions. Analysis of these actions has resulted in the identification of the following control/feedback inadequacies at the Code and standard agencies level:

Control/Feedback Inadequacies

Inadequate control/feedback - Did not mandate minimum specification for silicon content (pre 1985)

The failed 4SC carbon steel pipe followed the ASTM A53B regulations issued in 1985 which did not mandate the minimum silicon content at 0.1% weight resulting in steel pipe sections that were susceptible to high variable sulfidation corrosion rate.

Inadequate control - Provided voluntary and permissive language in standard or recommended practices

It was noted in the CSB report [7] that certain guidelines such as API RP 939-C contain voluntary language. These guidelines did not use "shall" like other safety RPs as some guidelines are published to facilitate the broad availability of proven sound engineering and operating practices. Therefore, the guidelines did not provide an obligation for the company to adopt this recommended practice.

Safety related responsibility

- Generate standards, codes and recommended practices for the industry
- Revise and keep standards, codes and recommended practice up to date by reflecting lesson learn from the industries.

Context

- Three carbon steel piping specifications available for industry prior to 1985
- Manufacturers started to comply with 3 manufacturing specifications which has minimum 0.1 weight% silica content after 1985
- Code revisions cycle time 1-3 years

Unsafe Decision & control action

- Did not mandate minimum specification for silicon content (pre 1985)
- Provided voluntary and permissive language in code and standards

Process model flaw

- None

Figure 5.20 code and standard agencies level analysis

Step 7 - Examination of Overall Communication & Coordination

In previous part of the STAMP/CAST process, the analysis has looked at each component separately. In this part, overall communications and coordination are examined to identify cases, where coordination and communication between controllers resulted in significant sources of hazards and/or contributed to/caused the 4CU fire accident.

This analysis showed that many areas of interaction were significantly lacking in terms of communications and coordination. This issue has been discussed previously in Step 6 from a component level perspective. The following discussion is from the system perspective:

1. Inadequate coordination and communication - Decisions and actions after discovered the leaked pipe

   The emergency response working team, consisting of engineers, operators, fire fighting crew and supervisors did not have a well-coordinated work plan According to the report [5], each sub team planned their tasks and there was no single meeting where all parties could collaboratively consider the potential risk and outcome together. As such they did not identify the risk of a pipe rupture and its mitigation plan. As a result, the response team, with different level of knowledge of hydrocarbon properties, had taken different precautionary and responsive action during the rupture. Added to that, a different work shift performed the planned tasks that, so it appeared there was a communication gap even between the same workgroups.

2. Conflicted communication – Delayed activation of emergency shutdown

   Refinery management provides control action to enforce safety of operation and provides the operator with emergency shutdown, as well as normal 4CU shutdown procedures. However, while flaring action is the safest means to release hydrocarbon out of refining process quickly, it also creates combustible products, by products and black smoke, as a result of burning crude oil hydrocarbon. Therefore, operators also perceive indirect communications from BAAQMD and communities regarding pollution emission control from flaring. This conflict was likely to impact their decision during initial leak discovery and initial flash fire.

3. Conflicted coordination/ inadequate communication between workgroups – Not replaced 4-SC piping prior to its failure

   Reliability engineer and inspector can only replace pipe or install CML during unit 4CU shutdown while production can only give a limited time during the Turnaround which occurs every 4-5 years. Turnaround team has to prioritize their work lists to fit with the resource, time and budget available. Reliability engineer and inspector did not work together to resolve pipe replacement refusal issue, while production did not inform inspector about change in process temperature and crude feed composition change, which has a direct impact on corrosion rate calculation. At the same time, the engineering team made mistake in a calculation and therefore, the conflict to management change on 4SC and inadequate information flow between decision makers had let the team decision to be one of the casualty of the accident.

4. Inadequate coordination – ETC to Maintenance management to drive change on existing equipment

   Operation and maintenance managements understand the cause of 2007 Richmond refinery fire incident as well as other accidents under Chevron operating facilities. While ETC continuously generates recommended guidelines to detect and mitigate sulfidation corrosion and the guideline is passed to M&R management and inspectors for implementation. However, ETC does not have a direct influencing power on local business unit prioritization or ranking decision and only provide knowledge and advices and hence the organizational structure was not designed for effective influence. Nevertheless, it appeared that there were many studies and ranking occurred within maintenance and reliability team since 2002 by material group and engineers. However, as the recommendations from these studies provided the same control action to replace 4-SC piping, it might have led to a confusion among maintenance team about who is responsible for preventing and mitigating sulfidation corrosion for crude units at any one time. Similarly, several inspectors rotated to inspect 4CU inspections and hence did not provide a constant drive to get 4-SC pipe replaced.

5. Inadequate coordination/ communication – Change in industrial and internal company codes and standards

   Part of Industrial codes and standards are updated timely, which results in change in company guideline, code and standards. However, this is mainly applicable to new construction or new project, but some gaps on old equipment and piping exist. From investigation report, it did not clearly show how these gaps are managed or coordinated, especially with production management and teams who are the area owners to support and drive the change.

6. Inadequate coordination / communication – How well each facility was aware of compliance requirement as well as change in code and standards

   There are many code agencies such as API, ANSI, NFPA, ASME, CPPS who publish new standards or recommended practice timely and sometimes it is difficult for an operating facility to be aware and regularly verify compliance against those codes. For example, it is mentioned in API RP 939-C that "if a refinery introduce new crude feed composition, the past inspection data will be less relevance to predict future corrosion rates". If the TA planning team were aware of this code section, they might have dealt with the mitigation of sulfidation corrosion in a different way. In addition, OSHA do not consolidate list of good practice for a company to utilize during operation, unlike regulators in other country. Therefore, this lack of coordination to code changes does not help operating company to reduce their risk effectively.

