Universidad Politécnica de Madrid

Escuela Técnica Superior de Ingenieros Industriales

Metodología para la Medición del Nivel de Seguridad
en la Industria de Procesos

Tesis Doctoral

Abouzar Yousefi, Master of Science

2020

Ingeniería Química Industrial y del Medio Ambiente,
Escuela Técnica Superior de Ingenieros Industriales

Metodología para la Medición del Nivel de Seguridad
en la Industria de Procesos

‘Methodology to Measure Safety Level in the
Process Industry’

Abouzar Yousefi, Master of Science

Professor Manuel Rodríguez Hernández

2020

Table of Contents

Table of Contents	3
List of tables	6
List of figures	7
Resumen.....	10
Abstract	15
Chapter 1: Introduction	20
1.1. Objective	25
Chapter 2: Accident Causation Models, Hazard Identification and Risk Assessment Techniques ..	27
2.1 Domino theory	27
2.2 Loss Causation Model or ILCI Model	29
2.3 Multiple causation theory	30
2.4 Multilinear events sequence model	30
2.5 Time sequence model.....	31
2.6 Accident Evolution and Barrier Function (AEB) model	32
2.7 Energy damage models	33
2.8 Epidemiological Theory	34
2.9 Management Oversight and Risk Tree (MORT).....	36
2.10 Swiss cheese Model	37
2.11 Bowtie	42
2.12 SHIPP	43
2.13 Rasmussen framework or AcciMap	46
2.14 FRAM	49
2.15 STAMP	51
2.16 Conclusion.....	53
Chapter 3: Systems-Theoretic Accident Model and Processes (STAMP)	55
3.1. Introduction	55
3.2. STAMP: an accident model based on systems theory	65
3.2.1. The central role of constraints in system safety	66
3.2.2. Control loops and process models.....	69

3.2.3.	Sociotechnical levels of control	71
3.2.4.	A classification of accident factors	73
Chapter 4:	Techniques and tools based on STAMP	77
4.1.	CAST.....	77
4.2.	STPA	79
Chapter 5:	Case Study: Analyzing Chevron Richmond Refinery Accident with AcciMap, FRAM and CAST.....	83
5.1.	Chevron Richmond Refinery Accident description	83
5.2.	Chevron Richmond Refinery Accident analysis using CAST model.....	88
STEP 1:	Identify the system(s) and hazard(s) involved in the loss	88
STEP 2:	Identify the system safety constraints and system requirements associated with that hazard	89
STEP 3:	Document the safety control structure in place to control the hazard and enforce the safety constraints	89
STEP 4:	Determine the proximate events leading to the loss	93
STEP 5:	Analyze the loss at the physical system level	93
STEP 6:	Moving up the levels of the safety control structure, determine how and why each successive higher level allowed or contributed to the inadequate control at the current level..	96
STEP 7:	Review contributions of coordination or communication failures.....	121
STEP 8:	Determine the dynamics and changes in the system and the safety control structure relating to the loss and any weakening of the safety control structure over time.....	122
STEP 9:	Generate recommendations.....	124
5.3.	Chevron Richmond Refinery Accident analysis using FRAM method	125
5.3.1	Creating FRAM Model – Functions and aspects	126
5.3.2	Analysis – Instantiation.....	132
5.3.3	Recommendations	134
5.4.	Chevron Richmond Refinery Accident analysis by CCPS using AcciMap method	135
5.5.	Discussion	138
Chapter 6:	Case Study: Applying STPA on a process plant and comparing the outcome with the result of HAZOP	142
6.1.	Process plant description	143
6.2.	Application of STPA.....	144
6.2.1	Define purpose of the analysis	144

6.2.2	Model the control structure	145
6.2.3	Identify Unsafe Control Actions	146
6.2.4	Identify Loss Scenarios	148
6.2.5	Discussion and Conclusion	175
Chapter 7: A methodology to measure safety level in process plants		179
7.1.	Introduction and background	179
7.2.	Theory behind the methodology	186
7.3.	The methodology and its application in a process plant.....	188
Chapter 8 Conclusions		220
Appendix I HAZOP Study of the process plant under study		224
References.....		227

List of tables

Table 1 “Contain the fluid” function and its aspects.....	133
Table 2 Summary of comparison made between recommendations generated by AcciMap, FRAM and CAST	138
Table 3 A list of guide words, parameters and examples of deviations	142
Table 4 A model of HAZOP sheet	142
Table 5 Identified Unsafe Control Actions	147
Table 6 Defined constraints on the behavior of controllers	147
Table 7 Identified loss scenarios for UCAs	149
Table 8 Identified further loss scenarios for control actions	153
Table 9 Safety measure recommended by STPA	153
Table 10 STPA recommendations using general control structure.....	158
Table 11 Identified Unsafe Control Actions from the refined control structure	159
Table 12 Controller constraints of the UCAs for air cooler and separator	161
Table 13 Loss Scenarios of the UCAs for air cooler and separator	162
Table 14 Safety measures recommended by STPA for the detailed control structure	168
Table 15 STPA recommendations using refined control structure of air cooler and separator	174
Table 16 Recommendations generated by STPA using general control structure and refined control structure of air cooler and separator	175
Table 17 Recommendations generated by HAZOP for air cooler and separator.....	177
Table 18 Safety levels and corresponding values established for acceptability criteria.....	188
Table 19 Defined safety checkpoint for loss scenario/safety measure at general control structure level	188
Table 20 Defined safety checkpoint for loss scenario/safety measure at refined control structure level	196
Table 21 The final list of safety checkpoints (The list of consolidated safety checkpoints)	207
Table 22 Number of loss scenarios related to each safety checkpoint for general control structure	209
Table 23 Number of loss scenarios related to each safety checkpoint for refined control structure	209
Table 24 Number of loss scenarios and weighing related to consolidated safety checkpoint of the final list	210
Table 25 Indicator, acceptability criteria and safety levels for each safety checkpoint of the final list	212
Table 26 Determined safety level of plant safety checkpoint.....	213
Table 27 Summary of the status (safety level) of each checkpoint	217

List of figures

Figure 1 Accident model classification proposed by (Xie Xuecai, Li Zonghan, & Ge Ying, 2020)	23
Figure 2 Heinrich Domino Theory (Heinrich, 1931)	28
Figure 3 Loss causation model (Bird & Germain, 1985)	30
Figure 4 Petersen's Multiple causation theory (Petersen D. , 1971)	30
Figure 5 multilinear events sequence model (Benner, 1975)	31
Figure 6 Generalized Time Sequence Model (Viner, 1991)	32
Figure 7 Graphical representation of the AEB-model. Failures, malfunctions and errors are located as error events in the boxes (Svenson, 2000)	33
Figure 8 Haddon's 10 accident prevention strategies	33
Figure 9 The Energy Damage Model based on (Viner, 1991)	34
Figure 10 A generic epidemiology	35
Figure 11 Johnson's three levels that represent different types of factors (Leveson N. G., 2001)	35
Figure 12 Arrangement of elements of Atwood's model (Attwood, Khan, & Veitch, 2006)	36
Figure 13 Reason's five levels of controls	38
Figure 14 Reason's representation of accident causation	39
Figure 15 Reason's updated representation of accident causation	40
Figure 16 Reason's accident model (Reason, Managing the risks of organizational accidents, 1997)	41
Figure 17 A typical bowtie and the relationships between its elements (CGE Risk Management Solutions, 2019)	43
Figure 18 Conceptual offshore oil and gas process accident model proposed by (Kujath, Amyotte, & Khan, 2010)	43
Figure 19 System hazard identification, prediction, and prevention (SHIPP) methodology (Rathnayakaa, Khana, & Amyotte, 2011)	45
Figure 20 The process accident model developed by Rathnayakaa et al. (Rathnayakaa, Khana, & Amyotte, 2011)	46
Figure 21 The socio-technical system involved in risk management (Rasmussen J. , Risk Management in a Dynamic Society: A Modelling Problem, 1997)	47
Figure 22 Under the presence of strong gradients, behavior will very likely migrate toward the boundary of acceptable performance (Rasmussen J. , Risk Management in a Dynamic Society: A Modelling Problem, 1997)	48
Figure 23 Hexagonal function representation (Hollnagel & Goteman, 2004)	50
Figure 24 Functions and coupling	51
Figure 25 General form of a model of sociotechnical control (Leveson N. G., 2012)	52
Figure 26 A chemical reactor design (Leveson N. G., 2004)	61
Figure 27 A typical control loop and the process models involved (Leveson N. G., 2004)	70
Figure 28 Two Types of Coordination Problems (Leveson N. G., 2004)	75
Figure 29 Overview of the basic STPA Method (Leveson & Thomas, 2018)	81
Figure 30 Photo taken of the leaking 4-sidecut pipe on August 6, 2012, at the Chevron Richmond Refinery. Insulation obscured the actual leak location. Stain signifies where hydrocarbon process fluid was leaking from the 4-sidecut piping	84

Figure 31 Timeline of events on August 6, 2012.....	85
Figure 32 Photo of the burned remains of the fire truck that was consumed by the fire. A firefighter was in the cab when the light gas oil ignited. The fire truck was positioned in the cold zone approximately 65 feet from the leak location.....	87
Figure 33 Initial vapor cloud formation (white cloud) and subsequent ignition (black smoke) as seen from a pier in San Francisco, California	88
Figure 34 Richmond Refinery safety control structure	90
Figure 35 summary of loss analysis at the physical system level	96
Figure 36 Operator team level analysis.....	97
Figure 37 Firefighting team level analysis	99
Figure 38 Operation support team level analysis	101
Figure 39 Reliability and Maintenance Support team level analysis	103
Figure 40 Inspector level analysis.....	105
Figure 41 Operation management level analysis	107
Figure 42 Reliability and maintenance level analysis	108
Figure 43 Refinery management level analysis	110
Figure 44 Energy Technology Company (ETC) level analysis	112
Figure 45 Corporate management level analysis	113
Figure 46 Codes and standard agencies level analysis.....	115
Figure 47 Bay Area Air Quality Management District (BAAQMD) level analysis	116
Figure 48 Richmond City and Contra Costa Health Service's Hazard Material Program (CCHMP) level analysis	117
Figure 49 Cal/OSHA level analysis	118
Figure 50 EPA level analysis	120
Figure 51 FRAM model developed to analyze the Chevron refinery accident.....	132
Figure 52 AcciMap of the Chevron accident (U.S. Chemical Safety and Hazard Investigation Board (CSB), Final Investigation Report, Report No. 2012-03-I-CA, 2015).....	137
Figure 53 A train of air cooler and separator	143
Figure 54 Safety Control Structure of the gas plant.....	146
Figure 55 Detailed Safety Control Structure for air cooler and separator.....	159
Figure 56 Effects of failure in terms of time to a Top Event (Knegtering & Pasman, 2013)	182
Figure 57 Operational safety improvement cycle (Maroño, Pena, & Santamaria, 2006)	183
Figure 58 The formula to obtain the 'PROCESO' index value (Maroño, Pena, & Santamaria, 2006)	184
Figure 59 Procedure followed to develop the 'PROCESO' index (Maroño, Pena, & Santamaria, 2006)	184
Figure 60 Process Safety Indicator Pyramid	185
Figure 61 Number of loss scenarios related to each safety checkpoint.....	212
Figure 62 A gauge designed to demonstrate the safety level of the plant.....	216
Figure 63 Pie chart of the overall safety status of the process plant and each safety checkpoint ...	218
Figure 64 Overall safety status of the process plant in a tape type meter	219

Resumen

Muchos accidentes graves como Flixborough (1974), Seveso (1976), Bhopal (1984), Piper Alpha (1988), Exxon Valdez (1989), Pasadena (1998), Longford (1998), Toulouse (2001), Petrobras P36 (2001), Buncefield (2005), Texas City (2005), Deep Water Horizon - Macondo (2010) sucedió en la industria de procesos en las últimas décadas con múltiples muertes, impactos ambientales significativos y pérdidas financieras.

En respuesta a la mayoría de estos accidentes, se produjeron muchos cambios y mejoras en las regulaciones, organizaciones y aspectos técnicos con la intención de prevenir este tipo de accidentes o mitigar sus consecuencias. Por ejemplo, en Europa, el accidente de Seveso (1976) impulsó la adopción de una legislación sobre prevención y control de accidentes graves (Directiva 82/501/CEE) que se denominó Directiva Seveso. En el Reino Unido, el accidente de Piper Alpha (1988) reformó por completo el régimen de seguridad en alta mar. Una de las principales recomendaciones llevó al Reglamento de Instalaciones Offshore (Safety Case).

Las empresas involucradas en la industria de procesos hacen muchos esfuerzos para prevenir y controlar accidentes graves. Realizan varios estudios de seguridad y actividades en diferentes etapas durante la vida de una planta de proceso. Identificación de peligros (HAZID), análisis BowTie, análisis funcional de operatividad (APO o HAZOP), estudio de nivel de integridad de seguridad (SIL), modelado de incendio, explosión y explosión, análisis cuantitativa de riesgos (ACR o QRA), evaluación de impacto ambiental, social y de salud (ESHIA), plan de respuesta ante emergencias (ERP), plan de respuesta ante derrames de hidrocarburos, revisión de seguridad previa a la puesta en marcha, auditorías de seguridad de la planta, inspección basada en riesgos y mantenimiento preventivo y predictivo, gestión del cambio, permiso para trabajar, análisis de seguridad de trabajo y evaluación de riesgos operativos son ejemplos de estudios y actividades realizadas por empresas durante el diseño, construcción, comisionado, puesta en marcha y operación.

A nivel de la industria, se han producido muchos avances en la tecnología, materiales, instrumentación y control, diseño y comunicación. A pesar de las modificaciones regulatorias, los esfuerzos por parte de las empresas y los avances tecnológicos, los accidentes graves continúan ocurriendo en la industria de procesos y a menudo tienen consecuencias graves. Esto ha generado preocupaciones sobre la gestión de la seguridad y ha resaltado problemas en el pensamiento científico sobre la seguridad. El pensamiento actual sobre cómo ocurren los accidentes y los sistemas de gestión basados en eso, aunque razonablemente exitoso, no hace posible que la industria de proceso logre la meta de cero accidentes (Ale, et al., 2014). Una de las razones principales es que la mayoría de las técnicas comúnmente utilizadas para la prevención de accidentes, o la definición de requisitos de seguridad a través de estudios de seguridad, se basan en modelos tradicionales de causalidad de accidentes desarrollados hace muchos años.

Existe el argumento de que se han producido cambios significativos en la industria de procesos, pero las técnicas comunes para el estudio de seguridad y la prevención de accidentes no se han actualizado como corresponde. En consecuencia, estas técnicas tradicionales pueden tener limitaciones para identificar los peligros relacionados con la industria moderna de procesos que se caracteriza por ser un entorno sociotécnico complejo.

Leveson indica que se han producido muchos cambios en la industria que hacen que los modelos tradicionales de causalidad de accidentes y las técnicas de ingeniería de seguridad basadas en ellos sean parcialmente efectivos para estudiar plantas complejas modernas (Leveson N. G., 2012):

- El ritmo rápido de cambio tecnológico
- Relaciones más complejas entre humanos y automatización.
- Aumento de la complejidad y el acoplamiento.
- Cambio en la naturaleza de los accidentes.
- Dificultad para seleccionar prioridades y hacer compensaciones
- Nuevos tipos de peligros.
- Disminución de la tolerancia a ni un solo accidente.
- Capacidad reducida para aprender de la experiencia.
- Cambios en regulaciones y visión pública de la seguridad.

Los modelos de causalidad de accidentes han evolucionado con el tiempo y se han introducido diferentes tipos de modelos de causalidad de accidentes. Hay diferentes formas de clasificar los modelos de accidentes. Algunos autores clasificaron los modelos de causalidad de accidentes en modelos secuenciales, epidemiológicos y sistemáticos donde:

- Los modelos secuenciales describen un accidente como una cadena de eventos que ocurren en un orden temporal.
- Los modelos epidemiológicos consideran eventos que conducen a accidentes similares a la propagación de una enfermedad, es decir, como el resultado de una combinación de factores que existen juntos en el espacio y el tiempo.
- Los modelos de accidentes sistémicos se basan en la teoría de sistemas y tratan de describir el rendimiento de un sistema en su conjunto, en lugar de en la relación específica de causa-efecto o incluso factores epidemiológicos.

Los modelos secuenciales y epidemiológicos se consideran como modelos tradicionales, mientras que los modelos sistémicos se consideran como modelos modernos. Uno de los primeros modelos de causalidad de accidentes es la teoría de Heinrich Domino que describe un accidente como una cadena de eventos. Fue actualizado por varios investigadores a lo largo de los años y puede considerarse como el origen de modelos secuenciales. La mayoría de las técnicas tradicionales, como el Análisis de modos y efectos de falla (FMEA), Análisis de árbol de fallas (FTA), Análisis de árbol de eventos y Análisis de causa y consecuencia, están basados en modelos secuenciales (Leveson N. , 1995).

Los modelos tradicionales funcionan bien para pérdidas causadas por fallas de componentes físicos o errores humanos en sistemas relativamente simples. La tecnología moderna ha cambiado significativamente la naturaleza de la industria y el trabajo humano de tareas principalmente manuales a predominantemente actividades intensivas en conocimiento. En consecuencia, la contribución humana a los accidentes ha cambiado del error humano al factor humano, que es más que un simple error cometido por una persona. Además, los modelos tradicionales no capturan completamente la dinámica y las interacciones no lineales entre los componentes del sistema en sistemas socio-técnicos complejos.

Los modelos sistémicos tienen sus raíces en la teoría de sistemas. La teoría de sistemas incluye los principios, modelos y reglas necesarias para comprender las complejas interrelaciones e interdependencias entre componentes (técnicos, humanos, organizacionales y de gestión) de un sistema complejo. El marco socio-técnico jerárquico de Rasmussen llamado AcciMap (Rasmussen J. , 1997), el modelo de accidentes de resonancia funcional (FRAM) de Hollnagel (Hollnagel E. , 2004) y el modelo de accidente y procesos de teóricos de sistemas (STAMP) de Leveson (Leveson N. G., 2004) son modelos notables sistémicos que intentan modelar sistemas socio-técnicos complejos.

El análisis causal basado en STAMP (CAST) y el análisis del proceso de teórico de sistema (STPA) son técnicas desarrolladas basadas en STAMP. CAST es una técnica de análisis de accidentes y STPA es una técnica de identificación de peligros. En este trabajo, CAST se utiliza para analizar un accidente ocurrido en la industria de procesos, el accidente de la Refinería Chevron 2012, y el resultado se compara con los obtenidos por AcciMap y FRAM. Además, STPA se utiliza para estudiar los peligros de una planta de proceso y el resultado se compara con el resultado de HAZOP de la planta como una técnica tradicional. STAMP parece ser uno de los modelos de causalidad de accidentes más apropiados para manejar sistemas complejos.

En este trabajo, los autores intentaron encontrar una solución basada en STAMP para la medición proactiva del nivel de seguridad de una planta de proceso, como un sistema complejo, antes de que se mueva gradualmente hacia un estado inseguro. Se ha desarrollado una metodología novedosa basada en STPA para medir el nivel de seguridad de una planta de proceso. La medición del nivel de seguridad se realiza de acuerdo con el estado de los puntos de control de seguridad ('Safety Checkpoint'). El punto de control de seguridad es un nuevo concepto introducido en este trabajo y agregado a STPA. Un punto de control de seguridad es un requisito definido para evitar que ocurra un escenario de pérdida ('Loss Scenario') o para satisfacer las medidas de seguridad asociadas al escenario de pérdida.

La metodología se ha aplicado a una sección de una planta de proceso. Se definen 16 puntos de control de seguridad sobre diferentes aspectos y en diferentes niveles del sistema socio-técnico:

- Diseño/Técnico/Ingeniería
- Sistema de control básico de proceso (BPC)
- Controles operativos (por ejemplo, deshabilitar BPC, modificación del 'set point')
- Desempeño operativo (por ejemplo, mantenimiento atrasado)
- Competencia del personal
- Controles organizacionales (por ejemplo, gestión de cambio (MOC), asignación de recursos, planificación de mantenimiento)

Cada punto de control de seguridad podría estar relacionado con uno o más escenarios de pérdida de la planta. En este caso se definen 118 escenarios de pérdida. Cuanto mayor sea el número de escenarios de pérdida relacionados con un punto de control de seguridad, mayor será su peso en el cálculo del nivel de seguridad. Para calcular el nivel de seguridad de la planta en base a esta metodología, se obtienen datos de la planta y se determina el estado de cada punto de control de seguridad. Teniendo en cuenta el peso de cada punto de control de seguridad, el nivel de seguridad de la planta se calcula a 67,8%.

Esta metodología está desarrollada para medir el nivel de seguridad de una planta de proceso. Sin embargo, el resultado puede presentarse de diferentes maneras para ayudar a la gerencia a tomar decisiones informadas basadas en el riesgo y tomar medidas proactivas y oportunas para prevenir accidentes:

- La lista de puntos de control de seguridad y su estado se pueden mostrar en un tablero. Eso ayuda a identificar fácilmente cualquier punto de control de seguridad que tenga un estado inaceptable para tomar las medidas necesarias a fin de que mejore el nivel de seguridad de la planta.
- El estado de seguridad de la planta de proceso se puede mostrar en un gráfico circular. Esto puede ayudar a identificar puntos de control de seguridad con un estado inaceptable y su importancia (peso) en la seguridad de la planta de proceso. Proporciona una información muy importante a los tomadores de decisiones para priorizar acciones de manera proactiva
- El estado general de seguridad de la planta de proceso también se puede mostrar en un medidor de tipo de cinta que ayuda a visualizar las partes faltantes. Los tomadores de decisiones tienen suficiente información sobre dónde actuar para tener una planta de proceso segura. Les ayuda a priorizar tareas y recursos y a trabajar proactivamente en áreas que necesitan más atención para mejorar la seguridad de la planta de proceso

Los resultados obtenidos de esta metodología son prometedores y proporcionan una mejora significativa en comparación con las soluciones existentes en entornos industriales y académicos para la medición de la seguridad.

En el entorno industrial, se han realizado muchos trabajos para medir la seguridad. Centro de la seguridad de proceso de América (CCPS, 2007), Instituto Americano del Petróleo (API, 2016), Asociación Internacional de Productores de Petróleo y Gas (IOGP, 2018), Consejo Europeo de la Industria Química (CEFIC, 2011), Organización para la Cooperación y el Desarrollo Económico (OECD, 2008) y el Ejecutivo de Salud y Seguridad del Reino Unido (HSE UK, 2006), entre otros, han publicado procedimientos y directrices sobre indicadores de seguridad de proceso. CCPS, API e IOGP asumieron una relación predictiva entre eventos de seguridad de proceso de consecuencias bajas y altas similar a la pirámide de accidentes introducida por Heinrich para lesiones personales. Donde la pirámide representa un continuo de indicadores de seguridad de procesos proactivos ('leading') y reactivos ('lagging') desde abajo hacia arriba. La mayoría de las mediciones de seguridad sugeridas en el entorno industrial se basan en gran medida en contar los accidentes y/o causi-accidentes. Esto no es solamente para seguridad de proceso e incluye la seguridad personal.

Respecto a la seguridad del proceso, los indicadores reactivos no pueden ser útiles para medir la seguridad porque los accidentes graves son extraordinarios y ocurren con poca frecuencia, especialmente a nivel de una planta. Por lo tanto, los indicadores reactivos no pueden usarse para medir la seguridad y posiblemente no pueden ser útiles como advertencias tempranas para prevenir accidentes. Se han realizado algunos esfuerzos, como la publicación IOGP sobre indicadores proactivos de seguridad de procesos (IOGP, 2016), que se enfocan en desarrollar indicadores que brinden cierta información antes de que ocurra un accidente (indicadores proactivos). Los indicadores proactivos generalmente están destinados a ayudar en la identificación de las primeras señales de deterioro y, por lo tanto, a proporcionar advertencia sobre problemas inminentes antes de que ocurra un accidente real. Las

advertencias tempranas de estos indicadores deberían iniciar una investigación adicional sobre las causas de los síntomas para garantizar que las acciones se tomen a tiempo. Dependiendo de cómo se definan los indicadores proactivos, puede haber una buena cobertura en un área y un vacío en otra área. La definición de los indicadores proactivos se basa principalmente en la experiencia y se centra en áreas conocidas sin contar con un enfoque basado en las teorías de sistemas.

Además de las publicaciones sobre medición de seguridad en el entorno industrial, ha habido algunas herramientas desarrolladas por empresas como e-Vision (e-Vision, 2019), CGE (CGE Risk Management Solutions, 2019), DNV-GL (DNV-GL, 2019), Petrotechnics (Petrotechnics, 2019), RiskPoynt (RiskPoynt, 2019) y Safetec (SAFETEC, 2019) entre otros para visualizar y monitorear el estado de las barreras de seguridad.

Las publicaciones o herramientas mencionadas no se basan en ningún enfoque sistémico sobre accidentes y, en algunos casos, se basan en el modelo ‘Swiss Cheese’ que es un modelo basado en la cadena de eventos. El modelo ‘Swiss Cheese’ tiene algunos componentes de los sistemas, pero no se considera un modelo completamente sistémico.

En el entorno académico, hubo algunos esfuerzos previos como ‘barómetro de seguridad’ de (Knegtering & Pasman, 2013) e índice ‘PROCESO’ de (Maroño, Pena, & Santamaria, 2006) con el objetivo de encontrar una solución para la medición de seguridad. Sin embargo, ninguno de ellos utilizó teorías de sistemas que es la solución prometedora para los sistemas socio-técnicos complejos que encontramos hoy en día en la industria de procesos.

La metodología se ha probado en una sección de una planta de proceso utilizando datos reales con resultados prometedores. Sin embargo, esto es solo una demostración para mostrar la capacidad de la metodología. Para uso industrial, es necesario extender el alcance a toda la planta de proceso y niveles más altos de la estructura socio-técnica de la planta de proceso. Para validar la metodología, es necesario usarla en una planta de proceso por un período de tiempo largo suficiente para evaluar y analizar los datos de accidentes antes y después de la implementación de la metodología y evaluar la validez y efectividad de la metodología en medir el nivel de la seguridad y apoyar a los responsables en la gestión proactiva de la seguridad. Cuando se implementa la metodología, otro mecanismo de validación sería verificar el nivel de seguridad obtenido por la metodología en el momento de los accidentes.

Como conclusión, aunque algunos investigadores en el entorno académico han realizado esfuerzos para medir la seguridad y en el entorno industrial se han realizado algunos trabajos y se han publicado guías o prácticas a fin de encontrar una solución para la medición de la seguridad, ninguno de ellos obtuvo resultados comparables a este trabajo, ni utilizaron teorías de sistemas que es la solución prometedora para los sistemas socio-técnicos complejos que encontramos en la actualidad en las plantas de proceso. En consecuencia, se recomienda continuar el trabajo mediante la implementación completa de la metodología en una planta de proceso y validarla como se mencionó anteriormente.

Abstract

Many major accidents like Flixborough (1974), Seveso (1976), Bhopal (1984), Piper Alpha (1988), Exxon Valdez (1989), Pasadena (1998), Longford (1998), Toulouse (2001), Petrobras P36 (2001), Buncefield (2005), Texas City (2005), Deep Water Horizon - Macondo (2010) happened in the process industry in the last decades with multiple fatalities, significant environmental impacts and financial losses.

In response to most of these accidents many changes and improvements happened in regulations, organizations and technical aspects with the intention to prevent similar accidents or mitigate their consequences. For example, in Europe, Seveso (1976) accident prompted the adoption of legislation on the prevention and control of major accidents (Directive 82/501/EEC) that was called as Seveso Directive. In UK, Piper Alpha (1988) accident completely reshaped the offshore safety regime. One of the main recommendations led to the Offshore Installations Regulations (Safety Case).

Companies involved in the process industry make many efforts to prevent and control major accidents. They carry out several safety studies and activities at different times during the life of a process plant. Hazard Identification (HAZID), BowTie Analysis, Hazard and Operability Studies (HAZOP), Safety Integrity Level (SIL) Study, Fire, Explosion and Release Consequence Modelling, Quantitative Risk Assessment (QRA), Environmental, Social and Health Impact Assessment (ESHIA), Emergency Response Plan (ERP), Oil Spill Response Plan, Pre-Startup Safety Review, Plant Safety Audits, Risk Based Inspection and Preventive and Predictive Maintenance, Management of Change, Permit to Work, Job Safety Analysis, Operational Risk Assessment are examples of studies and activities done by companies during the design, construction, commissioning, start up and operation.

At industry level, many improvements in technology, materials, instrumentation and control, design and communication have been occurring. Despite regulatory modifications, companies' efforts and technological improvements, major accidents continue to occur in the process industry and often have serious consequences. This has raised concerns about safety management and highlighted problems in scientific thinking about safety. The current thinking about how accidents happen and the management systems based on that, while reasonably successful, does not appear to enable the process industry to achieve zero accident goal (Ale, et al., 2014). One of the main reasons is that most of the techniques commonly used for accident prevention, or definition of safety requirements via safety studies, are based on traditional accident causation models developed many years ago.

There is an argument that significant changes have occurred in the process industry, but common techniques for safety study and accident prevention have not been updated accordingly. Consequently, these traditional techniques may have limitations in identifying hazards related to the modern process industry that is characterized for being a complex sociotechnical environment. Leveson indicates that many changes have happened in the industry that make traditional accident causation models and safety engineering techniques based on them partially effective for studying modern complex plants (Leveson N. G., 2012):

- Fast pace of technological change
- More complex relationships between humans and automation
- Increasing complexity and coupling

- Change in the nature of accidents.
- Difficulty in selecting priorities and making tradeoffs
- New types of hazards
- Decreasing tolerance for single accident
- Reduced ability to learn from experience
- Changes in regulatory and public views of safety

Accident causation models have evolved over time and different types of accident causation models have been introduced. There are different ways to classify accident models. Some authors classified accident causation models into sequential, epidemiological and systematic models where:

- Sequential models describe an accident as a chain of events occurring in a temporal order.
- Epidemiological models consider events leading to accidents similar to the spreading of a disease, i.e., as the outcome of a combination of factors that happen to exist together in space and time.
- Systemic accident models are based on systems theory and try to describe the performance of a system as a whole, rather than on the specific cause-effect relationship or even epidemiological factors.

Sequential and epidemiological models are considered as traditional models, whereas systemic models are considered as modern models. One of the earliest accident causation models is the Heinrich Domino theory that describes an accident as a chain of events. It was updated by several researcher over the years and it can be considered as the origin of sequential models. Most of the traditional techniques such as Failure Modes and Effects Analysis (FMEA), Fault Tree Analysis (FTA), Event Tree Analysis, and Cause-Consequence Analysis are based on sequential models (Leveson N. , 1995).

Traditional models work well for losses caused by failures of physical components or human errors in relatively simple systems. Modern technology has significantly changed the nature of the industry and human work from mainly manual tasks to predominantly knowledge intensive activities. Consequently, human contribution to accidents has changed from human error to human factor, which is more than a simple error made by a person. Additionally, traditional models do not fully capture the dynamics and non-linear interactions between system components in complex sociotechnical systems.

Systemic models have their roots in systems theory. Systems theory includes the principles, models, and laws necessary to understand complex interrelationships and interdependencies between components (technical, human, organizational and management) of a complex system. Rasmussen's hierarchical socio-technical framework AcciMap (Rasmussen J. , 1997), Hollnagel's FRAM-Functional Resonance Accident Model (Hollnagel E. , 2004) and Leveson's Systems-Theoretic Accident Model and Processes (STAMP) model (Leveson N. G., 2004) are notable systemic models trying to model complex sociotechnical systems.

Causal Analysis based on Stamp (CAST) and System Theoretic Process Analysis (STPA) are techniques developed based on STAMP. CAST is an accident analysis technique and STPA is a hazard identification technique. In this work, CAST is used to analyze an accident

happened in the process industry, 2012 Chevron Refinery accident, and the result is compared with the ones obtained by AcciMap and FRAM. In addition, STPA is used to study hazards of a process plant and the result is compared with the plant HAZOP as a traditional technique. STAMP seems to be one of the most appropriate accident causation models to handle complex systems.

In this work, authors tried to find a solution based on STAMP for proactive measurement of safety level before a process plant, as a complex system, gradually move toward an unsafe state. A novel methodology is developed based on STPA to measure the safety level of a process plant. The measurement of safety level is done according to the status of safety checkpoints. Safety checkpoint is a new concept introduced in this work and added to STPA. A safety checkpoint is a requirement defined to prevent a loss scenario to happen or to satisfy safety measures associated to the loss scenario.

The methodology is applied to a section of a process plant. 16 safety checkpoints are defined on different aspects and at different levels of the sociotechnical system:

- Design/Technical/Engineering
- Basic Process Control (BPC) functionality
- Operational controls (e.g. disabling BPC, set point modification)
- Operational performance (e.g. maintenance backlog)
- Staff Competency
- Organizational controls (e.g. MOC, resource allocation, maintenance planning)

Each safety checkpoint could be related to one or more loss scenario of the plant. In this case 118 loss scenarios are defined. The higher the number of loss scenarios related to one safety checkpoint the higher its weight in calculating the safety level. In order to calculate the safety level of the plant based on this methodology, data is obtained from the plant and the status of each safety checkpoint is determined. Taking into account the weight of each safety checkpoint the plant safety level is calculated as 67.8%.

This methodology is developed to measure the safety level of a process plant. However, the outcome can be presented in different ways to help management in making informed risk based decisions and taking proactive and timely actions in order to prevent accidents:

- List of safety checkpoints and their status can be shown in a dashboard. It helps to easily identify any safety checkpoint that has an unacceptable status in order to take required actions to improve the safety level of the plant.
- Safety status of the process plant can be shown in a pie chart. This can help to identify safety checkpoints with unacceptable status and their importance (weight) in safety of the process plant. It provides a very important information to decision makers to prioritize actions in a proactive manner
- Overall safety status of the process plant can also be shown in a tape type meter helping to visualize the missing parts. Decision makers have enough information on where to act in order to have a safe process plant. It helps them to prioritize tasks and resources and proactively work on areas that need more attention in order to improve safety of the process plant.

The results obtained from this methodology are promising and provide a significant improvement comparing with the existing solutions at industrial and academic environments for safety measurement.

In the industrial environment, many works have been done to measure safety. Center for Chemical Process Safety (CCPS, 2007), American Petroleum Institute (API, 2016), International Association of Oil & Gas Producers IOGP (IOGP, 2018), European Chemical Industry Council (CEFIC, 2011), Organization for Economic Cooperation and Development (OECD, 2008) and UK Health and Safety Executive (HSE UK, 2006) amongst others have published procedures and guidelines on process safety indicators. CCPS, API and IOGP assumed a predictive relationship between lower and higher consequence process safety events similar to the accident pyramid introduced by Heinrich for personal injuries. Where the pyramid represent a continuum of leading and lagging process safety indicators from the bottom to the top. Most of the safety measurements suggested in the industrial environment are heavily based on counting accidents and/or near misses. This is not limited to process safety and includes occupational safety.

Regarding process safety, lagging indicators cannot be helpful in measuring safety because major accidents are rare and occur so infrequently specially at a site level. Therefore, lagging indicators cannot be used to measure safety and may not be useful as early warnings to prevent accidents. There have been some efforts, like the IOGP publication on leading process safety indicator (IOGP, 2016), that focus on developing indicators that provide some information before an accident occurs (leading indicators). Leading indicators are generally intended to help in identifying early signals of deteriorating performance and thereby to provide means for warning of impending problems before an actual accident occurs. Early warnings from these indicators should initiate a further investigation on the causes of the symptoms to ensure that actions will be timely taken. Depending on how leading indicators are defined, there may be a good coverage in one area and a vacuum in another area. Definition of leading indicators is mainly experience based and focuses on known areas without counting on a system based approach.

In addition to the publications on safety measurement in the industrial environment, there have been some tools developed by companies like e-Vision (e-Vision, 2019), CGE (CGE Risk Management Solutions, 2019), DNV-GL (DNV-GL, 2019), Petrotechnics (Petrotechnics, 2019), RiskPoynt (RiskPoynt, 2019) and Safetec (SAFETEC, 2019) among others to visualize and monitor the status of safety barriers.

Mentioned publications or tools are not based on any systemic approach on accidents and in some cases they are based on Swiss Cheese Model that is a model based on chain of event. Swiss Cheese Model has some component of systems but it is not considered as a thoroughly systemic model.

In the academic environment, there were some previous efforts like ‘safety barometer’ by (Knegtering & Pasman, 2013) and ‘PROCESO index’ by (Maroño, Pena, & Santamaria, 2006) to find a solution for safety measurement. However, none of them used systems theories that is the promising solution for sociotechnical complex systems we encounter these days in process industry.

The methodology is tested on a section of a process plant using real data with promising results. However, this is only a demonstration to show the capability of the methodology. For industrial use, it is necessary to extend the scope to the whole process plant and higher levels of the sociotechnical structure of the process plant. In order to validate the methodology, it is necessary to use it in a process plant for a period of time long enough for evaluation and analysis of accident data before and after implementation of the methodology and assess the validity and effectiveness of the methodology in measuring safety level and helping the management in proactive management of safety. When the methodology is implemented, another validation mechanism would be to check the level of safety obtained by the methodology at the time of accidents.

As conclusion, although some researchers in the academic environment have made efforts to measure safety and in the industrial environment some works have been done and guides or practices have been published to find a solution for safety measurement, none of them obtained results comparable to this work, nor they used systems theories that is the promising solution for sociotechnical complex systems we encounter these days in process plants. Consequently, it is recommended to continue the work by full implementation of the methodology in a process plant and validate it as mentioned before.

Chapter 1: Introduction

Accidents in process industry can have disastrous consequences such as multiple fatalities, major environmental impacts, property loss or a combinations of these. Flixborough (1974), Seveso (1976), Bhopal (1984), Piper Alpha (1988), Exxon Valdez (1989), Pasadena (1998), Longford (1998), Toulouse (2001), Petrobras P36 (2001), Buncefield (2005), Texas City (2005), Deep Water Horizon - Macondo (2010), Amuay (2012), Oklahoma (2018) and Tarragona (2020) are examples of major accidents happened in the last decades. Some of these accidents resulted in changes in organizations and or regulations.

In Europe, the catastrophic accident in the Italian town of Seveso in 1976 prompted the adoption of legislation on the prevention and control of major accidents (Directive 82/501/EEC) that was called as Seveso Directive. The Seveso Directive was later amended in view of the lessons learned from later accidents such as Bhopal, Toulouse or Enschede resulting into Seveso-II (Directive 96/82/EC). In 2012 Seveso-III (Directive 2012/18/EU) was adopted taking into account, amongst others, the changes in the Union legislation on the classification of chemicals and increased rights for citizens to access information and justice (Environment Directorate General of the European Commission, 2019).

In UK, the Piper Alpha accident that happened in July 1988 completely reshaped the offshore safety regime. The Cullen Inquiry made 106 recommendations on 24 topics like safety case, management system, regulation, auditing, permit to work, pipeline shutdown, emergency management, lifeboats, drills and training amongst others (Cullen, 1990). One of the main recommendations led to the Offshore Installations (Safety Case) Regulations, which came into force in 1992. The safety case must be accepted by the Health and Safety Executive's (HSE) Hazardous Installation Division, Energy Division Offshore. The regime has been extended to other high-hazard industries in the UK and copied in other jurisdictions, including Australia and Singapore (ioshmagazine, 2019).

Although there are different regulations in different countries regarding process industry, all of them have a common objective and it is prevention and control of major accidents. In this regard, companies involved in the process industry make many efforts to prevent and control accident. They carry out different studies and activities at different times to prevent accidents or mitigate their consequences. Hazard Identification (HAZID), BowTie Analysis, Hazard and Operability Studies (HAZOP), Safety Integrity Level (SIL) Study, Fire, Explosion and Release Consequence Modelling, Quantitative Risk Assessment (QRA), Environmental, Social and Health Impact Assessment (ESHIA), Emergency Response Plan (ERP), Oil Spill Response Plan, Pre-Startup Safety Review, Plant Safety Audits, Risk Based Inspection and Preventive and Predictive Maintenance, Management of Change, Permit to Work, Job Safety Analysis, Operational Risk Assessment are examples of studies and activities done by companies during the design, construction, commissioning, start up and operation in order to establish and maintain safety requirements for accident prevention and mitigation.

At industry level, many improvements in technology, materials, instrumentation and control, design and communication have been occurring. Taking into account regulatory modifications, companies' efforts and technological improvements, it is expected to have a safer industry. However, major accidents continue to occur in the process industry and often have serious consequences. These accidents have raised concerns with the public,

stakeholders, and regulators (OECD, 2012). The Deep Water Horizon - Macondo (2010) has highlighted a number of serious problems in scientific thinking about safety. One of these is that our current thinking about how accidents happen and all the management systems based on that approach, while reasonably successful, does not appear to enable us to achieve the goal of zero accident (Ale, et al., 2014). One of the main reasons is that most of the techniques commonly used for accident prevent or definition of safety requirements during design are based on accident causation models that were developed many years ago.

There is an argument that significant changes have occurred in the process industry, but safety study and accident prevent have not been updated accordingly. Consequently, these traditional techniques may have limitations in identifying hazards related to the modern process industry that is characterized for being a complex sociotechnical environment. Leveson indicates that many changes have happened in the industry that make traditional accident causation models and safety engineering techniques based on them partially effective for studying modern complex plants (Leveson N. G., 2012):

- Fast pace of technological change
- More complex relationships between humans and automation
- Increasing complexity and coupling
- Change in the nature of accidents.
- Difficulty in selecting priorities and making tradeoffs
- New types of hazards
- Decreasing tolerance for single accident
- Reduced ability to learn from experience
- Changes in regulatory and public views of safety

Within literatures about safety and accident, different terms like accident causation model, accident analysis model, accident investigation model, accident prediction model and accident model are used interchangeably to explain how accidents happen (Xie Xuecai, Li Zonghan, & Ge Ying, 2020). These models have evolved over time and different types of accident models have been introduced.

There are different ways to classify accident models. Some authors like Qureshi classified accident models into sequential, epidemiological, systematic and formal models where (Qureshi, 2008):

- Sequential models describe an accident as a chain of events occurring in a temporal order.
- Epidemiological models consider events leading to accidents similar to the spreading of a disease, i.e., as the outcome of a combination of factors that happen to exist together in space and time.
- Systemic accident models are based on systems theory and try to describe the performance of a system as a whole, rather than on the specific cause-effect relationship or even epidemiological factors.
- Formal methods focus on the precision in definitions and descriptions, and provide notations for describing and reasoning about certain aspects of accidents.

Qureshi considered sequential and epidemiological model as traditional models, whereas systematic and formal models as modern models (Qureshi, 2008).

Xie Xuecai et. al. proposed a classification method that divides accident models into linear and nonlinear models. Linear accident models consider accident as a chain of logical sequence. For these models, different types of causes such as direct causes, indirect causes and root causes can be identified associated to different stages of an accident. Nonlinear accident models do not distinguish the cause of the accident associated to different stages, but analyze factors related to an accident. Subsequently, they classified nonlinear accident model into four categories: human based, statistics based, energy based and system based accident models where (Xie Xuecai, Li Zonghan, & Ge Ying, 2020):

- Human based accident models: For the most parts, these models examine the human factors of an accident. The study of human factors was the basis of the type of accident models.
- Statistics based accident models: Accident statistics are used in these models to analyze the relationship between the number and severity of accidents. These models talks about the proportion of accidents that falls under different severity groups. They use these statistics to build a theoretical foundation in order to prevent major accident.
- Energy based accident models: These models take energy release and transfer as research objects and propose related measures.
- System based accident models: These models have been developed recently. They are based on system theory and study the system as a whole. They include factors related to management, human and object. Consequently, the analysis of the cause of the accident is more profound.

Their proposed classification is shown in Figure 1.

Figure 1 Accident model classification proposed by (Xie Xuecai, Li Zonghan, & Ge Ying, 2020)

Some of the accident models mentioned in Figure 1 are explained in Chapter 2 of this work.

System based accident models or systemic accident models have been introduced recently to deal with the complexity of the systems. Systemic models view accidents as emergent phenomena that arise from interactions among system components, where the interactions may be non-linear and involve multiple feedback loops (Perrow, 1984). Alongside a succession of some studies like Perrow, Reason and others, Rasmussen's papers in 1990 and 1997 catalyzed efforts to shift the focus of accident causation studies from role of individual and human error towards underlying organizational factors (Waterson, Le Coze, & Andersen, 2017) meanwhile describing 'self-organization' and the 'defense in depth fallacy' (Le Coze, 2015).

Nevertheless, most of the commonly used safety analysis and risk assessment techniques are based on traditional accident models and do not take into account the new accident models based on system theory. Using safety analysis and risk assessment techniques based on systemic accident model may be more effective in prevention and mitigation of accidents. STAMP (Systems Theoretic Accident Model and Processes), FRAM (Functional Resonance Accident Model) and AcciMap are among the most widely known accident models based on systems theory. These models are explained in Chapter 2 of this work.

There are several works on quantitative accident analysis models that support predicting and preventing accidents (Attwood, Khan, & Veitch, 2006); (Rathnayakaa, Khana, & Amyotte, 2011); (Rathnayakaa, Khana, & Amyotte, 2011); (Markowski & Kotynia, 2011); (Weber, Medina-Oliva, Simon, & Iung, 2012); (Pasman & Rogers, 2013); (Ferdous, Khan, Sadiq, Amyotte, & Veitch, 2013); (Badreddine & Ben Amor, 2013); (Khakzad, Khan, & Amyotte,

2013); (Villa & Cozzani, 2016); (Araujo, Norte da Silva, & Silva, 2017). System Hazard Identification, Prediction and Prevention (SHIPP) is one of these models that combines qualitative and quantitative analyses to provide a comprehensive approach with updating and prediction capabilities. The fault tree and event tree analysis techniques are used to model accident in a holistic way providing a cause-consequence view of the accident and Bayesian approach is used to facilitate updating and prediction capabilities (Rathnayakaa, Khana, & Amyotte, 2011) and (Rathnayakaa, Khana, & Amyotte, 2011). Another quantitative accident analysis model proposed by integrating Human Factors Analysis and Classification System (HFACS) with Bayesian Network. This model proposed prevention measures that are ranked in a cost-effectiveness manner through Best-Fit method and Evidential Reasoning approach. In another work, layer of protection analysis (LOPA) which is a semi-quantitative method is completed with bow-tie model and fuzzy logic system. It is used to cope with the lack of knowledge of reliability data that describe probabilities of initiating events and safety functions (Markowski & Kotynia, 2011).