7. Redundant coordination/ insufficient communication – many resources within M&R department assess integrity risk of 4-SC piping at different time but none provide a continuous monitor and drive to change.

   From 2002 to 2012, there were many corrosion studies/reviews as well as inspections taking places on 4-SC piping. However, M&R team did not integrate all the information together to assess the situation and did not have a focal point to continuously take action to drive the change. Hence, there was no continuous improvement in 4-SC piping integrity management.

8. Inadequate coordination – multiple regulatory agencies have responsibility for oversight safety aspects of the refineries with overlapping jurisdictions

   Regulatory agencies such as EPA, Cal/OSHA and RISO have oversight responsibilities with overlapping jurisdictions. Some programs belonging to these agencies have similar requirements e.g. RISO/ISO expands requirements base on Cal ARP. However, as multiple agencies with varying authority engage in relatively limited information sharing about regulatory compliance requirements. Therefore, there is no single entity that has a complete picture of the compliance status of a refinery

Overall, this analysis revealed that there are many coordination and communication issues between different functions that had led the Richmond refinery operation to face a greater safety risk. With amount of equipment, degradation factors and other challenges, a complex decision system requires knowledge, adequate data and interaction and flow of information between components in the system to move system into a safer state.

Step 8 – Dynamics and Migration to a High Risk State

In the "Petrochemical world", everyone knows that safety suppose to be the first priority and the company has put a lot of effort to provide management systems and tools to allow employee to operate the refinery safely, but an accident like 2012 refinery fire still occurred. From a system perspective, safety is viewed as an emergence property that emerges from interactions of components in the system. Each component, or division in this refinery case, needs to provide adequate control and sufficient communications and coordination between controllers, and inside of the whole control structure.

According to Rasmussen, most major accidents result from a migration of the system toward reduced safety integrity over time and Richmond Refinery fire case was no exception. Maintaining integrity of miles of piping components in a refinery is acknowledged to be challenging. In addition, CSB made an observation that over time, the use of clamps or temporary repair on various piping sections had become more common in place in the refinery. Besides, there were many inferred contextual factors inside the refinery operation system that the investigation reports did not explicitly mention such as commercial pressure, budget, resource, time constraints, human factors etc.

In order to understand how certain contextual factors, mentioned in each level analysis in step 6, impact the dynamic in safety control function over time, the System Dynamic model [1] is constructed to link the casual and contextual factors as shown in Figure 5.21.

The "Positive" sign in the casual loop means the greater the magnitude of the cause, the greater the effect at the end of the corresponding arrow and vice versa with the "Negative sign"

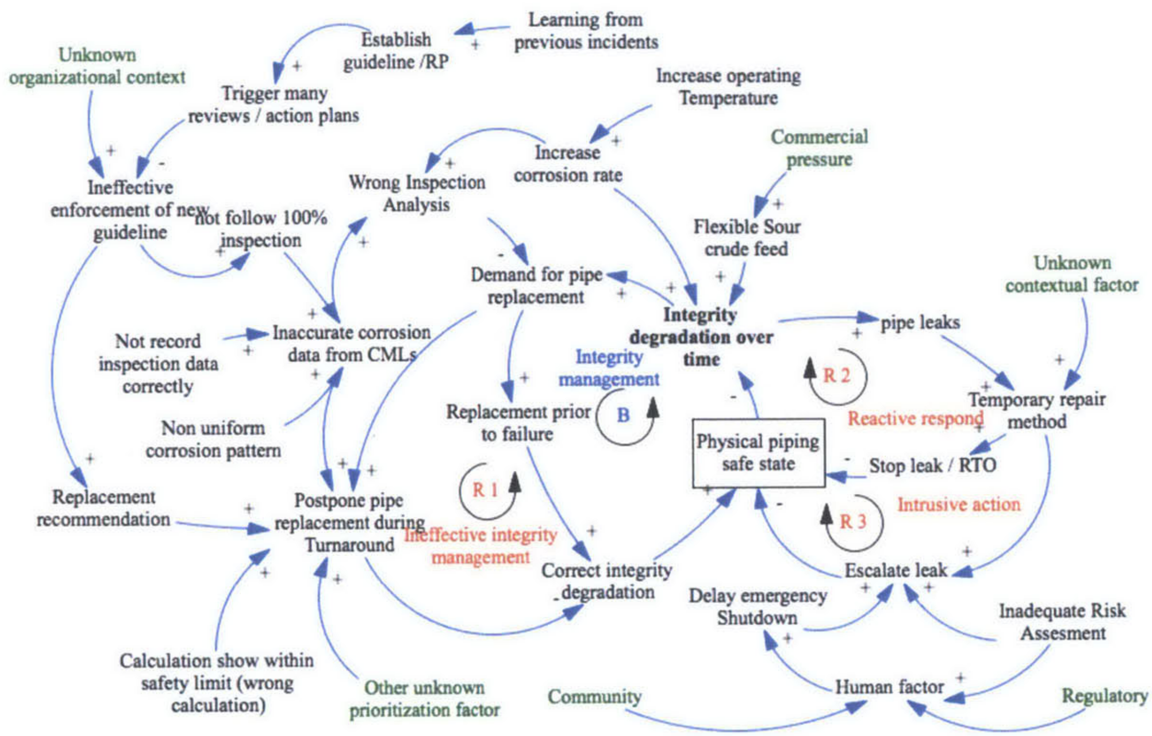

Figure 5.21 Simplified causal model of 4-CU fire accident

Many external disturbances, such as the commercial crude requirements, community perceptions and regulatory pressures, change over time which have direct and indirect impacts on physical equipment and piping safety as well as performance measurement as discussed below:

The balancing control loop labeled *B* or *integrity management* shows how internal reliability system management was designed. However, due to some errors in the corrosion database, as well as the unknown pressure during turnaround planning increasing piping replacements were postponed leading to greater integrity degradation over time and failure before detection as shown in *R1* or *ineffective integrity management* loop. This is a reinforcing loop or unstable system, which is going to reinforce unsafe behavior to the system as the time goes by.