Industry and companies use different safety indicators to measure safety performance. Fatality Rate, Lost Time Injury Frequency (LTIF) rate, Total Recordable Injury Rate (TRIR), Process Safety Event (PSE) rate, transport related accidents rate, first aid rate and near miss rate are examples of the most common used indicators. These indicators are lagging and mainly counting the number of accidents or near misses that happened in the past. Thus, they only demonstrate how the safety performance was in the past, and based on that, companies may take actions to prevent reoccurrence of similar accident in the future if they are successful in correct definition and implementation of actions. Consequently, these lagging indicators have limited effectivity in preventing accidents not happened before and in general in prevention of accidents.

Some organizations and companies try to define leading indicators with the objective to prevent accidents and published procedures and guidelines. Most of these leading indicator are related to the elements of management system or the way activities are executed. Yet, these efforts are not standardized and miss a scientific base to demonstrate their ability in accident prevention. The perfect solution may be an indicator that demonstrate the safety level in a proactive manner. It could ideally measure the safety level and before getting to an unsafe level, it could warn decision makers and let them to take required action in order to maintain the operation within safe limits and prevent accidents.

In addition to the publications on safety measurement in the industrial environment, there have been some tools developed by companies like e-Vision (e-Vision, 2019), CGE (CGE Risk Management Solutions, 2019), DNV-GL (DNV-GL, 2019) Petrotechnics (Petrotechnics, 2019), RiskPoynt (RiskPoynt, 2019) and Safetec (SAFETEC, 2019) among others to visualize and monitor the safety and status of safety barriers.

However, mentioned publications or tools are not based on any systemic approach on accidents and in some cases they are based on Swiss Cheese Model that is a model based on chain of event. Swiss Cheese Model has some component of systems but it is not considered as a thoroughly systemic model.

Some researchers like Knegtering & Pasman and Marono, Pena, & Santamaria tried to find a solution for safety measurement (Knegtering & Pasman, 2013) (Maroño, Pena, &

Santamaria, 2006). Nevertheless, none of them used systems theories that is the promising solution for sociotechnical complex systems we encounter these days in process plants.

1.1. Objective

The objective of this work is to develop a methodology for safety level measurement in process industry as a proactive approach in accident prevention. For this, it is necessary to understand how accidents happen. Accident causation model are studied and a summary of the most common and well-known accident causation models is provided in Chapter 2. As mentioned before and will be discussed in more details further in this work, accident models based on systems theory are considered the most suitable ones to deal with complex sociotechnical environment of the process industry.

STAMP seems to be one of the most appropriate systemic models to handle complex system of a process plant. In this work, STAMP is used to develop the methodology for safety measurement. STAMP is explained in Chapter 3 of this work.

Causal Analysis based on Stamp (CAST) is an accident analysis technique and System Theoretic Process Analysis (STPA) is a hazard identification technique. Both are main techniques developed based on STAMP. CAST and STPA are explained in Chapter 4 of this work.

In order to understand the details of the model, CAST and STPA are applied in process industry as part of this work. CAST is applied on an accident in process industry that is provided in Chapter 5 of this work. Then STPA is applied in process industry and it is provided in Chapter 6 of this work.

STPA is the technique used to develop the safety level measurement methodology. The methodology to measure safety level is explained in Chapter 7 of this work. Previous efforts made to measure safety by others did not use systemic models to support their idea. The methodology presented in this work is based on a systemic model and consequently, it helps in correct definition of basis for proper monitoring and measurement of safety level with the aim to prevent accidents. The methodology is applied to a section of a process plant with promising results and the outcome is presented in Chapter 7 of this work. However, this is only a demonstration to show the capability of the methodology. For industrial use, it is necessary to extend the scope to all the equipment in the plant and higher levels of the sociotechnical structure of the process plant. In order to validate the methodology, it has to be used in a process plant for a period of time long enough for evaluation and analysis of accident data before and after implementation of the methodology and assess the validity and effectiveness of the methodology in measuring safety level. Finally, conclusions are provided in Chapter 8 of this work.

Main contributions of this work are summarized below:

- Application of CAST in process industry. Provided in Chapter 5 of this work. A paper published in Process Safety Progress Journal DOI 10.1002/prs.12002.
- Application of STPA in process industry. Provided in Chapter 6 of this work. A paper published in Journal of Loss Prevention in the Process Industries: <https://doi.org/10.1016/j.jlp.2019.06.014>.

- Development of a novel methodology to measure safety level in process industry. Provided in Chapter 7 of this work. A paper published in Process Safety and Environmental Protection Journal: <https://doi.org/10.1016/j.psep.2020.01.035>.

Chapter 2: Accident Causation Models, Hazard Identification and Risk Assessment Techniques

Undoubtedly the main reason we want to understand how accidents happen is because we wish to prevent future ones (Wagenaar & P.T.W., 1987). The best way to do this is to have a solid theoretical basis that can be used both to describe what actually happened and to serve the goal of defining effective preventative measures (Hudson, 2010). A theory that explains how an accident happen and help to ascertain the causes of the accident is an accident causation model or simply an accident model.

Accident causation models started to appear in the early 20th century. First, simple linear models developed explaining a sequence of individual failures and surrounding circumstances causing accidents. Then, it gradually evolved and resulted in complex linear models. And finally, complex non-linear models have been developed to cope with the nowadays complex sociotechnical environment.

Simple linear models assume that an accident is the result of a series of sequential events resembling dominos that fall of first cause the fall of second and so on. It is expected that, the elimination of one of the dominos may prevent the accident. Sequential events could be individual failures, unsafe acts, unsafe conditions like mechanical/physical hazards, etc.

Complex linear models assume that an accident is the result of a combination of different unsafe conditions and factors. It is expected that an accident could be prevented by setting appropriate controls. Different type of models fall under this category: time sequence models, epidemiological models, Swiss Cheese model are examples of this group.

Complex non-linear models assume that an accidents is the result of interaction between different factors. It is expected that, by understanding these multiple interacting factors accidents could be prevented. System theoretic accident model and process (STAMP) and functional resonance accident model (FRAM) are examples of this category.

Accident causation models fall under either of these three basic types of accident causation models. However, most accident models view accidents as resulting from a chain or sequence of events. According to Leveson, such models work well for losses caused by failures of physical components and for relatively simple systems. But since World War II, the types of systems we are attempting to build and the context in which they are being built have been changing (Leveson N. G., A new accident model for engineering safer systems, 2004). Consequently, accident models other than those based on chain of events are required to understand how accident happen in systems designed these days. A review of the state of art of accident models, hazard identification and risk assessment techniques is provided in this chapter. It is not an exhaustive review, however, it facilitate to have an understanding on the accident causation models and techniques used for hazard identification and risk assessment. Eventually, it helps to identify the most suitable model or technique to develop a methodology to measure safety level that is the purpose of this study.

2.1 Domino theory

Some people believe that everything happen based on fate and even their decisions cannot modify the destiny. Some people partially agree with this, but they believe that their choices

and prayers can change the predetermined future. Peter L. Bernstein reviewed much early thinking about how people saw accidents as the acts of gods and other spirits, capricious or otherwise, and how they originally performed ritual or sacrifice to prevent accidents rather than really doing something about it (Bernstein, 1998).

On the other hand, not accepting predetermined future resulted in doing something and trying to understand why and how accidents happen. Herbert William Heinrich was one of these people and developed a theory called Domino theory. The Domino theory was developed by him in 1931. It states that an accident is only one of a series of factors, each of which depends on a previous factors in the following manner (Heinrich, 1931):

- Accident causes an injury.
- Individual's negligent act or omission, or a faulty machine, causes an accident.
- Personal shortcomings cause negligent acts or omissions.
- Hereditary and environment cause personal shortcomings.

Heinrich proposed a series of five factors in sequence. Based on his proposal, each factor acts on the next factor similar to the toppling dominoes lined up in a row as shown in Figure 2. The sequence of these factors is as following:

- Ancestry and social environment: Those conditions that make people to take or accept a certain level of risk. In the other words, willingness or culture of people in take risk.
- Worker fault or undesirable human character: Hastiness, carelessness, tiredness, anger, misunderstanding, lack of understanding.
- Unsafe act or condition together with mechanical and physical hazard: Short cutting, not following the procedures and instructions, poor planning, unsafe equipment, equipment failure, unsafe condition, hazardous environment.
- Accident: The accident occurs when the above events line up and result in something to go wrong.
- Damage or injury: Damage or injury occur when accident occur and impact persons, the environment or damage equipment and properties.

Figure 2 Heinrich Domino Theory (Heinrich, 1931)

Based on the domino model, accidents could be prevented by removing one of the dominos or factors. In the other words, accidents could be prevented by interrupting the toppling impact of the dominos. Heinrich argued that unsafe act or condition, mechanical failures and physical hazard have a central role in the sequence of an accident and removal of this central factor makes the previous factors being ineffective in causing the accident. He focused on the human factor, which he called 'Man Failure', as the cause of most accidents. Giving credence to this proposal, actuarial analysis of 75,000 insurance claims attributed some 88% of preventable accidents to unsafe acts of persons and 10% to unsafe mechanical or physical conditions, with the last 2% being acknowledged as being unpreventable (Heinrich, 1931).

The work of Heinrich can be summarized in two points: people are the fundamental reason behind accidents; and management is responsible for the prevention of accidents (Petersen D. , 1996).

The domino theory has been a very used methodology for many years. Some of Heinrich's views were criticized for oversimplifying the role of human behavior in causing accidents and for some statistics he gave on the contribution of unsafe acts versus unsafe conditions. Nevertheless, his work was the foundation for many others and over the years it has been updated by several researchers with an emphasis on management and identifying failures in the management system (Abdelhamid & Everett, 2000). For example Weaver in 1971 modified the original theory to propose that the last three dominos in the sequence were caused by management omissions (Weaver, 1971). Some of the models based on domino theory are provided below.

2.2 Loss Causation Model or ILCI Model

As already has mentioned, the domino theory has been modified and updated over the years resulting in different models known as updated domino models and also as management based models (Hosseinian & Jabbarani Torghabeh, 2012). Bird adapted Heinrich's domino theory to reflect the influence of management in the accident causation process (Bird F. E., 1974). Bird and Germain recognized the role of management to prevent and control accidents in a context that was becoming more complex because of rapid advances in technology. They developed an updated domino model by incorporation of arrows that show the multi linear interactions of the cause and effect sequence (Bird & Germain, 1985). This model became known as the Loss Causation Model. It is also known as International Loss Control Institute model (ILCI model). The ILCI model represents a more generic and broader view of accident propagation. In ILCI model, the immediate and root causes that lead to an accident are described as management deficiencies, personal and job factors and unsafe acts and conditions. Similar to domino model, it is represented by a line of five dominos, linked to each other in a linear sequence (Figure 3).

Lack of Control	Basic Causes	Immediate Causes	Incident	Loss
Inadequate: System Standards Compliance	Personal Factors Job/System Factors	Substandard Acts/ Practices Substandard Conditions	Event	Unintended Harm Or Damage

Figure 3 Loss causation model (Bird & Germain, 1985)

In 1976, Adams also changed the emphasis of the first three dominos of the Heinrich's domino theory to reflect organizational rather than person features (Adams, 1976)

2.3 Multiple causation theory

Petersen in 1971 (Petersen D. , 1971) developed a model based on management system rather than individual (Figure 4). Petersen in line with Heinrich's domino theory believed that unsafe act and unsafe condition are two major causes that lead to an accident. However, there are many contributing factors, causes and sub-causes in an accident scenario. In that sense, it is not simplified in the way that theory of domino does. Consequently, the model was named 'multiple causation'. Identification of these multiple contributing factors, causes and sub-causes of accident can help to prevent that unsafe acts and unsafe conditions happen. He indicated that unsafe acts and unsafe conditions are proximate causes. While, contributing factors, causes and sub-causes are related to management system, policies, procedure, supervision, etc. and in general are considered as root causes.

Figure 4 Petersen's Multiple causation theory (Petersen D. , 1971)

Multiple causation theory is considered as a branch of the domino theory. It suggests that there may be many contributory factors, causes and sub-causes for a single accident. A specific combinations of these items also can result to accidents.

2.4 Multilinear events sequence model

Ludwig Benner identified four issues which were not addressed in the basic domino type model: no clear delineation of the beginning and end of the accident phenomenon could be

found, no representation of the events that happened on a sequential time line, no structured method for discovering the involved factors and no charting method to define events and conditions (Benner, 1975).

Then, he postulated that a chronological array of the events aids in looking for the relevant factors and events involved in the accident in a structured manner. By displaying the events in which each actor is involved along a horizontal line the array can be obtained. The events for each actor could be displayed in a linear chain of events as each actor is usually involved in sequential events. Each event can be linked to another one by arrows depicting the flow of the events in a logical sequence. Then, conditions that must be existed for the events to occur are linked to the events with arrows. It shows a full explanation of the events for any actor involved in the accident. In parallel to the horizontal lines across the chart, arraying the events associated with each actor taking into account the timing of each event relative to the other events, can demonstrate the relationship of each event to other events in terms of both its timing and its proceed logic. This multilinear events sequence charting method provides a way for the investigator of any accident to identify, order, and display the explanation of the relevant factors in the accident (Benner, 1975). A summary of the explained multilinear event sequence is provided in Figure 5.

Figure 5 multilinear events sequence model (Benner, 1975)

2.5 Time sequence model

Viner's generalized time sequence model (Viner, 1991) is an example of a time sequence model that addresses Benner's four issues on domino model (Figure 6).

Figure 6 Generalized Time Sequence Model (Viner, 1991)

Viner considers that the structure for analyzing the events in the occurrence-consequence sequence provided by the time sequence model draws attention to countermeasures that may not otherwise be evident. In Time Zone 1 there is the opportunity to prevent the event occurring. Where there is some time between the event initiation and the event, Time Zone 2 offers a warning of the impending existence of an event mechanism and the opportunity to take steps to reduce the likelihood of the event while in Time Zone 3 there is an opportunity to influence the outcome and the exposed groups (Viner, 1991).

2.6 Accident Evolution and Barrier Function (AEB) model

Despite Viner's strict linear approach to the time sequence, Svenson takes a more complex approach in his Accident Evolution and Barrier Function (AEB) model (Svenson, 1991). The AEB model visualizes an accident as a flow chart and analyses its evolution as a series of interactions between human and technical systems. Failures, malfunctions or errors are considered as interactions that could result in or have led to an accident. The accident analysis method based on AEB forces analysts to integrate human and technical systems simultaneously when performing an accident analysis (Svenson, 2000) starting with the simple flow chart technique of the method provided in Figure 7.

Figure 7 Graphical representation of the AEB-model. Failures, malfunctions and errors are located as error events in the boxes (Svenson, 2000)

2.7 Energy damage models

James J. Gibson first introduced 'Energy damage model' in 1961 (Kjellén, 2000). William Haddon used 'Energy damage model' to introduce 10 strategies in order to avoid, control, and mitigate accidents (Haddon, 1980). Then, he extended his thinking beyond that model, a summary of his thinking is provided in Figure 8.

Figure 8 Haddon's 10 accident prevention strategies

Viner considered the energy model as a result of discussions between Gibson, Haddon and others (Viner, 1991). Figure 9 shows the energy damage model which assumes that damage like injury is the result of an incident energy whose intensity at the point of contact with the recipient exceeds the damage threshold of the recipient (Viner, 1991).

Figure 9 The Energy Damage Model based on (Viner, 1991)

2.8 Epidemiological Theory

Epidemiologic approach assumes that the interaction of agent, host, and environment causes the disease. Figure 10 shows these three component factors (agent, host, and environment) and graphically presents their relation to cause disease. Among others, Godfrey, Armstrong, Bauer, Dukelow, Press and Gordon were the first researchers who admit the use of epidemiologic approach in accident prevention (Godfrey, 1937), (Armstrong, Bauer, & Dukelow, 1945), (Press, 1948), (Gordon, 1949).

Figure 10 A generic epidemiology

Epidemiological approach is also shown in Figure 11 which is known as the epidemiologic trident levels (Leveson N. G., 2001).

Figure 11 Johnson's three levels that represent different types of factors (Leveson N. G., 2001)

Accident mechanism as chain of events (Domino theory) and direct factors are provided in the lower level. In the second level contributing factors are captured. Contributing factors are conditions that allowed the events at the first level to occur. However, it does not mean that that all conditions at second level have to be met before accident occurs. At the end, systemic factors are placed in the upper level. Systemic factors there are weaknesses in the system and often are the root causes of an accident. As long as they exist in the system, they can contribute to future accidents. In many cases, only specific causal factors are fixed as responses to accidents while more general or systemic factors are left behind (Leveson N. G., 2001).

In many cases instead of identifying systemic factors such as training, communication, risk management, management of change or organizational culture, it is more likely to put blame on operator or specific component. The hierarchical model can be used to extend prevention strategies so that future accidents resulting from similar systemic factors do not occur (Johnson W. G., 1980).

Attwood developed a holistic, quantitative model to predict occupational accident frequency in the offshore oil and gas industry (Attwood, Khan, & Veitch, 2006). Similar to the layers shown in Figure 11, this occupational model includes three layers: the direct layer, the corporate support layer, and the external layer, which were proposed based on factors that lead to occupational accidents in the offshore environment. Attwood's model has both qualitative and quantitative capabilities. Figure 12 shows the arrangement of elements of the

model. In this model, a reliability concept was used to evaluate the probability of an occupational accident under various scenarios in an asset's development cycle. The prediction capability of this model offers insight into safety improvement efforts in the offshore oil and gas industry (Attwood, Khan, & Veitch, 2006).

Figure 12 Arrangement of elements of Atwood's model (Attwood, Khan, & Veitch, 2006)

2.9 Management Oversight and Risk Tree (MORT)

In US nuclear industry a technique was developed for accident investigation and safety program analysis called Management Oversight and Risk Tree (MORT). MORT has a detailed and extensive check list for accident investigation that helps finding safety problems. The early project on MORT was documented by W.G. Johnson for US Atomic Energy Commission (Johnson W. G., 1973).

MORT is a formal and disciplined logic or decision tree that relate and integrate a wide variety of safety concepts in a systematic manner. It has ability to help different disciplines like safety,

management, engineering, sciences or other specialties to apply and broaden their skills in accident analysis and safety review. It also provides a common base for communication, cooperation, and planning for greater accident control (Johnson W. G., 1980).

MORT has been used to improve safety in specific activities and in organizations. It shows the value of charting as a device for communicating different aspects of an accident. The logic tree is also valuable for developing hypotheses to connect the dots when doing an accident investigation and also guides the investigator to look for evidences in an investigation (Johnson W. G., 1975).

2.10 Swiss cheese Model

The Swiss cheese model has its root in the James Reason's works on human errors. Reason made a distinction between active errors and latent errors. The latter were likened to resident pathogens in the body. Their adverse consequences could lie dormant within the system for a long time, only becoming evident when they combine with other factors to breach the system's defenses (Reason, Managing the risks of organizational accidents, 1997).

Barry Turner (Turner, 1978), Charles Perrow (Perrow, 1984) and William Johnson (Johnson W. G., 1980) among others had already observed that understanding human error without considering contextual system issues is not possible. Condition of workplace and organizational factors were considered to be related to the occurrence of disasters like Flixborough, Challenger, Three Mile Island, Bhopal, Chernobyl in late 1970s and 1980s.

Perrow had stressed the role of defenses in depth in creating complexity, tight coupling and opacity in the system (Perrow, 1984). Reason considered the biological or medical metaphor of pathogens, and the central role played by defenses, barriers, controls and safeguards which are analogous to the body's autoimmune system.

In order to understand how humans contribute to the breakdown of complex productive systems, it is needed to identify the necessary elements of production in order to describe how and why they might fail. It was depicted as a sequence of five planes lying one behind the other: top level decision makers, line management, preconditions, productive activities and defenses (Figure 13). Failures can arise at anyone of these levels.

Figure 13 Reason's five levels of controls

Reason did not originate the term 'Swiss cheese' for these planes but others used it for his approach on accident causation. He made a representation of his approach showing an accident trajectory passing through successive 'slices' (Figure 14).

Figure 14 Reason's representation of accident causation

Its purpose was to show the dynamics of accident causation arising from interactions between latent failures and a variety of local triggering events. Figure 14 is the one that probably caused the Swiss cheese label, however most applications of the model (e.g., HFACS, ICAM, etc.) derive from Figure 13 after adding holes in it.

Figure 15 was developed later by Reason which reduced the four productive planes (in Figure 13) to three (organization, workplace, person), but extended the single defensive layer to three layers. The aim here was to allow more specificity with regard to the influences at each level. He also distinguished errors and violations and their corresponding provocative factors. The organization box here included corporate culture and organizational processes as well as management decisions. With this the impact of safety culture became more evident. The final addition was a separate latent failure path leading from the organization box to the defenses. This pathway accommodated the fact that in many disasters there were no proximate active failures, simply longstanding systemic pathogens.

Figure 15 Reason's updated representation of accident causation

Figure 16 was introduced in the book 'Managing the Risks of Organizational Accidents' (Reason, Managing the risks of organizational accidents, 1997). There were some significant changes: It started with the premise that any accident causation model needs to have hazards, defenses and losses as three basic elements. The planes were represented as obvious Swiss cheese slices including all the required barriers, defenses, safeguards and controls. An important addition was an explanation of how the holes, gaps or weaknesses arise. Immediate breaches may be created by the errors and violations of operational staff. Chronic and undoubtedly more dangerous gaps may be created by the decisions of maintainers, designers, builders, procedure writers and managers which were called latent conditions rather than latent errors or latent failures. A condition is not a cause, but it is necessary for a causal factor to have an impact. The use of this term allows admitting that all top level decisions seed pathogens into the system, and consequently it is necessary that they be right.

Figure 16 Reason's accident model (Reason, Managing the risks of organizational accidents, 1997)

Reason's accident model has different views and it can be used for different purposes. It can be used as a conceptual framework, as a means of communication or as a basis for analysis which is discussed below in more details.

- It acts as a framework to explain the interactions that occur when a complex system suffers a catastrophic breakdown. In that sense it supports the idea that a single failure either by human or a technical one is not sufficient to cause an accident, and it is caused by the conjunction of several contributing factors at different levels of the system.
- It is used as a base for accident investigation methods and a means to communicate the accident and investigation's outcome. Human Factors Analysis and Classification System (HFACS) is one of the most widely used of these. Other examples are Incident Cause Analysis Method (ICAM), Tripod Beta, etc.
- It has also been applied to proactive process measurement, i.e. a repeated assessment of some signs that gives an indication of the current state of the safety and highlights the areas that need additional actions to improve the safety and prevent incidents. The first of these tools was Tripod-Delta created for Shell in 1988-1990 by Wagenaar, Hudson, Reason, Benson and Groeneweg. Other prospective techniques based upon these ideas are REVIEW an instrument that measure latent failures in safety management created for British Rail (Edkins & Pollock, 1996), MESH (Managing Engineering Safety Health) a tailored development for British Airways Engineering and for Singapore Airlines Engineering Company, and PAOWF

(Proactive Assessment of Organizational and Workplace Factors) a technique for measuring leading indicators in the US nuclear power industry.

2.11 Bowtie

Bowtie method is a graphical approach that demonstrates the complete path of an accident starting from accident causes or threats to critical event or top event and ending with its consequences. It is composed of a fault tree on the left side identifying the possible causes and events causing the top event, and an event tree on the right side showing the possible consequences of the top event (Khakzad, Khan, & Amyotte, 2013) (Ferdous, Khan, Sadiq, Amyotte, & Veitch, 2013).

The outcome of a bowtie analysis is a bowtie diagram that comprises following elements (CGE Risk Management Solution, 2019):

Hazard: A hazard is something in, around or part of the organization which has the potential to cause damage. The start of any bowtie is the 'hazard'.

Top Event: Once the hazard is chosen, the next step is to define the 'top event'. This is the moment when control is lost over the hazard.

Threats: Threats are whatever that cause top event. There can be multiple threats.

Consequences: Consequences are the result from the top event. There can be more than one consequence for every top event.

Barriers: Barriers in the bowtie appear on both sides of the top event: Preventive barrier and recovery barriers. Barriers on the left side interrupt the scenario so that the threats do not occur, and if they do, not result in a loss of control (the top event). Barriers on the right side make sure that if the top event is reached, the scenario does not escalate into an actual impact (the consequences) and/or they mitigate the impact. Barriers are also referred to as controls, safety measures or layers of protection.

Escalation Factor (EF): Escalation factor is anything that makes a barrier fail. Barriers for escalation factors are called EF Barriers.

Figure 17 shows a typical bowtie and the relationships between these elements.

Figure 17 A typical bowtie and the relationships between its elements (CGE Risk Management Solutions, 2019)

2.12 SHIPP

According to (Rathnayakaa, Khana, & Amyotte, 2011), System Hazard Identification, Prediction and Prevention (SHIPP) is a systematic methodology to identify, evaluate, and model the accident process, thereby predicting and preventing future accidents in a process facility. SHIPP is based on Kujath accident modeling approach. Kujath et al. has proposed a conceptual process accident model (Figure 18) prioritizing the prevention of process accidents in an offshore environment (Kujath, Amyotte, & Khan, 2010). This model is developed using features of both sequential and epidemiological models. In this model, hydrocarbon release accidents were modeled using the safety barrier concept.

Figure 18 Conceptual offshore oil and gas process accident model proposed by (Kujath, Amyotte, & Khan, 2010)

Their conceptual model is further developed by Rathnayakaa et al. to provide a holistic view of process hazard accident and quantification mechanisms with predictive capabilities (Rathnayakaa, Khana, & Amyotte, 2011). In SHIPP methodology, process hazard accidents are modeled using safety barriers rather than causal factors. The fault tree and event tree analysis techniques enhance the accident model to represent a holistic picture of the cause-consequence mechanism of the accident process. Quantitative analysis has two aspects: updating and prediction. The Bayesian theory updates failure probability and consequence occurrence probability when a new observation arrives. The predictive model forecasts the probability of a number of abnormal events occurring in the next time interval. The

qualitative and quantitative capabilities of the SHIPP methodology help to design and implement safety strategies into a process system.

According to Rathnayakaa et al. the purpose of the SHIPP methodology is to identify hazards, evaluate them, predict and prevent their occurrences, and continue monitoring. The SHIPP methodology is a systematic and comprehensive safety analysis procedure that demonstrates how the process accident model integrates process system safety, and is developed by focusing on accident analysis of process hazards. The advantages of the SHIPP methodology are that it can be applied to assess the risk of the entire process system, as well as subsystems, and that it can also identify the system's hidden interactions and their consequences through modeling the accident process using safety analysis techniques. Application of this methodology helps to determine the critical safety areas that should be prioritized to implement in order to prevent future accidents based on predictive accident occurrence and accident precursor data. The SHIPP methodology comprises four phases: (1) system definition, (2) hazard identification and analysis, (3) accident modeling and prediction, and (4) updating, decision making and implementation of accident prevention strategies. This methodology is shown in Figure 19.

Figure 19 System hazard identification, prediction, and prevention (SHIPP) methodology (Rathnayakaa, Khana, & Amyotte, 2011)

The process accident model used in SHIPP methodology was developed based on the modeling approach of Kujath et al. (Kujath, Amyotte, & Khan, 2010) and set of consideration related to process accidents.

Figure 20 The process accident model developed by Rathnayakaa et al. (Rathnayakaa, Khana, & Amyotte, 2011)

2.13 Rasmussen framework or AcciMap

According to Rasmussen the present dynamic society introduces some dramatic changes in the condition of industrial risk management due to a very fast pace of change of technology, increase in the scale of industrial installations, rapid development of information and communication technology and also the aggressive and competitive environment (Rasmussen J. , Risk Management in a Dynamic Society: A Modelling Problem, 1997). System modelling has been affected significantly by these changes and it cannot be based on structural decomposition anymore but also on functional abstraction including all involved disciplines (Hale, Wilpert, & Freitag, 1997) (Rasmussen, Pejtersen, & Goodstein, Cognitive Systems Engineering, 1994). Consequently, Rasmussen argues that a system model cannot be built by a bottom-up aggregation of models derived from research in the individual disciplines, but a top-down system oriented approach based on control theoretic concepts is required (Rasmussen J. , Risk Management in a Dynamic Society: A Modelling Problem, 1997) which is discussed below.

Rasmussen believes that accidents depend on loss of control of physical processes capable of injuring people or damaging property. Accordingly, many levels of politicians, managers, safety officers, and work planners are involved in the control of safety by means of laws, rules, and instructions that are formalized means for the ultimate control of some hazardous physical process (Rasmussen J. , Risk Management in a Dynamic Society: A Modelling Problem, 1997).

Rasmussen (Rasmussen J. , Risk Management in a Dynamic Society: A Modelling Problem, 1997) summarizes the socio-technical system involved in the control of safety in a figure which is provided below (Figure 21).

Figure 21 The socio-technical system involved in risk management (Rasmussen J. , Risk Management in a Dynamic Society: A Modelling Problem, 1997)

At the top, society seeks to control safety through the legal system. Research at this level is within the focus of political and legal sciences. Next level is the authorities and industrial associations, workers' unions and other organizations. This is the level of management scientists and work sociologists. Then the rules have to be interpreted and implemented in the context of a particular company, considering the work processes and equipment. Many details drawn from the local conditions and processes have to be added to make the rules operational and, again, new disciplines are involved such as work psychologists and researchers in human-machine interaction. Finally, at the bottom level, engineering disciplines are involved in the design of the processes and equipment, and in development of standard operating procedures.

Traditionally, each level is studied separately by a particular academic discipline, for example, risk management at the upper levels is studied without any detailed consideration of processes at the lower levels. Based on Rasmussen model vertical alignment between all levels is taken into account and consequently this critical factor is not overlooked anymore. The decisions made at upper levels should transmit down the hierarchy, whereas information

about processes at lower levels should move up through the level. This vertical flow creates a complete feedback system, which plays a crucial role in the safety of the overall socio-technical system. The belief is that accidents are not caused only by the workers at the process control level, but also by decisions and actions made at all levels.

Based on Rasmussen (Rasmussen J. , Risk Management in a Dynamic Society: A Modelling Problem, 1997), in any well designed work system, numerous precautions are taken to protect the actors against occupational risk and the system against major accidents, using a ‘defense-in-depth’ design strategy. One basic problem is that in such a system having functionally redundant protective defenses, a local violation of one of the defenses has no immediate, visible effect and then may not be observed in action. In this situation, the boundary of safe behavior of one particular actor depends on the possible violation of defenses by other actors, see Figure 22. Therefore, in systems designed according to the defense in depth strategy, the defenses are likely to degenerate systematically through time, when pressure toward cost-effectiveness is dominating. Correspondingly, it is often concluded by accident investigations that the particular accident was actually waiting for its release (Rasmussen J. , Risk Management in a Dynamic Society: A Modelling Problem, 1997).

Figure 22 Under the presence of strong gradients, behavior will very likely migrate toward the boundary of acceptable performance (Rasmussen J. , Risk Management in a Dynamic Society: A Modelling Problem, 1997)

Rasmussen’s approach on risk management requires identification of the boundaries of safe operation and the dynamic forces that may cause the socio-technical system to migrate towards these boundaries. Consequently these boundaries have to be visible to the actors with opportunities to control behavior at the boundaries.

Le Coze looked back on Rasmussen’s legacy, including the ‘skill-rule-knowledge’ (SRK) model, his theoretical approach of errors, the issue of investigating accidents, his model of migration and the socio-technical view. He called Rasmussen’s accident model as ‘a strong program for a hard problem’. The ‘strong program’ is the cross-disciplinary challenge both

from a conceptual and empirical point of view. The ‘hard problem’ is the ability to better understand but also anticipate accidents through a functional analysis going across levels and therefore disciplines (Le Coze, Reflecting on Jens Rasmussen’s legacy. A strong program for a hard problem, 2015). Additionally he claimed that cybernetics has had a profound influence on Rasmussen’s thinking and provided him key principles for his inspiring and successful models (Le Coze, 2017).

The AcciMap accident analysis technique is based on Rasmussen’s risk management framework (Reason, Managing the risks of organizational accidents, 1997) (Rasmussen & Svedung, 2000). An AcciMap shows the contributing factors in an accident mapped onto the levels of a complex socio-technical system by linking the causes and consequences both horizontally (within each level) and vertically (between levels). In this way, the AcciMap serves to identify relevant decision makers and the normal work situation in which they influence and create possible accidents, i.e. here the focus is not similar to the traditional search on identifying the “guilty person”.

It was created and first used by Rasmussen and has subsequently been employed to analyze accidents in various domains, e.g. oil and gas (Hopkins, Lessons from Longford: The Esso Gas Plant Explosion, 2000), aerospace (Johnson & de Almeida, An investigation into the loss of the Brazilian space programme’s launch vehicle VLS-1 V03, 2008), led outdoor activities (Salmon, Williamson, Lenne, Mitsopoulos, & Rudin-Brown, 2010) (Salmon, Cornelissen, & Trotter, 2012) and ferry accident (Lee, Moh, Tabibzadeh, & Meshkati, 2017).

2.14 FRAM

FRAM was developed by Hollnagel and is based on four principles or assumptions about how things happen (Hollnagel E. , Barriers and Accident Prevention, 2004) (Hollnagel E. , 2012):

- The principle of equivalence of successes and failures: this is the assumption that different kinds of consequences do not necessarily require different kinds of explanations causes. It means that an accident emerges from the same actions that describe the system.
- The principle of approximate adjustments: this is the assumption that people continuously adjust what they do so that the actions match the conditions.
- The principle of emergence: this is the acknowledgement that not all results can be explained as having a specific, identifiable cause.
- The principle of resonance: in cases where it is neither possible nor reasonable to base explanations on the cause-effect principle (causality), functional resonance can be used instead to describe and explain non-linear interactions and outcomes.

FRAM is a method to analyze how work activities take place either retrospectively or prospectively. This is done by analyzing work activities in order to produce a model or representation of how work is done. The model can serve as the basis for a risk analysis, an event investigation, or for something entirely different. The selected event or performance is described in terms of the functions that are necessary to carry out the activity, the potential couplings between the functions, and the typical variability of the functions (Hollnagel, Hounsgaard, & Colligan, 2014). Based on the adjustment principle every function of the system has an inherent variability. Main sources of variability are humans, technology, latent conditions and barriers. When the variability of the different functions within the system

becomes too great for the system to be absorbed, it generates undetectable and unwanted outcomes, i.e. accident. That is a ‘functional resonance’ which makes the system being unable to cope with its normal functioning mode (Toft & Dell, 2012).

A function in the FRAM represents the means that are necessary to achieve a goal, i.e. a function represents the acts or activities either simple or complex that are needed to produce a certain result. Functions are described by means of six aspects Figure 23.

Figure 23 Hexagonal function representation (Hollnagel & Goteman, 2004)

These aspects are explained below:

- Inputs (I), which are needed to perform the function. Inputs constitute the links to previous functions and can be either transformed or used by the function in order to produce the outputs.
- Outputs (O) that are produced by the function. Outputs constitute the links to subsequent functions.
- Resources (R), representing what is needed by the function to process the input (in terms of, e.g., hardware, procedures, software, energy, manpower).
- Controls (C), or constraints, that serve to supervise or restrict the function (to monitor it and adjusts it when it goes astray). Controls can be active functions or just plans, procedures and guidelines.
- Preconditions (P), which are system conditions that must be fulfilled before a function can be carried out. A common precondition is that another step or process has been completed or that a specific system condition has been established.
- Time (T), which can also be considered a special kind of resource. All processes take place in time and are governed by time. Time can also be a constraint in the sense that there is a time window for an activity (a duration).

If the same values (names) are assigned to aspects of different functions then there is a potential dependency or coupling between the functions. In Figure 24 the Output of Function 1 is same as the Control of Function 2 which creates a potential coupling between these two functions.

Figure 24 Functions and coupling

When FRAM model is prepared an instantiation of the model is done. An instantiation of the model uses detailed information about a particular situation or scenario to create an instance or a specific example of the model which is used to go through the functions in order to develop a common understanding of how the variability of functions may interact or how it did interact in the case of a retrospective analysis. For an event analysis the instantiation typically covers the entire event pathway and the duration of the whole event and the couplings that existed at that time. As a summary application of FRAM consists of the following steps:

- Identify and characterize essential system functions; the characterization can be based on the six connectors of the hexagonal representation.
- Characterize the (context dependent) potential for variability using a checklist.
- Define functional resonance based on identified dependencies among functions.
- Identify barriers for variability (damping factors) and specify required performance monitoring.

There are examples for both accident analysis and risk assessment applications: aircraft collisions (Herrera & Woltjer, 2010) and rail network control (Belmonte, Schoen, & Heurley, 2011).

2.15 STAMP

In 2004 Leveson proposed a model of accident causation called Systems-Theoretic Accident Model and Processes or STAMP (Leveson N. G., 2004). This model considers system theory as a useful way to analyze accidents, particularly system accidents. In STAMP systems are viewed as interrelated components that are kept in a state of dynamic equilibrium by feedback loops of information and control. In this sense, accidents in complex systems do not simply occur due to independent component failures, rather they occur when external disturbances, component failures, or dysfunctional interactions among system components are not adequately handled by the control system. Safety is seen as a control problem, and it is managed by a control structure embedded in an adaptive socio-technical system.

Instead of defining safety management in terms of preventing component failure events, it is defined as a continuous control task to impose the constraints necessary to limit system

behavior to safe changes and adaptations. Accidents can be understood, using this model, in terms of why the controls that were in place did not prevent or detect maladaptive changes, by identifying the safety constraints that were violated (Leveson N. G., 2004).

In STAMP, basic concepts are constraints, control loops and process models, and levels of control. The cause of an accident, instead of being understood in terms of a series of events, is viewed as the result of a lack of constraints imposed on the system design and on the operations, that is, by inadequate enforcement of constraints on behavior at each level of a socio-technical system (Leveson N. G., 2004). Each level imposes constraints on the activity of the level beneath it, i.e. constraints or lack of constraints at a higher level control lower-level behavior. For this, systems need to be modeled in hierarchical levels with control processes and constraints acting on the interfaces between levels. Figure 25 shows a general form of the control structure of a sociotechnical system. Controls of a system must have specific goals and ability to affect and ascertain the state of the system.

Figure 25 General form of a model of sociotechnical control (Leveson N. G., 2012)

The model is used in retrospective and prospective analyses within various domains, e.g. aerospace (Johnson & Holloway, 2003) (Ball, 2015), railroad (Dong, 2012), biodefence (Laracy, 2006), health (O'Neil, 2014) (Leveson & Finkelstein, Systems Approach to Analyzing and Preventing Hospital Adverse Events, 2016), process industry (Rodriguez & Diaz, 2016), outdoor activities (Salmon, Cornelissen, & Trotter, 2012), etc. The lack of formal guidance provides flexibility for the analyst and encourages them to consider interactions across the whole system, look beyond the proximal accident events, and consider the context of the actors involved (Hovden, Størseth, & Tinmannsvik, 2011) (Kontogiannis & Malakis, 2012). An evaluation conducted by (Hollnagel & Speziali, 2008) led the authors to declare that STAMP must still be considered as in need of further development.

From STAMP general theory two different techniques have been developed. One is STPA (System Theoretic Process Analysis) which is a hazard evaluation technique and the other one is CAST (Causal Analysis based on STamp) which is an accident analysis technique. STPA works on a model of the system for the analysis, but since in STAMP accidents are seen as resulting from inadequate control, the model used is a functional control diagram rather than the physical component diagram that is used in traditional hazard analysis techniques like HAZOP. In addition, the analysis is based on how the control is performed rather than hazardous deviations. STPA can be used at any stage of the system life cycle. Depending on when it is used, it provides the information and documentation necessary to ensure that safety constraints are enforced in design, development, manufacturing, and operation including the natural changes in these processes that will occur over time (Leveson N. G., 2012). STAMP and STPA the derived techniques are explained in the next chapter.

2.16 Conclusion

In this chapter a summary of accident models, hazard identification and risk assessment techniques is provided. It is not an exhaustive summary to include all the existing models and techniques. However, it includes the most representative ones. Understanding about how accidents happen has evolved over time. Different types of accident models have been introduced. Notwithstanding, there are many similarities between these accident models. Consequently, these models can be classified in few groups. Different authors classified accident models in different ways. The most common and generally accepted classification sorts accident models into sequential, epidemiological and systemic models where:

- Sequential models describe accidents as chain of events occurring in a temporal order.
- Epidemiological models consider an accidents as a phenomena similar to the spreading of a disease. Accident is seen as the outcome of a combination of factors that happen to exist together in space and time.
- Systemic accident models are based on systems theory. They try to describe accidents as consequence of the performance of a system as a whole. And not only to the specific cause effect relationship or even epidemiological factors.

Models based on chain of events and epidemiological models are considered as traditional models, whereas systemic models are considered as modern models. Heinrich Domino theory that describes an accident as a chain of events is one of the earliest accident causation models. It was updated by several researcher over the years and it can be considered as the origin of

sequential models. Most of the traditional techniques such as Failure Modes and Effects Analysis (FMEA), Fault Tree Analysis (FTA) and Event Tree Analysis (ETA) are based on domino theory.

Sequential models and epidemiological models help in analyzing and understanding accidents caused by failures of physical components or human errors in relatively simple systems. Consequently, techniques developed based on traditional accidents models work well for relatively simple systems. Modern technology has significantly changed the nature of the industry and human role. It changed from mainly manual tasks to knowledge based activities and decision making. As result, the role of human in accidents is changed from human error to human factor, which is more than a simple error made by a person. Another restriction of traditional models is their limitation to fully capture the dynamics and non-linear interactions between system components in complex sociotechnical systems.

Systemic models have their roots in systems theory. Systems theory includes the principles, models, and laws necessary to understand complex interrelationships and interdependencies between components (technical, human, organizational and management) of a complex system. Rasmussen's hierarchical socio-technical framework AcciMap (Rasmussen J. , 1997), Hollnagel's FRAM-Functional Resonance Accident Model (Hollnagel E. , 2004) and Leveson's Systems-Theoretic Accident Model and Processes (STAMP) model (Leveson N. G., 2004) are notable systemic models trying to model complex sociotechnical systems.

Based on the literatures and experience gained in this work after application of CAST and STPA in process industry, it seems that STAMP is one of the most appropriate accident models to handle complex systems.

Chapter 3: Systems-Theoretic Accident Model and Processes (STAMP)

As mentioned already, Nancy Leveson proposed STAMP model in 2004. This chapter provides more detailed information on STAMP, its basis, its comparison with traditional approaches on accident causation and the developed techniques based of this model.

3.1. Introduction

A summary of accident models is provided in the previous chapter and it shows that most of these models consider accidents as a result of a chain or sequence of events. Models based on chain or sequence of events work well for losses caused by failures of physical components and for relatively simple systems. This argument is elaborated in this chapter considering changes that happened in the industry after World War II, which caused the systems to be more complex. These changes were not been reflected in the accident models developed at that time and consequently those accident models had limitation in interpretation of accidents in complex systems. Not only these changes are challenging the accident models but also the accident prevention and risk assessment techniques based on them. Leveson summarized these changes as below (Leveson N. G., 2004):

- **Fast pace of technological changes:** Technology is changing very fast and in some cases it changes faster than the engineering techniques that are required for the application of new technologies. Whatever is learned over time and documented in the engineering practices about how to design in order to prevent accidents could be obsolete and ineffective when new technologies are pushing the old ones to the corner. New technology introduces unknowns into our systems and even unknown unknowns. At the same time as the development of new technology has sprinted forward, the time to market for new products has significantly decreased and strong pressures exist to decrease this time even further. Traditionally, required time to convert a technical discovery to commercial solution was about 30 years. These days, this time is reduced to almost 3 years or less and in many cases it will be out dated in 5 years. This makes it almost impossible to test the systems and designs rigorously in order to assess all the potential risks before make it commercial.
- **Changing nature of accidents:** Digital technology has created a quiet revolution in most fields of engineering. Digital systems introduce new failure modes that are changing the nature of accidents. Many of the approaches that worked on electromechanical components such as replication of components to protect against individual component failure (i.e., redundancy) are almost ineffective in controlling accidents that arise from the use of digital systems and software. Redundancy may even increase risk by adding complexity.
- **New types of hazards:** The most common accident models are based on an underlying assumption that accidents are the result of an uncontrolled and undesired release of energy or interference in the normal flow of energy. The increasing dependence on information systems is, however, creating the potential for loss of information or incorrect information that can lead to unacceptable physical, scientific, or financial losses.
- **Decreasing tolerance for single accidents:** The cost and potential destructiveness of the losses originating from accidents are increasing. The new scientific and

technological discoveries have not only created new or increased hazards (such as radiation exposure and chemical pollution) but have provided the means to harm increasing numbers of people as the scale of systems increases and to impact future generations through environmental pollution and genetic damage. Financial losses and lost potential for scientific advances are also increasing. For example, a spacecraft may take 10 years and up to a billion dollars to build. Learning from accidents needs to be supplemented with increasing emphasis on preventing the first one.

- **Increasing complexity and coupling:** Complexity has many facets, most of which are increasing in the systems, particularly interactive complexity. Systems are designed with potential interactions among the components that sometimes cannot be thoroughly planned, understood, anticipated, or guarded against. The operation of some systems is so complex that cannot be understood by all and sometimes even experts do not have complete information about its potential behavior. Software is an important factor as it allows implementing more integrated, multi-loop control in systems containing large numbers of dynamically interacting components where tight coupling allows disruptions or dysfunctional interactions in one part of the system to have far-ranging rippling effects. The problem is that increased interactive complexity and coupling make it difficult for the designers to consider all the potential system states or for operators to handle all normal and abnormal situations and disturbances safely and effectively. In fact this situation is not specific of these days. Throughout history, inventions and new technology have often gotten ahead of their scientific underpinnings and engineering knowledge, but the result has always been increased risk and accidents until science and engineering caught up. As an example, consider the introduction of high pressure steam engines in the first half of the nineteenth century, which transformed industry and transportation but resulted in frequent and disastrous explosions. While engineers quickly amassed scientific information about thermodynamics, the action of steam in the cylinder, the strength of materials in the engine and many other aspects of steam engine operation, there was little scientific understanding about the buildup of steam pressure in the boiler, the effect of corrosion and decay, and the causes of boiler explosions. High-pressure steam had made the current boiler design obsolete by producing excessive strain on the boilers and exposing weaknesses in the materials and construction of the boilers. Attempts to add technological safety fixes were unsuccessful because engineers did not fully understand what went on in steam boilers: It was not until well after the midcentury that the dynamics of steam generation was understood and effective procedures could be instituted that rapidly reduced accident rates.
- **More complex relationships between humans and automation:** Humans are increasingly sharing control of systems with automation and moving into positions of higher-level decision making with automation implementing the decisions. These changes are leading to new types of human error. All human behavior is influenced by the context in which it occurs, and operators in high-tech systems are often at the mercy of the design of the automation they use. Many recent accidents blamed on operator error could more accurately be labeled as resulting from flawed system and interface design. Inadequacies in communication between humans and machines are becoming an increasingly important factor in accidents.