Similarly, the reinforce loop labeled *R2* or *reactive responds* represents some piping failure before the permanent piping replacement is taking place. However, R2 loop still decreases the piping system integrity in a long run because clamp repair method only stops leak temporarily until the plant have time to shutdown and replaces the leaking section.

4-SC piping fall into *R3 or intrusive action,* which due to some unknown contextual factor such as time or resource constraints, it effects the decision of the refinery team. So the team decides to proceed with temporary repair and rushes to conduct an investigation on a lived flow pipe. These unknown contextual factors or pressures as well as the increasing hidden pressures from regulatory and community, which had, impact emergency response decisions and safety state of the refinery and personnel.

In order to understand and prevent the Refinery system operation migrating to states of high risk, the accident investigation model cannot only focus on proximate event and human actions, but must review the entire accident process. Besides, external and internal contextual factors or dynamics will impose pressures onto controllers or workgroups, which will impact their risk assessment process. As Richmond refinery has an intensive decision making process that requires a lot of interactions between various functions as well as information flow. Therefore, accurate information display especially on process safety related and sufficient communication between functions are extremely crucial for each workgroup to perform their work and maintaining effective process safety in operation.

Step 9 – Generate Recommendation

Not having access to refinery documents and unable to interview personnel involved in each function of the safety control structure, it is difficult to generate specific recommendation for the change required. Nevertheless, STAMP/CAST analysis identified the following major control and feedback inadequacies as shown in Figure 5.22

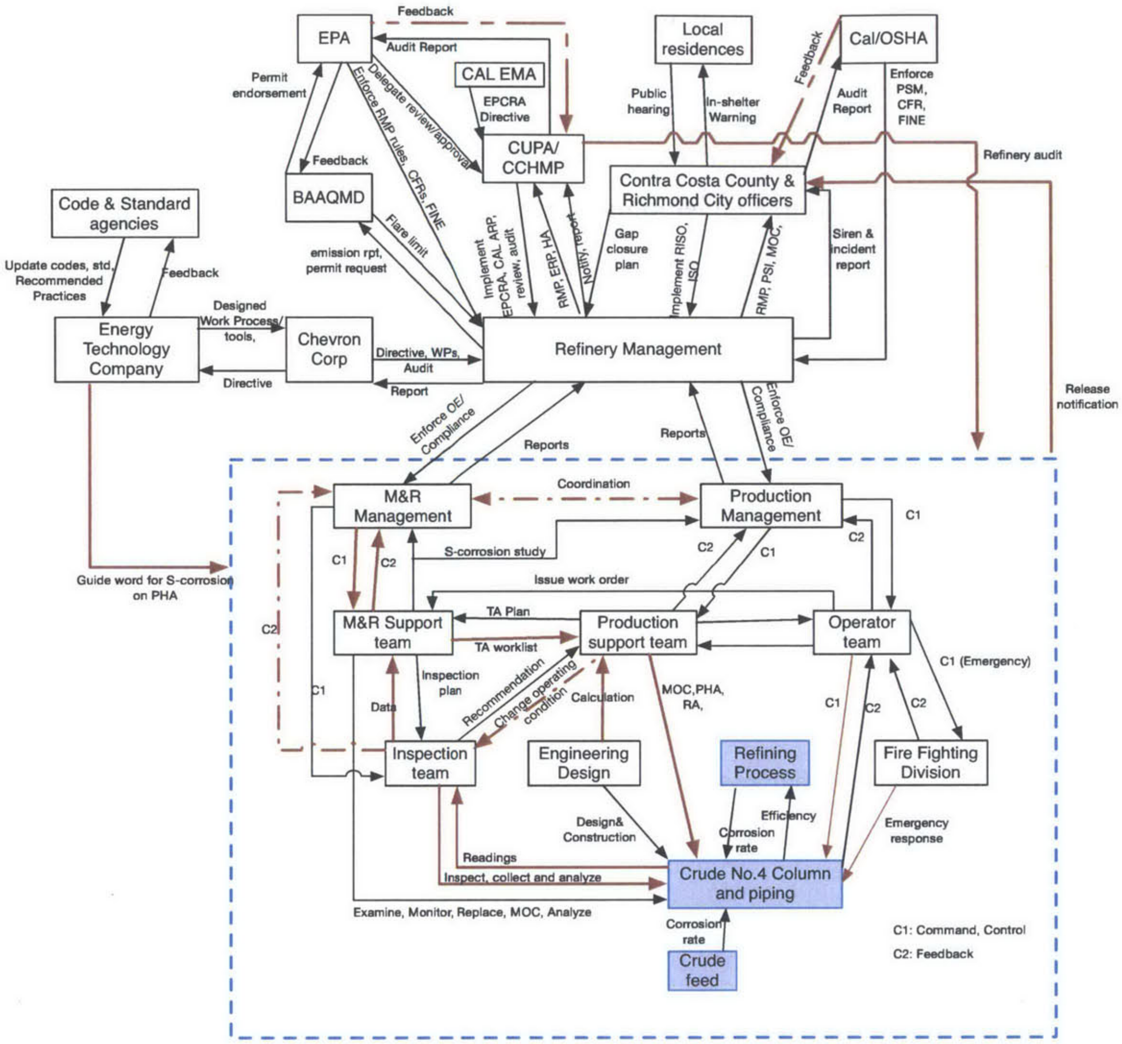

Figure 5.22 Richmond Refinery System inadequate control/ feedback

From Figure 5.22, inadequate controls/feedbacks in the Refinery system, which could not prevent the fire accident and protect local residents from the hazards are grouped into three areas. The recommendations are discussed below: -

<u>Inadequate control/feedback – Inadequate control to maintain piping integrity (4-SC piping)</u>

CAST analysis shows that missing and/or false information were used by controllers in turnaround planning team and emergency response teams. This resulted in decisions that compromised the safety integrity of the refinery. Whilst the Chevron investigation report identified a comprehensive list of recommendations as shown in Table 5.2, CAST identified additional generic recommendations to enhance the Refinery to solve issues of inadequate control/feedback to provide a sustainable solution in the long run.