- **Changing regulatory and public views of safety:** In the increasingly complex and interrelated societal structure, responsibility for safety is shifting from the individual to government. Individuals no longer have the ability to control the risks around them and are demanding that government assume greater responsibility for controlling behavior through laws and various forms of oversight and regulation. As companies come under increasing pressure to satisfy time-to market and budgetary pressures, government will have to step in to provide the protection the public demands.

Considering the abovementioned changes, Leveson explained the limitations of models based on chain or sequence of event as below (Leveson N. G., 2012):

Event-based accident models explain accidents in terms of multiple events sequenced as a chain over time. The events considered almost always involve some type of component failure, human error, or energy-related event. The chains may be branching or there may be multiple chains synchronized using time or common events (Benner, 1975). Forward sequences (as in FMEA or Event Trees) or backward ones (as in Fault Trees) may be used. Other relationships may be represented by the chain in addition to a chronological one, but any such relationship is almost always a direct, linear one. As such, event-based models encourage limited notions of causality, usually linear causality relationships are emphasized, and it is difficult to incorporate non-linear relationships, including feedback. In addition, some important causal factors are difficult to fit into simple event models. For example, studies have found that the most important factor in the occurrence of accidents is management commitment to safety and the basic safety culture in the organization or industry. In event-based models, the causal factors identified depend on the events that are considered and the selection of the conditions related to those events. However, other than the physical events immediately preceding or directly involved in the loss, the choice of events to include is subjective and the selection of conditions to explain the events is even more so.

Although the first event in the chain is often labeled the “initiating event”, the selection of an initiating event is arbitrary and previous events and conditions could always be added. This subjectivity in selection of a stopping point in a backward event chain means that the assignment of a “root cause” for an accident is a purely pragmatic question regarding the stopping rule applied for analysis after the fact there is no well-defined ‘start’ of the causal chain involved in accidents.

Why does the lack of a well-defined stopping point matter? There are two basic reasons for conducting an accident investigation: (1) to assign blame for the accident and (2) to understand why it happened so that future accidents can be prevented. When the goal is to assign blame, the backward chain of events considered often stops when someone or something appropriate to blame is found. As a result, an analysis based on such a model may provide too superficial explanation of why the accident occurred to prevent similar losses. When learning how to prevent accidents is the goal rather than identifying who to punish, then the emphasis in accident analysis needs to shift from cause, which has a potential blame orientation, to understanding accidents in terms of reasons, i.e., why the events and errors occurred. Leveson analyzed some aerospace accidents involving software in some way, and she found that most of the reports stopped after assigning blame (usually to the operators) and never got to the root of why the accident occurred. For example, why the operators made

the errors they did and how to prevent such errors in the future (Leveson N. G., Evaluating accident models using recent aerospace accidents Part1: Event-based Models, 2001).

Event chains developed to explain the accident usually concentrate on the proximate events immediately preceding the loss. Nevertheless, the foundation for an accident is often laid years before. One event simply triggers the loss, but if that event had not happened, another one would have. In the Bhopal disaster, for example, cost cutting and political pressures by Union Carbide and its Indian subsidiary resulted in eliminating refrigeration, putting off maintenance, reducing the workforce, changing worker shift replacement policies, etc., all of which led to the worst industrial accident in history (Bogart, 1989). This degradation in the safety margin occurred over time and without any particular single decision to do so but simply as a series of decisions that moved the plant slowly toward a situation where any slight error would lead to a major accident. Given the overall state of the Bhopal Union Carbide plant and its operation, if the slip disk had not been left out of the pipe washing operation that December day in 1984, something else would have triggered an accident. In fact, a similar leak had occurred the year before, but did not have the same catastrophic consequences (Ayres & Rohatgi, 1987). To identify one event (such as a maintenance worker leaving out the slip disk) or even several events as the root cause or the start of an event chain leading to this accident would be misleading at best.

In addition to subjectivity in selecting the events and stopping point, the links between the events that are chosen to explain the 'cause' are subjective and subject to bias. In the loss of an American Airlines B-757 near Cali, Colombia, in 1995, two significant events were (1) Pilot asks for clearance to take the Rozo approach followed later by (2) Pilot types R into the FMS (Flight Management System). In fact, the pilot should have typed the four letters ROZO instead of 'R', the latter was the symbol for a different radio beacon called Romeo near Bogota, and as a result the aircraft incorrectly turned toward mountainous terrain (Aeronautica Civil of the Republic of Colombia, 1995).

While these events are noncontroversial, the link between the two events could be explained by any of the following (Leveson N. G., 2001):

Crew Procedure Error: in the rush to start the descent, the captain entered the name of the waypoint without normal verification from the other pilot.

Pilot Error: in the rush to start the descent, the pilot executed a change of course without verifying its effect on the flight path.

Approach Chart and FMS Inconsistencies: the identifier used to identify Rozo on the approach chart (R) did not match the identifier used to call up Rozo in the FMS.

FMS Design Deficiency: the FMS did not provide the pilot with feedback that choosing the first identifier listed on the display was not the closest beacon with that identifier.

American Airlines Training Deficiency: the pilots flying into South America were not warned about duplicate beacon identifiers or adequately trained on the logic and priorities used in the FMS on the aircraft.

Manufacturers' Deficiencies: Jeppesen-Sanderson did not inform airlines operating FMS-equipped aircraft of the differences between navigation information provided by Jeppesen-Sanderson FMS navigation databases and Jeppesen-Sanderson approach charts or the logic and priorities employed in the display of electronic FMS navigation information.

International Standards Deficiency: no single worldwide standard provides unified criteria for the providers of electronic navigation databases used in flight management systems.

The selection of one of these linking conditions will greatly influence the 'cause' ascribed to the accident yet all are plausible and each fully explains (according to formal logic) the event sequence. Choosing only one may reflect more on the person or group making the selection than on the accident itself. In fact, understanding this accident and learning enough from it to prevent future accidents requires identifying all these factors: the accident model used should encourage and guide such a comprehensive analysis. Operators, managers, engineers, and regulatory agencies may all have different views of the flawed processes underlying an accident, depending on their perspective and the role they play in the overall socio-technical system. All of these views should be represented in the accident analysis; at the same time, the factual data should be separated from the interpretation of that data.

The countermeasures to prevent accidents considered as chains of events usually involve either removing events or conditions or adding enough gates (required simultaneous conditions or events) that the likelihood of the chaining factors being realized is very low, that is, the accident sequence is broken. Because the most common events considered in event-based models are component failures, engineering design has focused to a great extent on preventing such failures, i.e., increasing component integrity, and on adding redundancy (and gates) to reduce their likelihood of leading to a loss.

This focus on failure events and the reliability engineering techniques to prevent them, however, does not account for (1) social and organizational factors in accidents, (2) system accidents and software errors, (3) human error, (4) adaptation over time, and (5) Emergence and constraints.

1. Social and organizational factors

Event-based models are poor at representing systemic accident factors such as structural deficiencies in the organization, management deficiencies, and flaws in the safety culture of the company or industry. An accident model should encourage a broad view of accident mechanisms that expands the investigation from beyond the proximate events. Miles in describing the basic concepts of systems theory noted that underlying every technology is at least one basic science, although the technology may be well developed long before the science emerges. Overlying every technical or civil system is a social system that provides purpose, goals, and decision criteria (Miles, 1973).

Effectively preventing accidents in complex systems requires using accident models that include that social system as well as the technology and its underlying science. Without understanding the purpose, goals, and decision criteria used to construct and operate systems, it is not possible to completely understand and most effectively prevent accidents.

2. System accidents and software errors

Since World War II, we are increasingly experiencing a new type of accident that arises in the interactions among components (electromechanical, digital, and human) rather than in the failure of individual components. Perrow coined the term system accident to describe it (Perrow, 1984). In contrast, accidents arising from component failures, including the possibility of multiple and cascading failures, might be termed component failure accidents.

Accidents resulting from dysfunctional interactions among system components (system accidents) have received less attention than component failure accidents. This lack of concern may stem partly from the fact that in the simpler systems of the past, analysis and testing allowed exercising the system to detect all potential undesired interactions and changing the system design to eliminate them. Increasing complexity and the introduction of software control is reducing this ability and increasing the incidence of system accidents. System accidents can be explained in terms of inadequate control over component interactions, and prevention requires reducing or eliminating dysfunctional interactions, i.e., interactions that can lead to hazardous states in the controlled process.

The Ariane 5 and Mars Polar Lander losses are examples of system accidents. In both of these accidents, the components did not fail in terms of not satisfying their specified requirements. The individual components operated exactly the way the designers had planned, the problems arose in the unplanned or misunderstood effects of these component behaviors on the system as a whole, that is, errors in the system design rather than the component design, including errors in allocating and tracing the system functions to the individual components. The solution, therefore, lies in system engineering.

Consider an example of a system accident that occurred in a batch chemical reactor in England (Kletz, 1982). The design of this system is shown in Figure 26. The computer was responsible for controlling the flow of catalyst into the reactor and also the flow of water into the reflux condenser to cool off the reaction. Additionally, sensor inputs to the computer were supposed to warn of any problems in various parts of the plant. The programmers were told that if a fault occurred in the plant, they were to leave all controlled variables as they were and to sound an alarm. On one occasion, the computer received a signal indicating a low oil level in a gearbox.

Figure 26 A chemical reactor design (Leveson N. G., 2004)

The computer reacted as its requirements specified: it sounded an alarm and left the controls as they were. By coincidence, a catalyst had been added to the reactor, but the computer had just started to increase the cooling-water flow to the reflux condenser; the flow was therefore kept at a low rate. The reactor overheated, the relief valve lifted, and the contents of the reactor were discharged into the atmosphere.

Note that there were no component failures involved in this accident: the individual components, including the software, worked as specified but together they created a hazardous system state. Merely increasing the reliability of the individual components or protecting against their failure would not have prevented the loss. Prevention required identifying and eliminating or mitigating unsafe interactions among the system components.

Most software-related accidents have been system accidents, they stem from the operation of the software, not from its lack of operation and usually that operation is exactly what the software engineers intended. Thus event models as well as system design and analysis methods that focus on classic types of failure events will not apply to software.

3. Human error

Human error is usually defined as any deviation from the performance of a specified or prescribed sequence of actions. However, instructions and written procedures are almost never followed exactly as operators strive to become more efficient and productive and to deal with time pressures. In studies of operators, even in such highly constrained and high-risk environments as nuclear power plants, modification of instructions is repeatedly found and the violation of rules appears to be quite rational, given the actual workload and time constraints under which the operators must do their job (Fujita, 1991), (Vicente, A Field Study of Operator Cognitive Monitoring at Pickering Nuclear Generating Station, Technical Report CEL 9504, 1995), (Woods, Some results on operator performance in emergency events, 1984). In these situations, a basic conflict exists between error as seen as a deviation

from the normative procedure and error as seen as a deviation from the rational and normally used effective procedure (Rasmussen, Pejtersen, & Goodstein, Cognitive Systems Engineering, 1994).

One implication is that following an accident, it will be easy to find someone involved in the dynamic flow of events that has violated a formal rule by following established practice rather than specified practice. Given the frequent deviation of established practice from normative work instructions and rules, it is not surprising that operator 'error' is found to be the cause of 70–80% of accidents.

Most decisions are sound using a local judgment criterion and given the time and budget pressures and short-term incentives that shape behavior. Experts do their best to meet local conditions and in the busy daily flow of activities are unaware of any potentially dangerous side effects. Each individual decision may appear safe and rational within the context of the individual work environments and local pressures, but may be unsafe when considering the larger socio-technical system as a whole: It is difficult if not impossible for any individual to judge the safety of their decisions when it is dependent on the decisions made by other people in other departments and organizations.

Traditional decision theory research perceives decisions as discrete processes that can be separated from the context and studied as an isolated phenomenon. More recent research has taken a very different approach: Instead of thinking of operations as predefined sequences of actions, human interaction with a system is increasingly being considered to be a continuous control task in which separate decisions or errors are difficult to identify. Edwards, back in 1962, was one of the first to argue that decisions can only be understood as part of an ongoing process (Edwards, 1962). The state of the system is perceived in terms of possible actions, one of these actions is chosen, and the resulting response from the controlled system acts as a background for the next action. Errors then are difficult to localize in the stream of behavior; the effects of less successful actions are a natural part of the search on the part of the operator for optimal performance. Not only are separate decisions difficult to identify in this model of human control, but the study of decision making then cannot be separated from a simultaneous study of the social context, the value system in which it take place, and the dynamic work process it is intended to control (Rasmussen J. , 1990) (Rasmussen J. , 1997) (Vicente, 1999).

As argued by Rasmussen and many others, devising more effective accident models will require shifting the emphasis in explaining the role of humans in accidents from error (deviations from normative procedures) to focus on the mechanisms and factors that shape human behavior, i.e., the performance-shaping mechanisms and context in which human actions take place and decisions are made. Effective approaches to understanding the role of humans in safety must look at the goals and motives behind human behavior. Models are needed that account for the complex role that human decisions and behavior are playing in the accidents occurring in high-tech systems and that handle not simply individual decisions or even sequences of decisions, but the overall decision-making process and the interactions among decisions by multiple, interacting decision makers.

4. Adaptation over time

Any accident model that includes the social system and human error must account for adaptation. To paraphrase a familiar saying, the only constant is that nothing ever remains constant. Systems and organizations continually experience change as adaptations are made in response to local pressures and short-term productivity and cost goals. People adapt to their environment or they change their environment to better suit their purposes. A corollary of this propensity for systems and people to adapt over time is that safety defenses are likely to degenerate systematically through time, particularly when pressure toward cost-effectiveness and increased productivity is the dominant element in decision making. Thus, the redundancy and other precautions added to protect against human error often degenerate over time as work practices adapt to increase efficiency within the local environment. The critical factor here is that such adaptation is not a random process, it is an optimization process depending on search strategies, and thus should be predictable and potentially controllable (Rasmussen J. , 1997).

Woods has stressed the importance of adaptation in accidents. He describes organizational and human failures as breakdowns in adaptations directed at coping with complexity, and accidents as involving a 'drift toward failure as planned defenses erode in the face of production pressures and change' (Woods, 2000).

Similarly, Rasmussen has argued that major accidents are often caused not by a coincidence of independent failures but instead reflect a systematic migration of organizational behavior to the boundaries of safe behavior under pressure toward cost-effectiveness in an aggressive, competitive environment (Rasmussen J. , 1997). The Bhopal accident is one example of this type of systematic migration toward an accident, but most accidents in complex sociotechnical systems exhibit this same behavior. One implication of this viewpoint is that the struggle for a good safety culture will never end because it must fight against the functional pressures of the environment. Improvement of the safety culture will therefore require an analytical approach directed toward the behavior-shaping factors in the environment (Rasmussen J. , 1997).

Humans and organizations can adapt and still maintain safety as long as they stay within the area bounded by safety constraints. However, in the search for optimal operations, humans and organizations will usually close in on and explore the boundaries of established practice, and such exploration implies the risk of occasionally crossing the limits of safe practice unless the constraints on safe behavior are enforced.

For an accident model to handle system adaptation over time, it must consider the processes involved in accidents and not simply event and conditions: Processes control a sequence of events and describe system and human behavior over time rather than considering events and human actions individually. As Rasmussen argues, accident causation must be viewed as a complex process involving the entire sociotechnical system including legislators, government agencies, industry associations and insurance companies, company management, technical and engineering personnel, operations, etc. The idea of modeling sociotechnical systems using process control concepts is not a new one. Jay Forrester in the 1960s, for example, created System Dynamics using such an approach (Forrester, 1961). Industrial engineering models often include both the management and technical aspects of systems. As one example, Suokas describes a production system as four subsystems: physical, human, information, and management (Suokas, 1985). The physical subsystem

includes the objects, equipment, facilities, and materials. The human subsystem controls the physical subsystem. The information subsystem provides flow and exchange of information that authorizes activity, guides effort, evaluates performance, and provides overall direction. The organizational and management subsystem establishes goals and objectives for the organization and its functional components, allocates authority and responsibility, and generally guides activities for the entire organization and its parts.

Rasmussen and Svedung have described a hierarchical model of the sociotechnical system involved in risk management (Rasmussen & Svedung, 2000). At the social and organizational levels of their model, Rasmussen and Svedung use a control-based model, and at all levels they focus on information flow. At each level, however, and between levels, they model the events and their initiation and flow of effects using an event-chain modeling language similar to cause–consequence diagrams (which combine fault trees and event trees). In addition, they focus on the downstream part of the chain following the occurrence of the hazard. This downstream emphasis is common in the process industry, where Rasmussen has done most of his work. Finally, their model focuses on operations, and engineering design activities are treated as input to the model but not as a central part of the model itself.

The model introduced by Leveson (Leveson N. G., 2004), explained later in this section, is built on the ideas used in the upper levels of the Rasmussen–Svedung model, but it continues the control-theoretic approach down through and including the technical system and its development and operations. In addition, more emphasis is placed on the upstream process, i.e., in preventing the occurrence of the hazardous state, on the system development process, and on the components of control beyond information flow. Perhaps most important, the model provides a classification of the specific factors involved in accidents. This classification can be used in accident analysis, accident prevention, and risk assessment.

5. Emergence and constraints

Accident models that consider the entire sociotechnical system must treat the system as a whole, taking into account all facets relating the social to the technical aspects, and not just the parts taken separately. They must consider the relationships between the parts of systems: how they interact and fit together.

In systems theory, complex systems are modeled as a hierarchy of levels of organization, each more complex than the one below, where a level is characterized by having emergent or irreducible properties. Hierarchy theory deals with the fundamental differences between one level of complexity and another. Its ultimate aim is to explain the relationships between different levels: what generates the levels, what separates them, and what links them. Emergent properties associated with a set of components at one level in a hierarchy are related to constraints upon the degree of freedom of those components.

Safety is an emergent property of systems that arises from the interaction of system components. Determining whether a plant is acceptably safe, for example, is not possible by examining a single valve in the plant. In fact, statements about the ‘safety of the valve’ without information about the context in which that valve is used, are meaningless. Conclusions can be reached, however, about the reliability of the valve, where reliability is defined as the probability that the behavior of the valve will satisfy its specification over time

and under given conditions. This is one of the basic distinctions between safety and reliability: Safety can only be determined by the relationship between the valve and the other plant components, that is, in the context of the whole. Therefore, it is not possible to take a single system component in isolation and assess its safety. A component that is perfectly safe in one system may not be when used in another.

Treating safety as an emergent property that arises when the system components interact within a given environment leads to accident models that view accidents as a control problem: accidents occur when component failures, external disturbances, and/or dysfunctional interactions among system components are not adequately handled by the control system. Emergent properties are controlled or enforced by a set of constraints (control laws) related to the behavior of the system components.

Accidents result from interactions among components that violate the safety constraints, in other words, from a lack of appropriate control actions to enforce the constraints on the interactions. In the space shuttle Challenger accident, for example, the O-rings did not adequately control propellant gas release by sealing a tiny gap in the field joint. In the Mars Polar Lander loss, the software did not adequately control the descent speed of the spacecraft, it misinterpreted noise from a Hall effect sensor as an indication the spacecraft had reached the surface of the planet. Accidents such as these, involving engineering design errors, may in turn stem from inadequate control over the development process. Control is also imposed by the management functions in an organization, the Challenger accident involved inadequate controls in the launch decision process, for example.

3.2. STAMP: an accident model based on systems theory

The hypothesis underlying STAMP (Systems-Theoretic Accident Model and Processes) is that system theory is a useful way to analyze accidents, particularly system accidents. In this conception of safety, accidents occur when external disturbances, component failures, or dysfunctional interactions among system components are not adequately handled by the control system, that is, they result from inadequate control or enforcement of safety related constraints on the development, design, and operation of the system.

Safety then can be viewed as a control problem, and safety is managed by a control structure embedded in an adaptive sociotechnical system. The goal of the control structure is to enforce constraints on system development (including both the development process itself and the resulting system design) and on system operation that result in safe behavior. In this framework, understanding why an accident occurred requires determining why the control structure was ineffective. Preventing future accidents requires designing a control structure that will enforce the necessary constraints.

In STAMP, systems are viewed as interrelated components that are kept in a state of dynamic equilibrium by feedback loops of information and control. A system in this conceptualization is not a static design. It is a dynamic process that is continually adapting to achieve its ends and to react to changes in itself and its environment. The original design must not only enforce appropriate constraints on behavior to ensure safe operation, but the system must continue to operate safely as changes occur. The process leading up to an accident (loss event)

can be described in terms of an adaptive feedback function that fails to maintain safety as performance changes over time to meet a complex set of goals and values.

Instead of defining safety management in terms of preventing component failure events, it is defined as a continuous control task to impose the constraints necessary to limit system behavior to safe changes and adaptations. Accidents can be understood, using this model, in terms of why the controls that were in place did not prevent or detect maladaptive changes, that is, by identifying the safety constraints that were violated and determining why the controls were inadequate in enforcing them.

The basic concepts in STAMP are constraints, control loops and process models, and levels of control. Each of these is now described followed by a classification of accident factors based on this model and on basic systems theory concepts.

3.2.1. The central role of constraints in system safety

The most basic concept in the new model is not an event, but a constraint. In systems theory, control is always associated with the imposition of constraints. The cause of an accident, instead of being understood in terms of a series of events, is viewed as the result of a lack of constraints imposed on the system design and on operations, that is, by inadequate enforcement of constraints on behavior at each level of a sociotechnical system. In systems theory terminology, safety is an emergent property that arises when the system components interact within an environment.

Emergent properties are controlled or enforced by a set of constraints (control laws) related to the behavior of the system components. Accidents result from a lack of appropriate constraints on the interactions.

As an example, the unsafe behavior (hazard) in the Challenger loss was the release of hot propellant gases from the field joint. An O-ring was used to control the hazard, i.e., its role was to seal a tiny gap in the field joint created by pressure at ignition. The design, in this case, did not effectively impose the required constraints on the propellant gas release (i.e., it did not adequately seal the gap), leading to an explosion and the loss of the Space Shuttle and its crew. Starting from here, there are then several questions that need to be answered to understand why the accident occurred. Why was this particular design unsuccessful in imposing the constraint, why was it chosen (what was the decision process), why was the flaw not found during development, and was there a different design that might have been more successful? These questions and others consider the original design process.