Chevron Recommendations	Additional recommendations from CAST
(1) Enhance the Refinery's mechanical integrity program to ensure the Refinery properly identifies and monitors piping circuits for appropriate damage mechanisms using a standardized methodology and documentation system.	The Refinery to review the cause of widely uses temporary repair methods in the refinery whether it due to ineffective replacement plan, ineffective execution, insufficient time allocation or potential safety culture issues etc.
(2) Review and enhance the requirements for inspector training and competency.	Maintenance organization to provide a Quality Check on inspection works and enhances transparency and open communication within the organization.
(3) Develop and implement a process for additional oversight of mechanical integrity-related recommendation from industry alerts, ETC, and other subject-matter experts.	Chevron to verify guidelines e.g. Sulfidation corrosion whether it has provided a clear classification that distinguishes between mandatory and recommended requirements or not
(4) Inspection 4CU piping that fall under ETC Sulfidation corrosion guidelines criteria prior to restarting the 4CU.	Refinery to consider providing an audit of their internal work tools relate to PSM e.g. MOC, PHA to ensure quality of reviewing works are maintained which will lead to better communication and coordination of information flow.

Chevron Recommendations	Additional recommendations from CAST
(5) Implement the ETC Sulfidation Inspection Guideline for remainder of the Refinery.	
(6) Ensure relevant technical studies and inspection data are considered for the Refinery's equipment reliability plans and incorporate the recommendations into the ROI/IPR process.	
(7) Ensure Refinery business plan provide the appropriate implementation of Process Safety recommendation (such as the ETC Sulfidation Inspection Guidelines).	Collaborative work between operation managements and commercial to provide sufficient time and resources for executing necessary M&R tasks to alleviate pressure of the working team
(8) Consider additional training on expectation under the "Richmond Refinery Piping Maintenance Guideline" and internal reliability management system and guidelines.	Refinery to ensure cross-functional teams understand the original design basis, changes to current unit conditions (PSI) and risk encounters and utilize PHA and MOC processes effectively.

Table 5.2 Comparison of CAST and Chevron recommendations relate to inadequate control to maintain piping integrity

Inadequate control/feedback – Inadequate control during emergency response

CAST analysis shows that many controllers such as the fire-fighting department, the CCC local officer did not have sufficient information or have information in a timely manner to mitigate the impact from leaking pipe and the fire during the accident. Whilst the Chevron investigation report identified a list of recommendations, CAST provided additional recommendations as shown in Table 5.3

Chevron Recommendations	Additional recommendations from CAST
(1) Revise Refinery policies and checklist to ensure appropriate information including process safety and inspection information is considered when evaluating leaks and addressing the issue of whether to shutdown or continue operation of equipment.	Refinery to provide policy that demands risk assessment and functional involvements to ensure team have sufficient information and understanding of risk involve before making final decision.
(2) Review company/industry loss history on large fractionating tower to determine if internal Engineering Standard adequately addresses mitigation of accidental releases from these systems. Revise the standard as warranted by the findings of this review.	▪ Chevron to verify fire detection and shutdown systems whether they meet company code and industrial best practices. ▪ Refinery to verify why the bottleneck of the incident reporting channel, which resulted in fine penalty failed and provide sufficient control on this element.

Table 5.3 Comparison of CAST and Chevron recommendations relate to inadequate control during emergency response.

Inadequate control/feedback – Inadequate control of regulatory enforcement

CAST analysis shows that many controllers such as the EPA, Cal/OSHA, and local agencies did not have sufficient information or have information in a timely manner to prevent the refinery hazard as well as mitigate the impact of the fire to local residents. Whilst the Chevron investigation report focused on the cause of the leak and the fire inside the refinery, CAST provided additional identification of the inadequate control of components at External Refinery Management level of the structure. The recommendations have been identified in Step 6 and are also listed below:

- CUSA should provide an integrative monitoring capability, such as audit and follow up, to ensure each refinery can optimize the use of internal process and tools to meet and comply with external and internal standard requirements.
- OSHA should provide better review/ quality check on company's PSM and set up appropriate indicators for tracking. In addition, OSHA should evaluate and consolidate list of Recommended Practice, codes and standards for the industry to use as their baseline in their risk management. Additionally OSHA should be proactive in updating its regulations and reflecting on its lessons learnt from audit findings and incident investigations.
- Local agencies including CCHAMP and CCC/RC officers should work together to share resources and information such as status of compliance, requirements under different programs etc. to improve audit quality and maximize resource utilization. In addition, the collaboration will help agents to see the overall status of compliance, which will allow transparent monitoring and update.
- Local officers including CCC/RC should review and improve the effectiveness of the community warning system with adequate monitoring sensors to measure the efficiency of the notifications in different regions. In addition, CCC/RC should increase awareness of local residents on their required actions when they receive / hear different levels of the warning system.
- Regulatory and Code and standard agencies to provide a concise language for the codes and standards on recommended and mandatory practices.