Understanding the accident also requires examining the contribution of the operations process. One constraint that was violated during operations was the requirement to correctly handle feedback about any potential violation of the safety design constraints, in this case, feedback during operations that the control by the O-rings of the release of hot propellant gases from the field joints was not being adequately enforced by the design. There were several instances of feedback that were not adequately handled, such as data about O-ring blow by and erosion during previous shuttle launches and feedback by engineers who were concerned about the behavior of the O-rings in cold weather. In addition, there was missing

feedback about changes in the design and testing procedures during operations, such as the use of a new type of putty and the introduction of new O-ring leak checks without adequate verification that they satisfied system safety constraints on the field joints. As a final example, the control processes were flawed that ensured unresolved safety concerns were adequately considered before each flight, i.e., flight readiness reviews and other feedback channels to project management making flight decisions.

Why do design constraints play such an important role in complex systems, particularly software-intensive systems? The computer is so powerful and so useful because it has eliminated many of the physical constraints of electromechanical devices. This is both its blessing and its curse: we do not have to worry about the physical realization of our software designs, but we also no longer have physical laws that limit the complexity of these designs, the latter could be called the curse of flexibility (Leveson N. , 1995). Physical constraints enforce discipline on the design, construction, and modification of our design artifacts. Physical constraints also control the complexity of what we build. With software, the limits of what is possible to accomplish are different from the limits of what can be accomplished successfully and safely, the limiting factors change from the structural integrity and physical constraints of our materials to limits on our intellectual capabilities. It is possible and even quite easy to build software that we cannot understand in terms of being able to determine how it will behave under all conditions: We can construct software (and often do) that goes beyond human intellectual limits. The result has been an increase in system accidents stemming from intellectual unmanageability related to interactively complex and tightly coupled designs that allow potentially unsafe interactions to go undetected during development.

The solution to this problem is for engineers to enforce the same discipline on the software parts of the system design that nature imposes on the physical parts. Safety, like any quality, must be built into the system design. When software acts as a controller in complex systems, it represents or is the system design, it embodies or enforces the system safety constraints by controlling the components and their interactions. Control software, then, contributes to an accident by not enforcing the appropriate constraints on behavior or by commanding behavior that violates the constraints. In the batch reactor example of Section 3.1, the software needed to enforce the system safety constraint that water must be flowing into the reflux condenser whenever the flow of catalyst to the reactor is initiated. This system behavioral constraint translates to a constraint on software behavior (a software requirement) that the software must always open the water valve before the catalyst valve.

This control model provides a much better description of how software affects accidents than a failure model. The primary safety problem in computer-controlled systems is not software 'failure' but the lack of appropriate constraints on software behavior, and the solution is to identify the required constraints and enforce them in the software and overall system design. System engineers must identify the constraints necessary to ensure safe system behavior and effectively communicate these behavioral constraints to the software engineers who, in turn, must enforce them in their software.

The relaxation of physical constraints also impacts human supervision and control of automated systems and the design of interfaces between operators and controlled processes (Cook, 1996). Cook argues that when controls were primarily mechanical and were operated

by people located close to the operating process, proximity allowed sensory perception of the status of the process via direct physical feedback such as vibration, sound, and temperature. Displays were directly linked to the process and thus were essentially a physical extension of it. For example, the flicker of a gauge needle in the cab of a train indicated (1) the engine valves were opening and closing in response to slight pressure fluctuations, (2) the gauge was connected to the engine, (3) the pointing indicator was free, etc. In this way, the displays provided a rich source of information about the controlled process and the state of the displays themselves.

The introduction of electromechanical controls allowed operators to control the process from a greater distance (both physical and conceptual) than possible with pure mechanically linked controls. That distance, however, meant that operators lost a lot of direct information about the process, they could no longer sense the process state directly and the control and display surfaces no longer provided as rich a source of information about it (or the state of the controls themselves). The designers had to synthesize and provide an image of the process state to the operators.

An important new source of design errors was the need for the designers to determine beforehand what information the operator would need under all conditions to safely control the process. If the designers had not anticipated a particular situation could occur and provided for it in the original system design, they might also not anticipate the need of the operators for information about it during operations.

Designers also had to provide feedback on the actions of the operators and on any failures that might have occurred. The controls could now be operated without the desired effect on the process, and the operators might not know about it. Accidents started to occur due to incorrect feedback. For example, major accidents (including Three Mile Island) have involved the operators commanding a valve to open and receiving feedback that the valve had opened as a result, when in reality it had not. In these cases, the valves were wired to provide feedback that power had been applied to the valve, but not that it had actually opened. Not only could the design of the feedback about failures be misleading, but the return links were also subject to failure themselves.

Thus, electromechanical controls relaxed constraints on the system design allowing greater functionality. At the same time, they created new possibilities for designer and operator error that had not existed or were much less likely in mechanically controlled systems. The later introduction of computer and digital controls afforded additional advantages and removed even more constraints on the control system design, and introduced more possibility for error. It is this freedom from constraints that makes the design of such systems so difficult. The constraints shaped the system design in ways that efficiently transmitted valuable physical process information and supported the operators' cognitive processes. Proximity provided rich sources of feedback that involved almost all of the senses, enabling early detection of potential problems. We are finding it hard to capture and provide these same qualities in new systems that use computer controls and displays.

The most basic concept in STAMP is a constraint, rather than an event. Accidents are considered to result from a lack of appropriate constraints on system design. The role of the system engineer or system safety engineer is to identify the design constraints necessary to

maintain safety and to ensure that the system design, including the social and organizational aspects of the system and not just the physical ones, enforces them.

3.2.2. Control loops and process models

Instead of decomposing systems and accident explanations into structural components and a flow of events as do most event-based models, STAMP describes systems and accidents in terms of a hierarchy of control based on adaptive feedback mechanisms.

Some basic concepts from systems theory are needed here. In systems theory, open systems are viewed as interrelated components that are kept in a state of dynamic equilibrium by feedback loops of information and control. The plant's overall performance has to be controlled in order to produce the desired product while satisfying cost and quality constraints. In general, to effect control over a system requires four conditions (Ashby, 1956):

1. The controller must have a goal or goals (e.g., to maintain the set point),
2. The controller must be able to affect the state of the system,
3. The controller must be (or contain) a model of the system, and
4. The controller must be able to ascertain the state of the system.

Leveson shows a typical control loop where an automated controller is supervised by a human controller. The dotted lines indicate that the human supervisor may have direct access to system state information (not provided by the computer) and may have ways to manipulate the controlled process other than through computer commands

.

Figure 27 A typical control loop and the process models involved (Leveson N. G., 2004)

The human and/or automated controller(s) obtains information about the process state from measured variables (Condition 4, i.e., feedback) and uses this information to initiate action by manipulating controlled variables (Condition 2) to keep the process operating within predefined limits (constraints) or set points (Condition 1, i.e., the goal) despite disturbances to the process. In general, the maintenance of any open-system hierarchy, either biological or man-made, will require a set of processes in which there is communication of information for regulation or control (Checkland, 1981).

Control actions will, in general, lag in their effects on the process because of delays in signal propagation around the control loop: an actuator may not respond immediately to an external command signal (called dead time); the process may have delays in responding to manipulated variables (time constants); and the sensors may obtain values only at certain sampling intervals (feedback delays). Time lags restrict the speed and extent with which the effects of disturbances (both within the process itself and externally derived) can be reduced and impose extra requirements on the controller, for example, the need to infer delays that are not directly observable.

Condition 3 says that any controller, human or automated, must contain a model of the system being controlled (Conant & Ashby, 1970). This model at one extreme may contain only one or two variables (such as that required for a simple thermostat) while at the other extreme it may require a complex model with a large number of state variables and transitions (such as that needed for air traffic control).

Whether the model is embedded in the control logic of an automated controller or in the mental model maintained by a human controller, it must contain the same type of information: the required relationship among the system variables (the control laws), the current state (the current values of the system variables), and the ways the process can change state. This model is used to determine what control actions are needed, and it is updated through various forms of feedback.

Human controllers interacting with automated controllers, in addition to having a model of the controlled process, must also have a model of the automated controllers' behavior in order to monitor or supervise it (Figure 27). Accidents may result from inaccuracies in this mental model. In the loss of the American Airlines B-757 near Cali, Colombia, the pilots did not understand the model used by the computer for labeling waypoints. Unfortunately, surveys and studies are finding that many operators of high-tech systems do not understand how the automation works.

There may, of course, be multiple human and automated controllers in the control loop, and computers may be in other parts of the control loop than shown in

. For example, computers may act as automated decision aids that provide information to the human controller but do not directly issue control commands to the process actuators: If the software provides decision aiding, however, it is indirectly controlling the process and it must contain a model of the process. Common arguments that in this design the software is not safety critical are not justified, it is still a critical part of the functioning of the control loop and software errors can lead to accidents.

This discussion has been simplified by speaking only of process models. Models will also need to include the relevant properties of the sensors, actuators, and on occasion the environment. An example is the need for an automated controller to have a model of its interface to the human controller(s) or supervisor(s). This interface, which contains the controls, displays, alarm annunciators, etc., is important because it is the means by which the two controller's models are synchronized, and lack of synchronization between the models can lead to system accidents.

3.2.3. Sociotechnical levels of control

In systems theory, systems are viewed as hierarchical structures where each level imposes constraints on the activity of the level beneath it, that is, constraint or lack of constraints at a higher level allow or control lower-level behavior (Checkland, 1981). Control laws are constraints on the relationships between the values of system variables. Safety-related control laws or constraints therefore specify those relationships between system variables that constitute the nonhazardous system states, for example, the power must never be on when the access door is open. The control processes (including the physical design) that enforce these constraints will limit system behavior to safe changes and adaptations.

Modeling complex organizations or industries using system theory involves dividing them into hierarchical levels with control processes operating at the interfaces between levels (Rasmussen J. , 1997). Figure 25 shows a generic socio-technical control model. Each system, of course, must be modeled to reflect its specific features, but all will have a structure that is a variant on this one. The model is similar to the one devised by Rasmussen and

Svedung but their model contains only one control structure and the focus is on operations and not development (Rasmussen & Svedung, 2000).

The model in Figure 25 has two basic hierarchical control structures, one for system development (on the left) and one for system operation (on the right), with interactions between them. An aircraft manufacturer, for example, might only have system development under its immediate control, but safety involves both development and operational use of the aircraft, and neither can be accomplished successfully in isolation: Safety must be designed into the system, and safety during operation depends partly on the original design and partly on effective control over operations. Manufacturers must communicate to their customers the assumptions about the operational environment upon which the safety analysis was based, as well as information about safe operating procedures. The operational environment in turn provides feedback to the manufacturer about the performance of the system during operations.

Between the hierarchical levels of each control structure, effective communications channels are needed, both a downward reference channel providing the information necessary to impose constraints on the level below and an upward measuring channel to provide feedback about how effectively the constraints were enforced. Feedback is critical in any open system in order to provide adaptive control. At each level, inadequate control may result from missing constraints, inadequately communicated constraints, or from constraints that are not enforced correctly at a lower level.

The top two levels of each of the two generic control structures are government and general industry groups. The government control structure in place to control development may differ from that control operations. The appropriate constraints in each control structure and at each level will vary but in general may include technical design and process constraints, management constraints, manufacturing constraints, and operational constraints.

At the highest level in both the system development and system operation hierarchies is legislature that controls safety by passing laws and by establishing and funding government regulatory structures. Feedback as to the success of these controls or the need for additional ones comes in the form of government reports, hearings and testimony, lobbying by various interest groups, and, of course, accidents.

The next level contains government regulatory agencies, industry associations, user associations, insurance companies, and the court system. Unions may play a role in ensuring safe system operations or worker safety in manufacturing. The legal system tends to be used when there is no regulatory authority and the public has no other means to encourage a desired level of concern for safety in company management. The constraints generated at this level and enforced on the companies are usually passed down in the form of policy, regulations, certification, standards (by trade or user associations), or threat of litigation. Where there is a union, safety-related constraints on operations or manufacturing may result from union demands and collective bargaining.

In the development control structure (shown on the left in Figure 25), constraints imposed on behavior by government and other entities must be reflected in the design of company safety policy, standards, and allocation of resources. Recent trends from management by oversight

to management by insight reflect differing levels of feedback control exerted over the lower levels and a change from prescriptive management control to management by objectives, where the objectives are interpreted and satisfied according to the local context (Rasmussen J. , 1997). Attempts to delegate decisions and to manage by objectives require an explicit formulation of the value criteria to be used and an effective means for communicating the values down through society and organizations. The impact of specific decisions at each level on the objectives and values passed down need to be adequately and formally evaluated. While some generic functions will be required at a particular level to avoid accidents, the details about how the functions will be accomplished may be left to the lower levels. New objectives may also be added at each level. Feedback is required to measure how successfully the functions were performed.

3.2.4. A classification of accident factors

It was hypothesized earlier that accidents result from inadequate control, i.e., the control loop creates or does not handle dysfunctional interactions in the process including interactions caused both by component failures and by system design flaws. Starting from this basic definition of an accident, the process that leads to accidents can be understood in terms of flaws in the components of the system development and system operations control loops in place during design, development, manufacturing, and operations. A classification of those flaws are provided here:

1. Inadequate Enforcement of Constraints (Control Actions)

- 1.1. Unidentified hazards
- 1.2. Inappropriate, ineffective, or missing control actions for identified hazards
  - 1.2.1. Design of control algorithm (process) does not enforce constraints
    - Flaw(s) in creation process
    - Process changes without appropriate change in control algorithm (asynchronous evolution)
    - Incorrect modification or adaptation
  - 1.2.2. Process models inconsistent, incomplete, or incorrect (lack of linkup)
    - Flaw(s) in creation process
    - Flaws(s) in updating process (asynchronous evolution)
    - Time lags and measurement inaccuracies not accounted for
  - 1.2.3. Inadequate coordination among controllers and decision makers (boundary and overlap areas)

2. Inadequate Execution of Control Action

- 2.1. Communication flaw
- 2.2. Inadequate actuator operation
- 2.3. Time lag

3. Inadequate or missing feedback

- 3.1. Not provided in system design
- 3.2. Communication flaw
- 3.3. Time lag
- 3.4. Inadequate sensor operation (incorrect or no information provided)

The classification can be used during accident analysis or accident prevention activities to assist in identifying the factors involved in an accident (or a potential accident) and in showing their relationships.

In each control loop at each level of the sociotechnical control structure, unsafe behavior results from either a missing or inadequate constraint on the process at the lower level or inadequate enforcement of the constraint leading to its violation. Because each component of the control loop may contribute to inadequate control, classification starts by examining each of the general control loop components and evaluating their potential contribution: (1) the controller may issue inadequate or inappropriate control actions, including inadequate handling of failures or disturbances in the physical process; (2) control actions may be inadequately executed, or (3) there may be missing or inadequate feedback. These same general factors apply at each level of the sociotechnical control structure, but the interpretations (applications) of the factor at each level may differ.

For each of the factors, at any point in the control loop where a human or organization is involved, it will be necessary to evaluate the context in which decisions are made and the behavior-shaping mechanisms (influences) at play in order to understand how and why unsafe decisions have been made.

Note that accidents caused by basic component failures are included here. Component failures may result from inadequate constraints on the manufacturing process; inadequate engineering design such as missing or incorrectly implemented fault tolerance; lack of correspondence between individual component capacity (including humans) and task requirements; unhandled environmental disturbances; inadequate maintenance, including preventive maintenance; physical degradation over time (wear out), etc. Component failures may be prevented by increasing the integrity or resistance of the component to internal or external influences or by building in safety margins or safety factors. They may also be avoided by operational controls, such as operating the component within its design envelope and by periodic inspections and preventive maintenance. Manufacturing controls can reduce deficiencies or flaws introduced during the manufacturing process. The effects of component failure on system behavior may be eliminated or reduced by using redundancy. The model goes beyond simply blaming component failure for accidents and requires that the reasons be identified for why those failures occurred and led to an accident. Classification of flaws is explained below:

1. Inadequate enforcement of safety constraints

The first factor, inadequate control over (enforcement of) safety constraints, can occur either because hazards (and their related constraints) were not identified or because the control actions do not adequately enforce the constraint. The latter may, in turn, result from flawed control algorithms, inconsistent or incorrect process models used by the control algorithms, or by inadequate coordination among multiple controllers and decision makers.

Control algorithms may not enforce safety constraints because they are inadequately designed originally, the process may change and thus they become inadequate, or they may be inadequately modified by maintainers (if they are automated) or through various types of natural adaptation if they are implemented by humans. Many accidents relate to asynchronous evolution where one part of a system (in our case the hierarchical control structure) changes without the related necessary changes in other parts (Leplat, 1987). Changes to subsystems may be carefully designed, but consideration of their effects on other parts of the system, including the control aspects, may be neglected or inadequate.

Asynchronous evolution may also occur when one part of a properly designed system deteriorates. In both these cases, the erroneous expectations of users or system components about the behavior of the changed or degraded subsystem may lead to accidents.

Communication is a critical factor here as well as monitoring for changes that may occur and feeding back this information to the higher-level control. For example, the safety analysis process that generates constraints always involves some basic assumptions about the operating environment of the process. When the environment changes such that those assumptions are no longer true, the controls in place may become inadequate.

To summarize, process models can be incorrect from the beginning (where correct is defined in terms of consistency with the current process state and with the models being used by other controllers) or they can become incorrect due to erroneous or missing feedback or measurement inaccuracies. They may also be incorrect only for short periods of time due to time lags in the process loop.

When there are multiple controllers (human and/or automated), control actions may be inadequately coordinated, including unexpected side effects of decisions or actions or conflicting control actions. Communication flaws play an important role here.

Leplat suggests that accidents are most likely in boundary areas or in overlap areas where two or more controllers (human and/or automated) control the same process (Leplat, 1987). In both boundary and overlap areas Figure 28, the potential exists for ambiguity and for conflicts among independently made decisions.

Figure 28 Two Types of Coordination Problems (Leveson N. G., 2004)

When controlling boundary areas, there can be confusion over who is actually in control (which control loop is currently exercising control over the process), leading to missing control actions. The functions in the boundary areas are often poorly defined. For example, Leplat cites an iron and steel plant where frequent accidents occurred at the boundary of the blast furnace department and the transport department. One conflict arose when a signal informing transport workers of the state of the blast furnace did not work and was not repaired because each department was waiting for the other to fix it.

Overlap areas exist when a function is achieved by the cooperation of two controllers or when two controllers exert influence on the same object. Such overlap creates the potential for conflicting control actions (dysfunctional interactions among control actions). In Leplat's study of the steel industry, he found that 67% of technical incidents with material damage

occurred in areas of co-activity, although these represented only a small percentage of the total activity areas.

2. Inadequate execution of the control action

A second way for constraints to be violated in the controlled process is if there is a failure or inadequacy in the reference channel, i.e., in the transmission of control commands or in their execution (actuator fault or failure). A common flaw in system development is that the safety information gathered or created by the system safety engineers (the hazards and the necessary design constraints to control them) is inadequately communicated to the system designers and testers.

3. Inadequate or missing feedback

The third flaw leading to system hazards involve inadequate feedback. A basic principle of systems theory is that no control system will perform better than its measuring channel. Important questions therefore arise about whether the controllers or decision makers (either automated or human) have the necessary information about the actual state of the controlled process to satisfy their objectives. This information is contained in their process models and updating these models correctly is crucial to avoiding accidents. Feedback may be missing or inadequate because such feedback is not included in the system design, flaws exist in the monitoring or feedback communication channel, the feedback is not timely, or the measuring instrument operates inadequately.

Chapter 4: Techniques and tools based on STAMP

According to Leveson (Leveson N. G., 2012), STAMP provides a new theoretical foundation for system safety on which new and more powerful techniques and tool for system safety can be constructed. Some examples of tools developed based on STAMP are named here:

- CAST: Causal Analysis based on Systems Theory (Leveson N. G., 2012)
- STPA: System Theoretic Process Analysis (Leveson N. G., 2012)
- STECA: Systems-Theoretic Early Concept Analysis (Fleming, 2015)
- EWaSAP: Early Warning Sign Analysis based on the STPA (Dokas, Feehan, & Imran, 2013)

The most important tools developed based on STAMP are CAST (Causal Analysis based on Systems Theory) for accident investigation and analysis and STPA (System Theoretic Process Analysis) for hazard assessment and risk analysis. There tools are explained in the following sections.

Further than accident investigation and analysis and hazard assessment and risk analysis, STAMP has also been used for other purposes like identification of leading indicators (Leveson N. , 2015) (Ball, 2015) (Khawaji, 2012), Systemic Risk Management Approach for CO2 Capture Transport and Storage Projects (Samadi, 2012), management of change (DNV GL Limited Oil & Gas, 2018), biodefense (Laracy, 2006), etc.

4.1. CAST

According to (Leveson N. G., 2012), CAST (Causal Analysis based on STAMP) is an accident analysis approach based on STAMP model that can be used to identify the questions that need to be answered to fully understand why the accident occurred. It provided the basis for maximizing learning from the events. The use of CAST does not lead to identifying single causal factors or variables. Instead it provides the ability to examine the entire sociotechnical system design to identify the weaknesses in the existing safety control structure and to identify changes that will not simply eliminate symptoms but potentially all the causal factors, including the systemic ones.

One goal of CAST is to get away from assigning blame and instead to shift the focus to why the accident occurred and how to prevent similar losses in the future. To accomplish this goal, it is necessary to minimize hindsight bias and instead to determine why people behaves the way they did, given the information they had at the time.

Here the steps to go through in doing CAST analysis are described. An accident investigation process is not being specified here, but only a way to document and analyze the results of such a process. Accident investigation is a much larger topic and here it only considers how to analyze the data once it has been collected and organized. The accident analysis process described here does, however, contribute to determine what questions should be asked during the investigation. When attempting to apply CAST analysis to existing accident reports, it often become apparent that crucial information was not obtained, or at least not included in

the report, that is needed to fully understand why the loss occurred and how to prevent future occurrences.

In STAMP, an accident is regarded as involving a complex process, not just individual events. Accident analysis in CAST then entails understanding the dynamic process that led to the loss. That accident process is documented by showing the sociotechnical safety control structure for the system involved and the safety constraints that were violated at each level of this control structure and why. The analysis results in multiple views of the accident, depending on the perspective and level from which the loss is being viewed.

Although the process is described in terms of steps or parts, no implication is being made that the analysis process is linear or that one step must be completed before the next one is started. The steps of the CAST are as following:

1. Identify the system(s) and hazards(s) involved in the loss.
2. Identify the system safety constraints and system requirements associated with that hazard
3. Document the safety control structure in place to control the hazard and enforce the safety constraints. This structure includes the roles and responsibilities of each component in the structure as well as the controls provided or created to execute their responsibilities and the relevant feedback provided to them to help them do this. This structure may be completed in parallel with the later steps.
4. Determine the proximate events leading to the loss
5. Analyze the loss at the physical system level. Identify the contribution of each of the following to the events: physical and operational controls, physical failures, dysfunctional interactions, communication and coordination flaws, and unhandled disturbances. Determine why the physical controls in place were ineffective in preventing the hazard.
6. Moving up the levels of the safety control structure, determine how and why each successive higher level allowed or contributed to the inadequate control at the current level. For each system safety constraints, either the responsibility for enforcing it was never assigned to a component in the safety control structure or a component or component did not exercise adequate control to ensure their assigned responsibilities (safety constraints) were enforced in the components below them. Any human decisions or flawed control actions need to be understood in terms of (at least): the information available to the decision maker as well as any required information that was not available, the behavior-shaping mechanisms (the context and influences on the decision-making process), the value structure underlying the decision, and any flaws in the process models of those making the decisions and why those flaws existed.
7. Examine overall coordination and communication contribution to the loss.
8. Determine the dynamics and changes in the system and the safety control structure relating to the loss and any weakening of the safety control structure over time.
9. Generate recommendations.