Difficulties to obtain accurate data from inspection	Piping circuit inspections need to include appropriate damage mechanisms using a standardize methodology and documentation system	CAST did not identify inspection technology as a cause for this. However, issue of inspection data were reflected under inspector inadequate control
Physical equipment complied to old code and standard	The leaking line could not be isolated on the upstream side to mitigate loss of containment	Same
Risk assessment and decision making during emergency	The emergency response and assessment after the discovery of the leak did not fully recognize the risk of piping rupture and the possibility of auto-ignition	CAST sees this as a common issue that insufficient information were available to decision makers to make decision and take action. (Discussion under STEP 7 Coordination/ Communication section)
Hazard re-evaluation	The process hazard analysis for 4CU did not consider the potential corrosion due to the high sulfur content of liquid at high temperature and pressure and the low silicon content of the failed carbon steel pipe	Same
Late release notification	None	CAST identifies late notification as one finding where there was a time delay when Chevron formally informed CCC officer after significant release occurred. This resulted in exposure of residents to particulates from refinery fire
Awareness of codes, standards and guideline update	Chevron provides recommendation to provide additional training to inspectors and awareness of PSM to engineers in the refinery.	CAST views the importance of accurate knowledge / information especially on available codes, standard and RP that engineers should have, as it will impact their decision-making.
Delay of Emergency Shutdown	Chevron provides recommendation to revise	CAST identifies a conflicting function of safety critical

Chapter 6 Discussion of CAST Findings and The Application

CAST Findings

Company Crude 4 Unit fire investigators use Taproot method, which is based on the Swiss Cheese Model and identify many crucial findings. However, CAST has identified some additional issues in that will be compared and discussed below in Table 6.1:

Issue	Chevron findings	CAST findings
Wrong calculation of required thickness for normal operating condition	Pipe wall thickness threshold for repair of piping did not incorporate safety factors stated in Chevron's existing guidelines or API RP 574	Same. Inaccurate information was delivered to turnaround planning team leading to the postponement of 4-SC pipe replacement
Inadequate corrosion data available for decision makers	- The 2002 pipe wall thickness testing information was not captured by Chevron's data system - The June 2012 pipe inspection results were not entered in the database and no re-inspection occurred.	Same. CAST identifies that there were no cross check of data collection leading to insufficient corrosion data to support justification of pipe replacement
Review did not request additional 4-SC piping corrosion data collection	The 2009 review of piping circuit did not include a 100% component by component inspection	There had been many corrosion related studies/ reviews since 2002. However, it appeared that the M&R team neither had all pieces of information together nor track status of those recommendations to completion.
No additional corrosion data collected on 4-SC the piping	The 2011 turnaround did not include every component in the 4-SC carbon steel piping connecting the 4CU to atmospheric distillation tower.	Same. CAST inferred some contextual factors during turnaround and turnaround planning such as cost, resource and timing
One-way provision of recommendation	Inspection guidelines of piping were not fully implemented and action items were not tracked until completion	Same

	guideline on circumstance to utilize shutdown functions.	equipment, the flare system, in the refinery, which may have a human factor impact. BBAQMD and local residents see flare as pollution sources and try to reduce this emission. However, it is also used as a safety device during emergency. Therefore, it may be a factor that had delayed emergency shutdown utilization during initial rupture.
Design basis and contextual change	None	CAST identifies a gap in change management when commercial context change resulted in introduction of different crudes. It is inferred that the design basis used crude removal unit as safeguard against sulfidation corrosion on carbon steel piping. However, many process changes such as equipment removal, change in crude compositions were made without adequate review and mitigation actions resulted in high sulfidation corrosion rate on 4-SC.
Regulators and agencies did not provide effective regulation enforcements.	None	Various agencies prescribe regulation; rules for the Refinery to comply, which are rather high-level. However, agencies such as OSHA did not provide detailed consolidated list of codes requirements and inadequate review and feedback of RMP, ERP etc. Besides, most state and federal programs rely on local officer to conduct audits and inspection where there were resource constraints so local officer like CHHAMP could not detect potential

		process safety issues at the refinery.

Table 6.1 Comparison of CAST and Chevron findings

It appears that the recommendations from Chevron were more specific to address mechanical integrity management problems within the refinery. While several of these recommendations do tackle systemic factors, most are strictly focused on the details of this particular incident. Due to the limited information contained in the official investigation report, it was difficult to evaluate why the flawed management control actions and decision making related to the incident occurred at higher levels of the CAST safety control structure. Nevertheless, CAST does help us to find some general issues in the communications or coordination that act as latent conditions. These conditions, which were not explicitly addressed in company investigation report, are:

- Functional conflict of flare – pollutant versus safety
- Coordination and communication across the functions as the company has many processes/tool, information and many decision-makings involves multifunctional team.
- Awareness of updated information on internal and external codes and standards, which also impact the decision-making processes.
- Connection from external system of the refinery and the failure linkages to prevent an accident.

The Applications

So far, CAST has helped us to analyze the causal factors relate to the Richmond fire accident from the whole socio-technical system through the control structure. In Chapter 5, the CAST model helps identify inadequate controls of each component inside the control structure, from physical level to management and regulators, to overall communication and coordination of the Richmond Refinery system. In order to answer the research question "What could be done differently to understand the causes of accidents and prevent them?" the next part of this thesis will look further into those inadequate control actions identified from CAST to generate early warning signs of control problems.

To develop an early warning sign for the Richmond Refinery fire accident, the hazard analysis method based on the STAMP model--STPA will be used in continuation from CAST analysis. As CAST analysis in Chapter 5 already identified safety control structures relating to this accident, we already have information on how the controller controls the process one level below, and how the controlled process provides feedback to the controller. For demonstration purpose, a control function relate to the Inspector will be used in STPA analysis to show how inconsistent information along the control loops and process model can impact the behavior of the controllers. The control function chosen is the interaction between inspector- M&R engineer – Physical piping as shown on Figure 6.1.

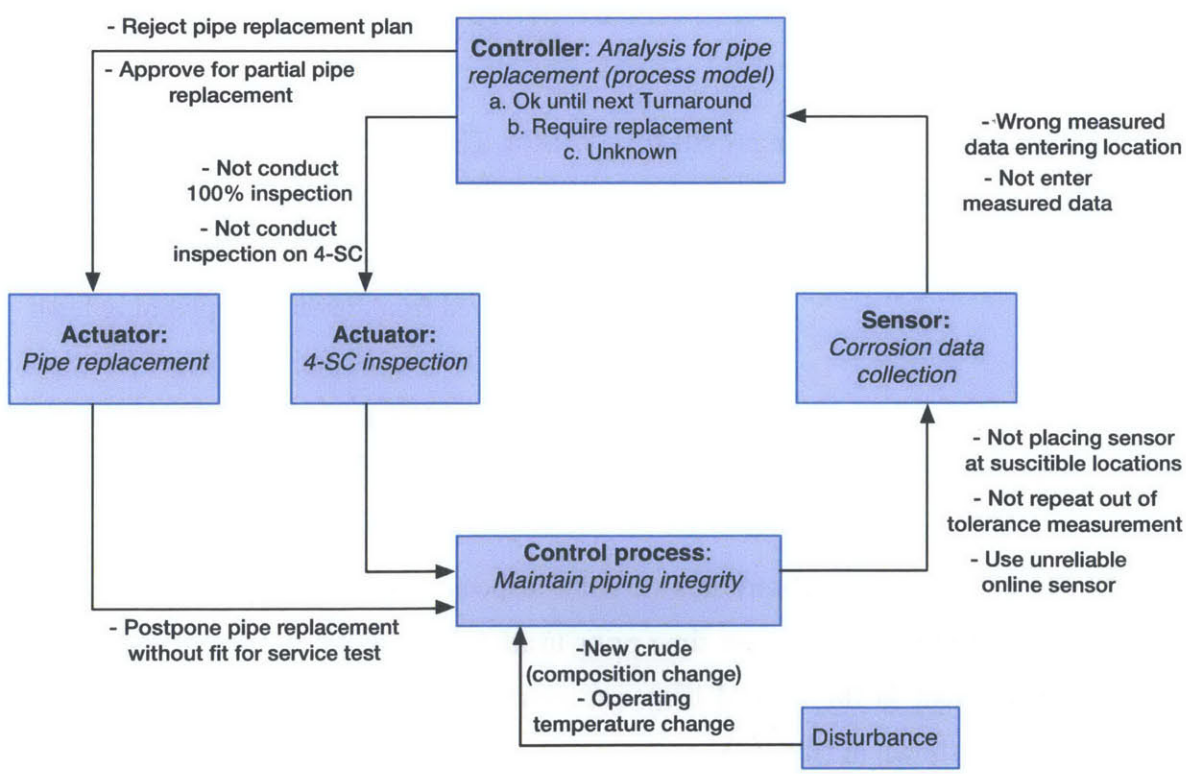

Figure 6.1 Control structure of piping replacement process

From the above control structure, the next step is to identify inadequate control action (ICA) types as well as safety constraints for this control system The possible categories of inadequate control actions from CAST can be converted into STPA, falling in four general categories as table 6.2 shows.. The inadequate control actions are then restated to define the safety constraint. Safety constraints define the conditions that if proceed could potentially allow the pipe to enter into a hazardous state

Inadequate control actions	Safety constraints
ICA1. S-Corrosion identification was not provided	SC1. 100% piping component-by-component inspection should be provided on 4-SC piping
ICA2. S-Corrosion identification was provided incorrectly	SC2. Monitoring systems should be placed on low silicon content section and using reliable measurement method.
ICA3. Piping replacement provided but partially	SC3. Piping replacement should be provided to highly corroded sections
ICA4. Piping replacement not provided	SC4. The need for piping replacement should be identified. SC5. Piping replacement should be approved from turnaround planning team SC6. Deferral of piping replacement should be verified by fit-for service test

Table 6.2 Inadequate Control Action (ICA) and Safety Constraints (SC)

The main action of both controllers (i.e. the inspector and Engineer) is to detect pipe deterioration and replace pipe on time prior to its failure. The next step is to determine how each element in the control loop can contribute to the system level hazard. This examination is shown in table 6.3

Safety Constraints	Flaw	Feature of sensor	Warning Signs
SC1, SC2, SC4 and SC5	Not conduct 100% component by component inspection	1) Should able to match number data points against number of pipe components of that pipe circuit.	Not enough data points entered into corrosion database
SC1, SC2, SC4 and SC5	Not conduct inspection on 4-SC	1) Should be able to raise alert on the missing inspection action on high priority piping	No data entry of high priority pipe sections
SC3, SC4	Not able to identify severe corrosion	1) Should be able to see the non uniformity of inspection data obtained 2) Should compare location of CMLs against S-Corrosion guideline	Uniform reading trends on high S-Corrosion circuit
SC2, SC4, SC5	Not using an accurate measuring method	1) Should notice a great deviation in reading, e.g. high standard deviation than mean.	Great variation of readings from the same measurement location
SC2, SC4	Not repeat out-of-tolerance measurements	1) Should be able to detect and raise alert on out-of-range reading.	Out of range readings on corrosion database
SC2, SC4	Utilize unreliable online monitoring sensor for continuous monitoring	1) Should notice a great deviation in reading, e.g. high standard deviation than mean.	Great variation of readings from the same measurement location
SC2, SC3, SC4, SC5	Enter measured data incorrectly to corrosion database (2002)	1) Should conduct independent sample check or verification of available data in database	No calculation data available on completed jobs.
SC2, SC3, SC4, SC5	Enter incomplete measured data into corrosion database	1) Should conduct independent sample check or verification of	No calculation data available on completed jobs.