The first three steps are the same ones that form the basis of all the STAMP-based techniques. In general. The description of the role of each component in the control structure will include the following:

- Safety Requirements and Constraints
- Controls
- Context
  - Roles and responsibilities
  - Environmental and behavior-shaping factors
- Dysfunctional interactions, failures, and flawed decisions leading to erroneous control actions
- Reasons for the flawed control actions and dysfunctional interactions
  - Control algorithm flaws
  - Incorrect process or interface models
  - Inadequate coordination or communication among multiple controllers
  - Reference channel flaws
  - Feedback flaws

The result of an accident analysis using CAST is presented in chapter 5 and the outcome is compared with the result of accident analysis using other methods.

4.2. STPA

STPA (System Theoretic Process Analysis) is an approach to hazard analysis based on the STAMP. According to Leveson (Leveson N. G., 2012), the primary reason for developing STPA was to include the new causal factors identified in STAMP that are not handles by older techniques like Fault Tree Analysis, Event Tree Analysis, FMEA and HAZOP. More specifically, the hazard analysis technique should include design errors, including software flaws; component interaction accidents; cognitively complex human decision-making errors; and social, organizational, and management factors contributing to accidents. In short, the goal is to identify accident scenarios that encompass the entire accident process, not just the electromechanical components. While attempts have been made to add new features to traditional hazard analysis techniques to handle new technology, these attempts have had limited success because the underlying assumption of the old techniques and the causality models on which they are based do not fit the characteristics of these new causal factors. STPA is based on the new causality assumptions identified before.

An additional goal in the design of STPA was to provide guidance to the users in getting good results. Fault tree and event tree analysis provide little guidance to the analyst, the tree itself is simply the result of the analysis. Both the model of the system being used by the analyst and the analysis itself are only in the analyst's head. Analyst expertise in using these techniques is crucial, and the quality of the fault or event trees that result varies greatly.

HAZOP, widely used in the process industries, provides much more guidance to the analyst. HAZOP is based on a slightly different accident model than fault and event trees, namely that accidents result from deviations in system parameters, such as too much flow through a pipe or backflow when forward flow is required. HAZOP uses a set of guidewords to examine each part of a plant piping and instrumentation diagram, such as more, less, opposite. Both guidance in performing the process and a concrete model of the physical structure of the plant are therefore available.

Like HAZOP, STPA works on a model of the system and has 'guidewords' to assist in the analysis, but because in STAMP accidents are seen as resulting from inadequate control the model used is functional control diagram rather than a physical component diagram. In addition, the set of guidewords is based on lack of control rather than physical parameter deviations. While engineering expertise is still required, guidance is provided for the STPA process to provide some assurance of completeness in the analysis.

The third and final goal for STPA is that it can be used before a design has been created, that is, it provides the information necessary to guide the design process, rather than requiring a design to exist before the analysis can start. Designing safety into a system, starting in the earliest conceptual design phases, is the most cost-effective way to engineer safer systems. The analysis technique must also, of course, be applicable to existing designs or systems when safety-guided design is not possible.

STPA can be used at any stage of the system life cycle. It has the same general goals as any hazard analysis technique: accumulate information about how the behavioral safety constraints, which are derived from the system hazards, can be violated. Depending on when it is used, it provides the information and documentation necessary to ensure the safety constraints are enforced in system design, development, manufacturing, and operations, including the natural changes in these processes that will occur over time.

STPA uses a functional control diagram and the requirements, system hazards, and the safety constraints and safety requirements for the component as defined before. When STPA is applied to an existing design, this information is available when the analysis process begins. When STPA is used for safety-guided design, only the system-level requirements and constraints may be available at the beginning of the process. In the latter case, these requirements and constraints are refined and traced to individual system components as the iterative design and analysis process proceeds.

STPA has two main steps:

1. Identify the potential for inadequate control of the system that could lead to a hazardous state. Hazardous states result from inadequate control or enforcement of the safety constraints, which can occur because:
  - a. A control action required for safety is not provided or not followed.
  - b. An unsafe control action is provided.
  - c. A potentially safe control action is provided too early or too late, that is, at the wrong time or in the wrong sequence.
  - d. A control action required for safety is stopped too soon or applied too long.
2. Determine how each potentially hazardous control action identified in step 1 could occur.

- a. For each unsafe control action, examine the parts of the control loop to see if they could cause it. Design controls and mitigation measures if they do not already exist or evaluate existing measures if the analysis is being performed on an existing design. For multiple controllers of the same component or safety constraints, identify conflicts and potential coordination problems.
- b. Consider how the designed controls could degrade over time and build in protection, including
  - i. Management of change procedures to ensure safety constraints are enforced in planned changes.
  - ii. Performance audits where the assumptions underlying the hazard analysis are the preconditions for the operational audits and controls so that unplanned changes that violate the safety constraints can be detected.
  - iii. Accident and incident analysis to trace anomalies to the hazards and to the system design.

While the analysis can be performed in one step, dividing the process into discrete steps reduces the analytical burden on the safety engineers and provides a structured process for hazard analysis. The information from the first step (identifying the unsafe control actions) is required to perform the second step (identifying the cause of the unsafe control actions).

Leveson and Thomas published a handbook to support correct application of STPA (Leveson & Thomas, 2018). Based on STPA handbook, in order to carry out STPA it is required to do steps shown in Figure 29.

Figure 29 Overview of the basic STPA Method (Leveson & Thomas, 2018)

Defining the purpose of the analysis is the first step with any analysis method. Losses, hazards and system boundaries have to be defined in this step. The second step is to build a model of the system called a control structure. A control structure captures functional relationships and interactions by modeling the system as a set of feedback control loops. The control structure usually begins at a very abstract level and is iteratively refined to capture

more detail about the system. This step does not change regardless of whether STPA is being applied to safety, security, privacy, or other properties.

The third step is to analyze control actions in the control structure to examine how they could lead to the losses defined in the first step. These unsafe control actions are used to create functional requirements and constraints for the system. This step also does not change regardless of whether STPA is being applied to safety, security, privacy, or other properties.

The fourth step identifies the reasons why unsafe control might occur in the system. Scenarios are created to explain:

1. How incorrect feedback, inadequate requirements, design errors, component failures, and other factors could cause unsafe control actions and ultimately lead to losses.
2. How safe control actions might be provided but not followed or executed properly, leading to a loss.

Once scenarios are identified, they can be used to create additional requirements, identify mitigations, drive the architecture, make design recommendations and new design decisions (if STPA is used during development), evaluate/revisit existing design decisions and identify gaps (if STPA is used after the design is finished), define test cases and create test plans, develop leading indicators of risk, and for other uses.

STPA is applied to a section of a gas production plant and the outcome is presented in chapter 6 that is compared with the result of plant HAZOP.

Chapter 5: Case Study: Analyzing Chevron Richmond Refinery Accident with AcciMap, FRAM and CAST

In this chapter the following systemic accident models are compared: STAMP (CAST methodology), FRAM and AcciMap. According to Underwood and Waterson, these models are the most cited ones within research society: Underwood and Waterson identified 13 systemic models within the 449 non-duplicated articles collected during their literature search (Underwood & Waterson, 2012). They performed a citation search for these techniques and three most cited models were STAMP, FRAM and AcciMap by 52.0%, 19.9% and 17.9% of the identified references respectively.

A real accident, 2012 Chevron Richmond Refinery accident, is selected to be used for the comparison study. U.S. Chemical Safety and Hazard Investigation Board (CSB) carried out an investigation on this accident and the report includes an AcciMap developed by the investigation team. The accident is also analyzed by the author using the other mentioned accident models for comparison.

The Chevron Richmond Refinery Accident is explained below and then the analysis done by each model is provided followed by a discussion section.

5.1. Chevron Richmond Refinery Accident description

Based on CCPS report, at approximately 3:50 p.m. on August 6, 2012, an outside operator performing routine checks of piping and equipment found an 18-inch puddle of what appeared to be a diesel-like material on the refinery concrete pad. Identifying that the leak was occurring from overhead, the operator observed intermittent drips as they accumulated on the underside of an insulated pipe 14 feet above ground level. The leaking pipe was identified to be a portion of the 4-sidecut piping that originated on the Crude Column. Visually analyzing the piping, the operator determined that the line could not be isolated from the process.

The operator's supervisor arrived at the leak location, shortly followed by the shift team leader. These individuals observed that the leak was dripping at a rate of approximately 40 drips per minute. The piping was insulated, so the individuals gathered near the leak could not identify its precise source (Figure 30). They concluded that the leak was not significant enough to require a shutdown, but was still a serious situation. Shortly after 4:00 p.m., they called the Chevron Fire Department to the scene, a typical practice at the refinery when leaks are discovered. Firefighters began to arrive at approximately 4:07 p.m. and established an Incident Command structure. A hot zone of 20 feet by 20 feet was established and taped off around the leak location by the Incident Commander. The area outside of the hot zone was considered the cold zone, or safe zone.

Figure 30 Photo taken of the leaking 4-sidecut pipe on August 6, 2012, at the Chevron Richmond Refinery. Insulation obscured the actual leak location. Stain signifies where hydrocarbon process fluid was leaking from the 4-sidecut piping

Beginning at approximately 4:15 p.m., many additional personnel were called to the scene of the leak to assist in the leak analysis. Various operations personnel were called to the leak. Two Chevron inspectors reported to the leak location to provide information on inspection history of the 4-sidecut line. The lead Crude Unit process engineer also arrived at the leak location to determine an estimate of the hole size and the quantity of material leaking so that proper environmental release calculations could be performed. At approximately 5:00 p.m., the shift team leader left the scene of the leak and went to the control room. He directed the board operator to reduce the feed to the 4-sidecut line by 5,000 bpd. Timeline of the events on the day of accident is provided in Figure 31.

Figure 31 Timeline of events on August 6, 2012

Ultimately, a large group of Chevron employees, 40 people in total throughout the hours leading to the incident, accumulated at the leak location. They began discussing their options to mitigate or stop the leak. The inspectors informed the group that the 4-sidecut pipe walls were thinning due to sulfidation corrosion, but data collected as recently as two months prior indicated the 4-sidecut line had sufficient wall thickness to last until the next turnaround in 2016. This assessment led the group to believe that a localized mechanism, such as abrasion on the line from a pipe support near the dripping location, was the likely cause of the leak. The group then called the leak repair contractor to the leak location to assess the possibility of clamping the line in an effort to stop the leak.

The group then decided to remove the insulation from the 4-sidecut pipe to determine the cause of the leak, a practice Chevron personnel call “daylighting the leak”. This procedure, they determined, would help in the decision either to repair the leak on-line or to shut down the unit.

During preparation for the daylighting activity, the fire engine was repositioned in the cold zone to a location approximately 65 feet from the leak, fire monitors were set up pointing towards the leak location, and two hose lines were run from the fire engine to a position near the 4-sidecut piping. Two teams of three firefighters operated the hoses. All hoses and monitors were at-the-ready, able to respond should any incident occur.

The first attempt to remove insulation was made by pulling on the insulation bands from the ground using a pike pole. This was unsuccessful. Rather, the piping actually moved from the force of the pulling, so the group determined it was too dangerous trying to remove the insulation in that way. The group then decided that scaffolding should be built to provide easy access so that firefighters could manually cut loose the piping insulation.

At this point, shift change was occurring. Some individuals left for the day, and some volunteered to stay past their shift end time after their relief showed up. This change resulted in an increase of people standing near the 4-sidecut leak location.

Contractors arrived at the scene to build the scaffold. During a pre-response safety meeting consisting of the Incident Commander, a safety officer, firefighters, and key operations personnel, one group of firefighters operating a hose was directed to spray the scaffold builders should an incident occur, and the other group of firefighters operating the second hose was directed to spray the pipe if needed. Three scaffold contractors then built the scaffold beneath the leaking 4-sidecut pipe.

Once the scaffolding was built, two firefighters were directed to climb the scaffold and remove the aluminum sheathing and insulation (shown in Figure 30) from the 4-sidecut pipe. The battalion chief was aware that vapors leaking from under the insulation could mix with air and “light off,” or catch on fire, as the insulation was removed, so the firefighters made preparations for such a possibility by being at-the-ready with fire hoses. The firefighters on the scaffolding began to remove the aluminum sheathing surrounding the insulation by using a hook to pull the bands securing the insulation and sheathing sufficiently away from the insulation to allow for snipping the bands with cutters. Using this technique, the firefighters were able to remove several three-foot sections of the aluminum sheathing surrounding the insulation.

As the firefighters were removing the sheathing of the 4-sidecut line (shown in Figure 30), white hydrocarbon vapor visibly began to emerge from under the now-exposed insulation material. The firefighters continued to remove the sheathing despite the formation of hydrocarbon vapor. During the continued sheathing removal, insulation that was soaked with hot 4-sidecut hydrocarbon autoignited once exposed to oxygen only feet from the firefighters. The team immediately put out the fire, and both firefighters quickly came down from the scaffold.

The firefighters on the scaffolding successfully removed much of the aluminum sheathing surrounding the insulation; however, underlying insulation still obscured the location of the leak. Directed by the operations personnel, the Chevron Fire Department sprayed the insulation with hard, straight streams using the fire hoses in an attempt to knock the insulation off the pipe. The hose teams knocked off the insulation up to the location where the aluminum sheathing had been removed. At this point, they realized that the leak had significantly worsened; hydrocarbon liquid was now spraying from the pipe. Several operations managers present then decided to shut the unit down, an action that requires hours to complete.

A vapor cloud quickly began to accumulate. The hose teams attempted to keep the cloud at bay by spraying it with firefighting water. Suddenly, the vapor cloud worsened, engulfing 19 firefighters and operators standing in both the hot zone and cold zone in the hot hydrocarbon cloud. The cloud was dense and very hot, and many of the individuals caught in the cloud were not able to see anything around them.

One person caught in the cloud told the CSB that he could not see his hand if he had held it directly in front of his face. Each person engulfed in the cloud began working their way out of the vapor cloud. Several of the firefighters operating the two hoses dropped to their hands and knees to follow their hose lines to safety, feeling their way out of the cloud. At approximately 6:30 p.m., two minutes after the large vapor cloud formed, the light gas oil ignited. Eighteen employees safely escaped from the cloud just before ignition. One employee, a firefighter, was inside a fire engine that was engulfed in the fireball when the light gas oil ignited (Figure 32). He told CSB interviewers, “... All I could see [was] heavy hydrocarbon-type boiling fire in every window of that truck. I can’t even begin to

A photograph of a severely damaged white truck cab, likely a fire engine, with significant structural damage and debris. The truck is parked in an industrial or construction area. A red caution tape with the text "ONLY DANGER AUTHORIZED ENTRY ONLY DANGER AUTHORIZED ENTRY ONLY DANGER AUTHORIZED ENTRY ONLY DANGER AUTHORIZED" is stretched across the foreground.

The leak resulted in a large plume of vapor which traveled across the surrounding area. The ignition and subsequent burning of the hydrocarbon process fluid created a large black cloud of smoke, which also swept across the surrounding area (Figure 33). This situation resulted in a Community Warning System (CWS) Level 3 alert, and a shelter-in-place advisory (SIP) was issued at 6:38 p.m. for Richmond, San Pablo, and North Richmond. It was lifted later that night at 11:12 p.m. after the fire was fully under control. In the weeks following the incident, nearby medical facilities received over 15,000 members of the public seeking treatment for ailments including breathing problems, chest pain, shortness of breath, sore throat, and headaches. According to information provided to the CSB by local hospitals, approximately 20 people were admitted to local hospitals as inpatients for treatment.

Figure 33 Initial vapor cloud formation (white cloud) and subsequent ignition (black smoke) as seen from a pier in San Francisco, California

5.2. Chevron Richmond Refinery Accident analysis using CAST model

In this study Chevron accident is analyzed using CAST methodology that is based on STAMP model. The CAST methodology is followed and following steps are done:

- STEP 1: Identify the system(s) and hazard(s) involved in the loss
- STEP 2: Identify the system safety constraints and system requirements associated with that hazard
- STEP 3: Document the safety control structure in place to control the hazard and enforce the safety constraints
- STEP 4: Determine the proximate events leading to the loss
- STEP 5: Analyze the loss at the physical system level
- STEP 6: Moving up the levels of the safety control structure, determine how and why each successive higher level allowed or contributed to the inadequate control at the current level
- STEP 7: Review contributions of coordination or communication failures
- STEP 8: Determine the dynamics and changes in the system and the safety control structure relating to the loss and any weakening of the safety control structure over time
- STEP 9: Generate recommendations

All the steps are explained in detail below.

STEP 1: Identify the system(s) and hazard(s) involved in the loss

System is defined as below:

System: Richmond Refinery is the system to be analyzed here.

Accident is defined as below:

Accident: Accident is the pipe rupture and fire in Chevron Richmond refinery on Aug 6th 2012.

And system hazard is defined as below:

System Hazard: Uncontrolled release of hydrocarbon from the process and subsequent fire, explosion or exposure associated with uncontrolled release is the hazard.

STEP 2: Identify the system safety constraints and system requirements associated with that hazard

The required system safety constraints (SC) to prevent the hazards are:

SC1: Hydrocarbon must be contained in the process and under control at all times. This excludes planned and designed releases like sampling or venting.

SC2: Safety measures must be taken to minimize exposure of refinery personnel and prevent fire and explosion if inadvertent release occurs.

SC3: Plan, organization, arrangements and protective measures must be available to protect workers and assets in the plant in case of inadvertent fire and explosion and also to minimize public exposure and losses to the outside community

SC4: Medical and emergency response equipment must be available and effective to treat and evacuate injured individuals and minimize and mitigate impacts to assets.

The system requirements necessary to prevent the mentioned hazard and appropriate for the Richmond refinery safety roles and responsibilities are:

SR1: Operation must control process parameters within design and operating envelope.

SR2: Operation and maintenance staff must maintain equipment and piping integrity according to the design, operating manual and maintenance procedures.

SR3: Safety devices like fire and gas system, firefighting system, flare system and emergency shutdown system must be operational and maintained at all times.

SR4: Safety Critical Equipment and refinery emergency procedure must be provided to prevent fire and explosion and reduce exposure in the event of an inadvertent hydrocarbon release

SR5: Emergency Response Plans and Emergency response equipment must be available and operational at all time to minimize the impact of fire and explosion. Plant has to be designed in a way that during emergency, personnel can access and bring emergency equipment with any limitation.

SR6: Training like safe execution of job, proper use of safety equipment, safety related roles and responsibilities, job related hazards and emergency response must be given to refinery personnel.

SR7: Adequate education must be given to responsible for safety in Richmond City and Contra Costa County.

SR8: In order to reduce the risk of exposure and minimize fire and explosion consequences, municipal safety equipment, emergency equipment and emergency procedures must be provided.

STEP 3: Document the safety control structure in place to control the hazard and enforce the safety constraints

A high-level system control structure was created to capture the major controllers as well as the control actions and feedback flow. The system control structure is depicted in Figure 34. It shows our best reconstruction of the safety control structure from what we could obtain from the accident reports

and also from our knowledge of the refinery process and management in general. It is understood that there could be some errors in it, nevertheless, it is adequate for demonstration and analysis.

Figure 34 Richmond Refinery safety control structure

Each of the components in the safety control structure has their own responsibilities in safety and based on the available information in the accident report these responsibilities are assigned to each group at the company. There is a belief that the assigned responsibilities are reasonable, but in case of error or misunderstanding, it has little impact on the analysis, as those responsibilities should be assigned to someone.

As example, the maintenance department assumed to be responsible for maintaining critical equipment and safety department responsible for performing hazard analyses and risk assessments. When using CAST to analyze an accident, the objective is to determine whether abovementioned responsibilities were carried out blaming and if not, why not and to identify weaknesses in the safety control structure and required improvement to prevent accidents in the future. Responsibilities of different departments/functions within Richmond refinery safety control structure are provided below:

Operator team including field operators, control room operators and lead operators. They monitor the operations and take necessary actions to guaranty that the process runs according to the design and produce the products according to the specifications. They are the owner of processing facilities. They provide operations reports and provide operational feedback to different departments.

Fire Fighting department is the department responsible mainly to respond to emergencies. They maintain firefighting equipment in good conditions. They practice to be able to respond to emergency scenarios as defined in the emergency response plan (ERP). They keep contact with local agencies and work with them closely in term of preparations, planning and emergency drills. They are professional fire fighters and first aiders for the refinery.

Operation Support team are engineers supporting the daily operations in technical terms. They ensure that process plants are operating smoothly. They work closely with operator team, maintenance team and engineering, team. They provide support in management of change, operational decisions, and shutdown planning and engineering projects.

Reliability & Maintenance team are reliability engineers, maintenance engineers and metallurgists. This team is involved in preventative maintenance and in the case of failure repairing. Reliability & Maintenance team analyzes obtained information from equipment to defined actions in order to guaranty the equipment are fit for service. They work closely with engineering and production to assess the risk of equipment with mechanical integrity problems in order to prioritize works and plan accordingly.

Inspectors team is responsible to guaranty the equipment and repair works comply with local regulations, standards and engineering codes. They do inspections and consolidate inspection data. They provide recommendation to different departments like operation and maintenance and reliability team.

Operation management implement operational management systems and ensure that the process plants operate according to the established operational framework. Operation management supervise the operator team, firefighting team and production support team.

Reliability & Maintenance management consists of reliability and maintenance engineers and inspectors. This team implements the reliability related sections of management system with objective of operational excellence and optimizing the plant availability for production.

Refinery management manages the refinery according to the Company plans, standards and applicable rules and regulations. It covers planning of all the projects and activities aligned with the Company strategic plan, vision and values. Liaison with authorities and regulators, communication of accidents or events according to requirements are included in the management scope of work.

Chevron Energy Technology Company (ETC) is the technology center of the Company to develop technical, solutions, products and services in all areas related to the business of the Company. It includes petroleum engineering, reservoir and subsurface, drilling and completion, production and facilities engineering. ETC maintains Company engineering codes and standards according to the updated best practice, industrial codes and standards. It provides technical advices to business units and projects and develops technical instructions and guidelines to improve operational performance and engineering design activities.

Chevron FER BIN is an expert group at corporate level called as Fixed Equipment Reliability Business Improvement Network (FER BIN). This group monitors reliability efforts in refineries of the Company, promotes reliability programs and standardized reliability plants within the Company. The subject matter expert in charge of FER BIN promotes the implementation of best practices or reliability initiatives in refineries. FER BIN works closely and collaborate with ETC.

Chevron Corporation defines vision, values and prepares strategic plans applicable to all business units including exploration & production, transport, refineries, petrochemicals, marketing, fuels and lubricants distributions. Corporate develops management systems and standards to improve operational efficiency in all business units. Zero accident is the target defined by Corporate and policies, processes and tools are provided to achieve it. Corporate carries out governance role by doing audit in all business units.