Safety Constraints	Flaw	Feature of sensor	Warning Signs
SC4, SC5, SC6	Not conduct fit-for-service test on pipes with postponed replacement	1) Should have visual tag to indicate need for fit-for-service test on pipe scheduled for replacement but yet to be conducted	No document record to confirm results of fit for service
SC3, SC4, SC5	Reject pipe replacement proposal	1) Should be able to track life-cycle status of each pipe section	Backlog of piping replacement. Many clamps on site.
SC3, SC5	Partially replaced corroding 4-SC pipe	1) Should be able to track life-cycle status of each pipe section	Backlog of piping replacement. Many clamps on site.
SC2, SC4, SC6	Not identify impact from change in operating temperature of 4-SC	1) Should be able to see constant corrosion rate used against various process condition changes	Use of constant corrosion rate under different process conditions
SC2, SC4	Not identify impact from change in sulfur composition in crude feed	1) Should be able to see constant corrosion rate used against various process condition changes	Many change to process conditions but use constant corrosion rate
SC2, SC4	Infrequent piping inspection period (once every 4-5 years)	1) Should be able to have online monitoring of corrosion data available	Reading data that shows a significantly greater than predicted change in reading data can indicate need for more frequent inspection

Table 6.3 Flaw, features and warning sign of pipe integrity deterioration

If this STPA analysis is applied to other component within the system, a set of early warning signs can be developed and compared against leading indicators that are currently used in the refinery. This would help the refinery to utilize pragmatic sign to show actual status or process safety risk of each barrier within the refinery.

Chapter 7 Conclusion

Although current root cause analysis methods derived from the Swiss cheese model address accident causal identifications, not all the contributing factors are always fully addressed. In this study a more systematic approach using CAST-STAMP was applied to a refinery accident aimed at uncovering systemic factors that contributed to the fire accident. In the Richmond Refinery accident analyzed in Chapter 5, the CAST-STAMP model helped identify more inadequate controls inside of the control structure, including physical process, management, overall communication and coordination and the dynamic migration to higher risk, which is potentially associated with the safety culture of the refinery. From the CAST analysis, we are able to identify previously missed inadequate controls and needed improvements in the following areas:

1. *Physical Process Analysis*: Changing in feed composition, although overall sulfur composition stays within the original design limit, not only a review on operational impact should be considered but the impact to overall life cycle of equipment/ piping system including maintenance needs to be examined. As one example, when production introduced new crude into the 4CU, an inspector was not notified and hence did not adjust the corrosion rate use in piping life prediction. After the CAST analysis, we understand how the linkage of these inadequate controls at physical level to the higher level controls that contributed to the accident.

2. *System Interactions Analysis*: By employing a dysfunctional interactions analysis of the Refinery System Operation, we discovered that both the possession of inaccurate information within teams and insufficient communication of information between working teams contributed to inadequate safety control action of each team as well as in group decisions. We believe the Refinery management needs to further investigate gaps in existing Management of Change and Risk Assessment processes to improve these interface issues.

3. *Contextual Factor Analysis*: Identifying these contextual factors in STAMP, we understand the potential impact that each contextual factor may have provided to each functional team of the safety control structure. This not only contributed to our understanding of the accident, it also provided important insights when looking into dynamic migration to higher risk state where further examination can be provided to determine appropriate policies to improve safety performance of the refinery operating system.

4. *Refinery System Operation and External Refinery System Management Analysis*: From the CAST analysis, we discovered potential conflicts between safety and social/ regulatory pressure, which might have impacted decisions at operational level during the emergency. In addition, the overlap of prescriptive regulatory enforcements and inadequate communication between agencies did not provide adequate safety control for the community because of ineffective reviews, audit and inspection efforts. We recommended establishing more integrative work between agencies so they can oversee and are aware of the safety status of the refinery more effectively.

5. *Overall Communication and Coordination Analysis*: From the CAST analysis, we were able to identify the missing communications and inadequate communication from both within each system and between the refinery system operation and the external refinery system management. In order for the safety control of these systems to be improved accurate information in a timely manner needs to be transferred between related teams to perform their control actions and facilitate decision-making.

6. *Warning sign generation*: Within the CAST analysis, we discussed dynamic migration of refinery equipment into higher risk states where the piping integrity was compromised. There were many safety-warning signs from the Refinery prior to the accident and STAMP-STPA analysis can be used to demonstrate how inadequate control actions can generate the warning signs. If a full analysis is performed, the findings from this STPA-EWASAP analysis can then be used to verify against current process safety indicator that the Refinery uses.

In summary, the CAST accident analysis provides us insight into how inadequate control can happen within the safety control structure, how the contextual factor and wrong process model can impact the behavior of the controllers and migrate the system towards an unsafe state. CAST identified several important system control/feedback inadequacies, and associated recommendations to resolve these inadequacies within the refinery system operation and external refinery system management that were not documented in the Chevron's investigation findings and recommendations. In addition, the STPA-based modeling can be used as a basis for developing the safety integrity deterioration warning sign as it treats safety as control problem, and it addresses the systemic aspects thoroughly. In order to answer the research question "What could be done differently to understand the causes of accidents and prevent them?" the analysis contained herein, this thesis concludes:

- The Richmond Refinery and agencies should implement all 15 of the recommendations contained in Step 9 of the CAST analysis (see Chapter 5 of this thesis) in order to address systemic issues resulting in system hazards that contributed to the Crude No.4 Unit Richmond Refinery Fire.
- The STAMP/CAST model is more comprehensive than the 'Swiss Cheese' model at identifying accident causality.
- The preliminary work in STPA only focuses on the maintaining piping integrity part of the system. Further work can be done to other team, to generate warning signs and compare against current process safety indicators associated with the refinery. This will provide additional effective safety indicators for the industry.

Using current accidental model analysis and process safety indicator practices may result in a decent safety performance. However, better safety performance can be achieved by focusing on systems aspects of the accidents to reduce systemic issues and provide a robust information interface to build an effective safety control model to stop the dynamic migration to higher risk state and catastrophic accident from occurring.

References:

[1] Reason, James. Human Error. New York: Cambridge University Press. 1990

[2] UK HSE. Guidance on Risk Assessment for Offshore Installations. Offshore Information Sheet No.3/2006

[3] OGP. Process safety – Recommended Practice for Key Performance Indicators. United Kingdom: Report number 456. November 2006

[4] UK Health and Safety Executive. Develop Process Safety Indicators. United Kingdom: Crown press. 2006

[5] CUSA Richmond investigation team. Richmond Refinery 4 Crude Unit Incident. Richmond: Chevron. April 2013

[6] Leplat, Jacques, Rasmussen, Jens, Duncan, Keith. Occupational Accident Research and Systems Approach. New Technology and Human Error, 181-191. New York: John Wiley & Sons. 1987.

[7] U.S. Chemical Safety and Hazard Investigation Board. Interim Investigation Report Chevron Richmond Refinery Fire. CSB. April 2013

[8] Hassan, Mohamed. Modeling an Oil Drilling Total Productive Maintenance System Using Casual Loop Diagram Simulation. Okahoma: International Journal of Technology, December 2012

[9] Anamet, Inc. Metallurgical Evaluation of Samples from the Chevron U.S.A. Inc., Richmond #4 Crude Unit 8-Inch and 12-Inch 4-Sidecut Piping Involved in the August 6, 2012, Hydrocarbon Release and Fire. Prepared for: The Chemical Safety and Hazard Investigation Board (CSB), February 11, 2013.

[10] Steve Wildman. "7th update to 30-day report to CWS level 3 event of August 6, 2012" Prepared for: Contra Costa Health Service (CCHS), April 12, 2013

[11] U.S. Chemical Safety and Hazard Investigation Board. Interim Regulatory Report for Chevron Richmond Refinery Fire. CSB. Dec 2013

[12] Ramo, Simon. In system concept: Lectures on Contemporary Approaches to System. 13-32. New York: John Weiley & Sons. 1973

[13] Leveson, Nancy. Engineering a Safety World – System Thinking Apply to Safety. Cambridge: MIT press. 2011

[14] Leveson, Nancy. ESD Working Paper Series - A Systems Thinking Approach to Leading Indicators in the Petrochemical Industry. Cambridge: MIT

[15] Dokas, Ioannis M. Feehan, John. Imran, Syed. EWaSAP: An early warning sign identification approach based on a systemic hazard analysis. Ireland: Safety Science 58, 11-26. 2013

[16] Sterman, John D. Business Dynamics - Systems Thinking and Modeling for a Complex World. Irwin McGraw-Hill, 2000.

[17] Reason, J. T. Managing the risks of organizational accidents. Aldershot, UK: Ashgate Publishing Limited, 1997

[18] EUROCONTROL Experimental Centre. Revisiting the Swiss cheese model of accidents. EEC Note No. 13/06

[19] The American Petroleum Institute. Process Safety Performance Indicators for the Refining and Petrochemical Industries, ANSI/API 754, First Edition, April 2010.

[20] Dulac, N. A framework for Dynamic Safety and Risk Management Modeling in Complex Engineering System. Dept. of Aero, Astro. MIT Cambridge, 2007

[21] Dokas, Ioannis M. Feehan, John. Imran, Syed. EWaSAP: An early warning sign identification approach base on STPA presentation slide. Ireland. Cork Constraint Computation Centre, University College Cork, 2012

[22] The Health and Safety Executive. Temporary/permanent pipe repair – Guidelines Offshore Technology Report, 2001/038

[23] Khawaji, Ibrahim A. Developing System-Based Leading Indicators for Proactive Risk Management in the Chemical Processing Industry Thesis. MIT. June 2012

[24] Leveson, Nancy, Stringfellow, Margaret and Thomas, John. A Systems Approach to Accident Analysis paper. MIT. 2009

[25] American Institute of Chemical Engineers, Center for Chemical Process Safety Center of Chemical Process Safety, *Guidelines for Risk Based Process Safety*. New Jersey: Wiley & Sons. 2007.

[26] American Institute of Chemical Engineers, Center for Chemical Process Safety Center of Chemical Process Safety, Process Safety Leading and Lagging Metrics. 2008.

[27] American Institute of Chemical Engineers, Center for Chemical Process Safety Center of Chemical Process Safety, *Guidelines for Process Safety Metrics*. New Jersey: Wiley & Sons, 2010.

[28] Cal/OSHA Process Safety Management District Office. Citation and Notification of Penalty to Chevron U.S.A. Inc. Richmond: Inspection Number 314331877. January 2013

[29] https://www.osha.gov/Publications/osha3133.html

[30]http://yosemite.epa.gov/opa/admpress.nsf/2dd7f669225439b78525735900400c31/3056d9f3089d69d9852570d8005e13f5!OpenDocument&Highlight=2,fines,refinery

[31] http://www.sfgate.com/bayarea/article/EPA-cites-62-Richmond-violations-by-Chevron-5072914.php

[32] http://richmond.chevron.com/home/environmentandsafety/safetyandhealth.aspx

[33] http://en.wikipedia.org/wiki/Chevron_Richmond_Refinery

[34] http://www.baaqmd.gov/Divisions/Planning-and-Research/Rules-and-Regulations.aspx

[35] http://www.csb.gov/chevron-refinery-fire/

[36] http://richmondpulse.org/richmond-and-chevron-a-story-of-love-and-hate/

[37]http://www.sfgate.com/bayarea/article/Richmond-air-quality-safe-analysis-says-3774298.php#ixzz234ZJxrRt

[38] http://www.sfgate.com/bayarea/article/Refinery-warning-worked-mostly -
3770326.php#ixzz234fjVlFd

[39] http://www.chevron.com/documents/pdf/OEMS_Overview.pdf

[40] http://www.chevron.com/about/operationalexcellence/managementsystem/