Code and standards agencies like American Society of Mechanical Engineers (ASME), National Fire Protection Association (NFPA) or American Petroleum Institute (API) are responsible to prepare codes, standards, and recommended practices help companies in having safe operations and also be aligned with technological change required products. Companies during design, engineering and operations use these codes, standards and recommended practices. Companies and manufacturers are members of codes and standards agencies.

Bay Area Air Quality Management District (BAA QMD) is the public agency within counties that surround San Francisco Bay with regulating stationary sources of air pollution.

Contra Costa County (CCC), Richmond City (RC) and Contra Costa Health, Service's Hazard Material Program (CCHMP) is public services to improve viability of local businesses through improvement of prosperity, safety and health local people. Their staff carry out audits in the industry in order to ensure compliance with applicable laws, regulations and standards. They receive industry communication on incidents and inform the situation o local people via established communication channels. They also provide services on emergency preparedness.

Occupational Safety and Health Administration (OSHA)/Cal OSHA enforces safety and health standards. It is in charge to ensure work conditions are safe and healthy. It establishes and standards and also delivers training, and assistance.

Environmental Protection Agency (EPA) has the highest responsibility in regulating, and enforcing environmental laws, environmental licensing, monitoring, analyzing and reporting in order to ensure that environment is protected. However, environment protection is a common responsibility among government, industry and public.

STEP 4: Determine the proximate events leading to the loss

Proximate events are explained in section 5-1 on accident description.

STEP 5: Analyze the loss at the physical system level

Analysis starts with the physical process, identifying the physical failures, dysfunctional interactions and communication, or unhandled external disturbances that contributed to the events. The main objective is to determine why the existing physical controls were not able to control the hazard and ultimately prevent the accident.

Following the CAST methodology, physical system level was reviewed for the followings:

- Safety Requirements and constraints violated
- Emergency and Safety Equipment (Controls)
- Failure and Inadequate Controls
- Physical Contextual Factors

The outcome is summarized in Figure 35 which shows the requirements and controls at physical plant level as well as failures and inadequate controls. The physical contextual factors contributing to the events are included. The analysis of the physical controls does not differ significantly from the one done in most accident analyses. It has been started by looking at the physical plant safety controls at the bottom of the safety control structure and continue upward. Only those controls related to the 4 side-cut release are included. However, it has been tried to include general responsibilities as far as possible based on the available information.

The physical system analysis results in the identification of the following control/feedback inadequacies at this level:

Inadequate control/feedback – 4-sidecut material was not designed to tolerate sulfur content higher than design after hydrogen sulfide removing equipment

The original design of the 4-sidecut circuit has some equipment for removing dissolved hydrogen sulfide. This had been allowed the 4-sidecut to be constructed of carbon steel. Later, in 1991 this 4-sidecut equipment was taken out of service without adequate management of change. Consequently, the effect of the elimination of this hydrogen sulfide removing equipment on 4-sidecut circuit was not analyzed. An adequate MOC would have helped in understanding the increase in sulfur concentration on the carbon steel 4-sidecut piping before removing the equipment.

Inadequate feedback – Means to detect sulfidation corrosion across all unit sections were not available

Between Crude column and crude pumps there are many pieces of piping components like elbows, fittings, and straight pipe with different percentages of silicon concentration. Consequently, sulfidation corrosion rate of these pieces may vary. However, there are only few permanent Condition Monitoring Locations or corrosion probes along the 4 side cut piping on elbow components. Since

elbows have relatively a higher silicon content, corrosion probes did not show a high corrosion rate. Consequently, engineers made their assumptions based on these data that did not show the high corrosion rate of the pieces with lower silicon concentration.

Inadequate control/ feedback – was not designed and constructed for higher corrosion rate due to feed composition change like higher Sulfur content or higher operating temperature

Different sources were used as feed for Richmond refinery while carbon steel was used for 4 side cut circuit. Consequently, when sour crude feed used or higher operating temperature applied carbon steel didn't have the original design life. In case of new crude, management of change applied, however, it mainly assessed the potential general impacts on operation without analyzing corrosion impact from sulfidation corrosion due to higher sulfur content.

Inadequate control – 4 side cut could not be isolated from main crude unit

There was not isolation valve between the 4 side cut and the crude unit. Consequently, this section could be inspected only when the crude unit pumps were shutdown. Within 4 side cut there were relatively low hydrocarbon risk comparing to the hydrocarbon contained in the crude unit and specifically in the column as multiple hydrocarbon components were there.

Inadequate Control / Feedback – Process leak was not detectable by process instruments to trigger the automatic shutdown in the initial rupture

According to the investigation reports after low pressure caused by leak and also after detection of gas and fire there was no automatic activation of shutdown system. In case of pinhole pipe leakage probably process instrument couldn't detect the pressure loss, but when first fire occurred it could be detected. When flash fire happened, an automatic shutdown action could have been started

A summary of the critical control/feedback inadequacies at physical part of the refinery control structure is provided in Figure 35. Addressing these inadequacies could have removed corresponding hazards in the control structure.

Safety Requirements and Constraints violated:

SC1: Hydrocarbons must be under control (contained) at all times. (Excluding properly designed flaring or venting)

SC2: Measures must be taken to minimize exposure of refinery personnel and prevent fire and explosion if inadvertent release occurs.

SC3: Arrangements and measures must be available to protect workers and assets in the plant in case of inadvertent fire and explosion and also to minimize public exposure and losses to the outside community

SR2: Operation and maintenance staff must maintain equipment and piping integrity within target.

SR4: Safety critical equipment and refinery emergency procedure must be provided to prevent fire and explosion and reduce exposure in the event of an inadvertent hydrocarbon release

SR5: Emergency procedures and equipment must be available and operable to minimize the impact of fire and explosion. Also all areas of the plant must be accessible to emergency personnel and equipment during emergencies.

SR6: Refinery personnel must train to: a) perform their job safely and understand proper use of safety equipment b) understand their roles and responsibilities regarding safety and the hazard relate to their job c) respond appropriately in an emergency

Emergency and Safety Equipment (Controls):

Pressure alarm

Liquid containment system

Block valves, bypass valve

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:

4-sidecut material was not designed to tolerate sulfur content higher than what remained in the 4-sidecut stream after hydrogen sulfide-removing equipment

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

Not designed for conditions that cause higher corrosion rate like change in feed composition (higher Sulfur content) and/or higher operating temperature

4 side cut cannot be isolated from main 4CU

Process instruments were not able to detect process leakage and commence automatic shutdown during initial rupture

Physical contextual factors:

Prior to the mid-1980s multiple carbon steel specifications were commonly and independently in use for refinery piping which resulted in piping being manufactured with different silicon content.

A lot of piping components, 4600+ components, in the refinery were subject to corrosion and monitoring

Small leak was undetectable from process parameter monitoring

Unable to see piping condition due to presence of insulation and location of leak point.

Figure 35 summary of loss analysis at the physical system level

STEP 6: Moving up the levels of the safety control structure, determine how and why each successive higher level allowed or contributed to the inadequate control at the current level
After analyzing the loss at the physical system level and identification of physical control failures/inadequacies, next step is to move to higher levels of the hierarchical safety control structure of refinery in order to understand why those physical control failures/inadequacies occurred. By performing the analysis at higher levels we will be able to understand the reasons behind failures and inadequacies at physical system level and why each component at the lower levels acted in the way they did.

The analysis goes through all the levels as demonstrated in Figure 34 and starts with the refinery system operation level.

Based on the CAST methodology each controller was reviewed for the followings:

- Safety-Related Responsibility
- Unsafe Decisions and Control Action
- Process Model Flaw
- Context

The analysis of some of these controllers is provided below:

Operator team:

According to refinery safety control structure as depicted in Figure 34, the operator team controls the refining process by automation control system and also taking actions in the field. The team does it by receiving signals from the process and sending commands through the control system. In case of an emergency, operators coordinate the emergency response with the firefighting team and keep continuous communication with them.

Operators' safety related responsibilities, unsafe decisions and control actions, process model flaws and operational context are provided in Figure 36. Within control structure, role of this team is very important as they are considered as the area owner of the crude unit. Their safety related responsibilities during an emergency include unsafe operating conditions detection and providing appropriate reaction like shut down to prevent major consequences.

Safety related responsibilities:

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

Unsafe decisions and control actions:

Agreed to investigate the leak source on a non-isolated 4-sidecut pipe without unit shutdown
Ordered the firefighters to remove the insulation with high pressure water jet
Delayed in unit emergency shutdown after the initial flash fire
Delayed in moving the refinery personnel (especially non-essential personnel) away from the 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.
Believed that the corrosion is local and not a thinning process, hence didn't consider the pipe rupture as a valid scenario

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 they were 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
Presence of hot surface around distillation column
Distillation column contains multiple components with different physical properties

Figure 36 Operator team level analysis

Operators did several unsafe control actions as provided in details in Figure 36. In order to identify inadequacies in the control/feedback at the operator team level these unsafe actions are analyzed. Control/feedback inadequacies are provided below:

Inadequate Control – Operator team agreed to look for leak source on a 4 side cut pipe without unit being shutdown

When the leak was detected, operators and people from other disciplines on the scene came into a conclusion that the leak was not enough important that required a shutdown. However, they considered it as a serious situation. At the end, they decided to take out the insulation in order to determine the cause of the leak. In Chevron they called it as 'daylighting the leak'. Then, they could decide to either repair the leak or to shut down the unit.

Inadequate Control – Delayed in unit emergency shutdown after the initial flash fire

After the first 2.5 hours of the leak discovery and even after the initial flash fire operators didn't shutdown the unit. Since control room operator had to wait for shutdown order or approval from head operator at the scene and the refinery shift leader it took a delay of 7 minutes from the initial flash fire to initiate the shutdown system manually.

Inadequate Feedback - Delayed in removing nonessential personnel away from the scene

Like other people onsite operators didn't consider the possibility of pipe rupture and let 19 refinery personnel including nonessential personnel in the proximity of the leak location.

Firefighting team:

According to the refinery control structure depicted in Figure 34, firefighting team gave command and provided control on the leak by doing intervention and communications. This team observed the crude unit and visually and received communications from control room.

A summary of safety related responsibilities, unsafe decisions and control actions, process model flaws and operational context of firefighting team is provided in Figure 37. The firefighting team directly was involved with the leak. This made them as the closest team to the scene during the emergency situation. Their main responsibility was to bring back the condition to a safe and normal conditions.

Safety related responsibilities:

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 firefighting 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

Unsafe decisions and control actions:

Did not safely remove the insulation which facilitated the pipe rupture
Did not anticipate the risk of a gas leak and ignition or inadequate communication with the previous shift
Did not define the 'Hot Zone' large enough to prevent putting personnel and equipment at fire risk

Process model flaw:

Knowledge about Auto Ignition Temperature / Flash point
Distillation and piping hydrocarbon content mixture led to wrong risk assessment contained gas and more volatile hydrocarbon

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

Figure 37 Firefighting team level analysis

Firefighters did some unsafe control actions as provided in details in Figure 37. In order to identify inadequacies in the control/feedback related to firefighters these unsafe actions are analyzed. Control/feedback inadequacies are provided below:

Inadequate control/feedback – Unsafe removal of the insulation which helped the pipe rupture

Some unsafe actions like pipe pike, hook and high pressure water jet were taken by firefighters which put unnecessary forces on leaking pipe.

Inadequate control/feedback - Inadequate communication with the previous shift and not anticipating the risk of a gas leak and ignition

Potential flash fire due to exposing oily insulation into air were known for firefighters. However, CSB investigation reports showed that some firefighters didn't understand fully the risk of dealing with product within 4 side cut. Most of the firefighters of the next shift were not involved in the risk assessment and planning. Consequently, there might be different understanding of the situation between shifts.

Inadequate control/feedback - 'Hot Zone' was not established large enough to prevent exposing personnel to the risk of fire

Firefighters defined an area of 20 foot by 20 foot around the leak location and taped it off as 'hot zone'. According to Chevron definition it is 'the immediate release area of the incident where there is risk of exposure or injuries due to flame contact, radiant heat, or hazardous materials'. A 'cold zone' outside of the hot zone also was defined. Key operational personnel, firefighting support team and Incident Commander were located in the 'cold zone' to provide support. The fire truck that was burned completely during the fire was also located in the 'cold zone'. If the potentiality of pipe rupture had been taken in account, a larger area might be established as 'hot zone'.

Operation support team:

According to the safety control structure depicted in Figure 34, operation support team delivered engineering services, conducted Process Hazard Analysis and Management of Change managing. The operation support team received information from operation and maintenance teams and monitored automation control system. This team also worked with reliability team.

Figure 38 summarizes the operation support team safety related responsibilities, unsafe decisions and control actions, process model flaws and operational context.

Safety related responsibilities:

Provide engineering support in safety analysis during design and operation
Follow operational excellence and principle
Follow emergency response procedure
Plan turnaround work list subject to improvement of equipment reliability
Ensure each change to process equipment and piping is reviewed comprehensively and execute correctly

Unsafe decisions and control actions:

Did not provide sufficient input during leak investigation planning
Did not provide sufficient hazard reviews and management of change associated with new operating condition and feed introduction
Contributed to the 4-sidecut pipe replacement work scope reduction during 2006 turnaround planning process
Rejected chrome pipe replacement plan on 4-sidecut during 2011 turnaround planning process

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

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

Figure 38 Operation support team level analysis

Operation support team did some unsafe control actions as provided in details in Figure 38. In order to identify inadequacies in the control/feedback at the operation support team level these unsafe actions are analyzed. Control/feedback inadequacies are provided below:

In adequate control - Did not provide sufficient input while analyzing the leak

Operation support team knew the process and understood the Company safety management system and its requirements. Nevertheless, whether they were involved in the risk assessment of finding the leak was not mentioned. Consequently, 19 plant personnel were exposed to the risk and clamp repairing was considered as a solution for such a corroded pipe.

Inadequate control/ feedback – Was not involved sufficiently in hazard analysis related to management of change associated with new operating condition and feed introduction

According to CSB investigation reports, the management of change of the feed took into account only generic operational issues without analyzing the corrosion impact due to higher sulfur content in the changed crude. Operation support team was not involved in this MOC and consequently, they didn't update process condition like temperature and sulfur concentration to the inspection and reliability team in order to modify their corrosion rate.

Inadequate control - 4 side cut pipe replacement work scope reduced in 2006 turnaround planning process

During 2006 turnaround planning, operation support team was not supportive to replace 4 side cut completely as reliability engineer suggested due to the limited available corrosion data points.

Inadequate control – The proposal to replace chrome pipe on 4 side cut in 2011 turnaround planning process was rejected

According to the CSB investigation report turnaround core team rejected the 4 side cut pipe replacement proposal in 2011 turnaround. Insufficient data to verify the severity of corrosion status was the reason behind. Turnaround core team was composed of operation support team, inspectors and reliability engineers.

Reliability and maintenance team

Based on the CBS accident reports (interim, regulatory, and final) it is understood that reliability and maintenance engineers owned the management of change scope for 4 side cut piping replacement and also material engineer was part of this team.

According to the safety control structure depicted in Figure 34, the reliability and maintenance team managed the integrity of the refinery equipment by preventive and corrective maintenance programs. They also replaced provided input to other teams during process hazard analysis and management of change process. Operator team and inspector provided information to the reliability and maintenance team. This team also works closely with operation support team and engineering on the reliability of equipment. This is done through Risk Base Inspection program. They are also involved in providing information regarding repairs and recommendations to operations in order to help in making a correct decision during emergency situations.

A summary of the reliability and maintenance team's safety related responsibilities, unsafe decisions and control actions, process model flaws and operational context is provided in Figure 39.

Safety related responsibilities:

Follow operational excellence and principle
Follow emergency response procedures
Provide reliability input to PHA, MOC work processes
Take appropriate action to improve equipment and piping reliability
Be competent and aware of current ongoing industrial issue relate to their working area e.g. sulfidation corrosion.

Unsafe decisions and control actions:

Revised scope of 4-sidecut pipe replacement instead of going for an 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-sidecut (2009)
Did not take into account valuable data obtained during 2011 turnaround about actual progress of sulfidation corrosion in 4-sidecut section

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 emphasizes on higher operating pressure service rather drive for inherent design approach

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.
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 (RBI, ROI/IPR, Inspection guideline, 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.
The team is subject to reliability, capital budgets and other goals imposed on them
Turnaround is very schedule driven and time constraining in nature
Complex data tracking system

Figure 39 Reliability and Maintenance Support team level analysis

As listed in Figure 39, the reliability and maintenance team took several unsafe control actions. Analysis of these actions identifies the following control/feedback inadequacies at the reliability and maintenance team level:

Reliability and maintenance team took some unsafe control actions as provided in details in Figure 39. In order to identify inadequacies in the control/feedback at the reliability and maintenance team level these unsafe actions are analyzed. Control/feedback inadequacies are provided below:

Inadequate control - Instead of adopting an inherently safe approach the scope of 4 side cut pipe replacement was changed

The reliability and maintenance engineer was not informed about the reduction of previous inspection data. Apparently, when there was an objection on the full replacement of 4 side cut, reliability and maintenance engineer revised the scope to partially upgrade the 4 side cut. Since the entire 4 side cut circuit has the same operating conditions reliability and maintenance team could have justified total replacement and convinced reviewers to approve it.

Inadequate control – Higher level management was not communicated properly by this team to support corrosion issue

On three different occasions 4 side cut replacement were proposed to be included in the turnaround plan, but all here were rejected. This has been identified while reviewing investigation reports. Apparently, the reliability and maintenance team did not transmit this point adequately to higher levels in the organization. They might not see it as an important problem since the corrosion data was predicting a longer life for the circuit and they could waited for the next time.

Inadequate control/ feedback - During 2007 turnaround 100% inspection using continuous monitoring technology was not followed

Based on existing corrosion data, replacement proposals were rejected by the turnaround core team. However, the existing corrosion data was limited and was not demonstrating the corrosion risk accurately.

Inadequate control -Valuable data obtained during 2011 turnaround on the actual progress of sulfidation corrosion in 4 side cut section was not taken into account

One part of the 12” 4 side cut circuit was identified not acceptable during the 2011 turnaround because of the low thickness and was replaced. The age, material of construction, and contained materials of the 8” side cut were same as 12” side cut. However, since the team understanding was based on existing inspection and reliability data, they didn’t consider that this situation could be occurring in the 8” section as well.

Inspectors

According to the safety control structure depicted in Figure 34, the inspectors perform inspections, collect and analyze corrosion data, and provide recommendations to other teams to execute their role in controlling the integrity of refinery equipment. They communicate with maintenance team, operation team, reliability team and ETC team. They collect data from corrosion monitoring system and feed them to the meridian database system.

A summary of safety related responsibilities, unsafe decisions and control actions, process model flaws and operational context related to inspectors is provided in Figure 40.

Safety related responsibilities:

Follow operational excellence and principle

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, ASME, National Boiler Inspection Code) to perform inspection and develop appropriate inspection plan for their units

Unsafe decisions and control actions:

Did not correctly enter inspection (Radiographic testing) data into condition manager section of the software (2002)

Did not install 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 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 did not enter these measurement data into condition manager database (2012)

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.

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 imposed goals

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 4-sidecut piping

Silicon concentration is higher in fitting component than straight piping

Require destructive testing to measure silicon concentration for detecting risk of sulfidation

Figure 40 Inspector level analysis

Inspectors did several unsafe control actions as provided in details in Figure 40. In order to identify inadequacies in the control/feedback at the inspectors team level these unsafe actions are analyzed. Control/feedback inadequacies are provided below:

Inadequate control – Corrosion monitoring probes were not installed at the right locations

Inspectors of crude unit didn't know that the current locations considered for monitoring did not reflect the severity of the sulfidation corrosion. Monitoring probes mainly were located on the fittings and elbows of the 4 side cut circuit. Despite the fact that these fittings and elbows were generally more susceptible to corrosion, the risk of sulfidation corrosion existed in straight pipe components high due to low silicon content in the carbon steel.

Inadequate control – Adequate number of continuous monitoring instruments were not installed to cover 100% inspection plan of 2007: Corrosion Mitigations Plan

According to the CSB investigation reports, only 16 continuous monitoring sensors were installed on 67 components of the 4 side cut. The reason is not mentioned in the investigation report, however, it could have been because of financial issues or the credit given to the continuous readings.

Inadequate control – Despite 2011 ETC guideline, 100% inspection were not implemented

In 2011 turnaround, inspection of 4 side cut circuit was included however, it didn't follow the ETC guide on doing 100% component inspection. Consequently, inspection team installed some additional monitoring probes but still far from being 100%. It caused an understanding of sulfidation corrosion status that was wrong.

Inadequate control / feedback - Measurements on out of tolerance were not repeated

Based on the investigation reports, according to the Refinery inspection guideline any reading resulted in out of tolerance had to be repeated. However, it didn't happen. In addition to this, the data was not registered in the database and consequently, flaws in the data were not detected.

Operation management

According to the safety control structure depicted in Figure 34, the operation management implemented managed the refinery via implementation of corporate processes, operational management systems and tools. This included supervising all the teams within the refinery and communicating with internal and external stakeholders.

A summary of safety related responsibilities, unsafe decisions and control actions, process model flaws and operational context related to the operation management is provided in Figure 41.

Safety related responsibilities:

Follow operational excellence and principle
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
Ensure personnel are competent and trained for their roles
Ensure that equipment and piping are maintained properly and accurate records are maintained

Unsafe decisions and control actions:

Did not enforced safety culture to operation working teams adequately
Were not able to detect socio and regulatory pressure impact related to flaring

Process model flaw:

Emphasize on compliance to demonstrate good operational discipline
Inadequate communication and means to detect problem at execution level
Prioritize high priority on data driven over industrial lessons learned and recommendation from experts in decision making

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

Figure 41 Operation management level analysis

Operation management did several unsafe control actions as provided in details in Figure 41. In order to identify inadequacies in the control/feedback at the operation management level these unsafe actions are analyzed. Control/feedback inadequacies are provided below:

Inadequate control - Safety culture was not enforced in operation working teams adequately

Many accidents happened before because of sulfidation and lessons learned were available. Additionally, related training was provided to refinery staff. However, apparently operation team not given enough credit to this important safety related topic and priority had been given to other issues than piping integrity.

Inadequate feedback – Social and regulatory impact on flaring was not detected

Operation management missed to detect or foresee the impact other division such as commercial or community could have had on the decision of workers when it comes flaring and its impact on community, social and regulatory bodies.

Reliability and maintenance management

According to the safety control structure depicted in Figure 34, the reliability and maintenance management implements the reliability related sections of management system with objective of operational excellence and optimizing the plant availability for production. This team consists of reliability and maintenance engineers and inspectors. Reliability and maintenance management sets and monitors performance indicators of reliability and maintenance team and inspectors.

A summary of safety related responsibilities, unsafe decisions and control actions, process model flaws and operational context related to reliability and maintenance management is provided in Figure 42.

Safety related responsibilities:

- Follow operational excellence and principle
- Follow emergency response procedures
- Drive ETC recommendations to improve safety/reliability performances
- Ensure compliance to company code/standard requirements
- Maintain refinery equipment and piping in order to ensure they meet integrity requirements
- Ensure effectiveness of cooperate safety related work process utilization

Unsafe decisions and control actions:

- 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
- Inadequate communication and means to detect issues at execution level

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

Figure 42 Reliability and maintenance level analysis

Reliability and maintenance management did several unsafe control actions as provided in details in Figure 42. In order to identify inadequacies in the control/feedback at the operator team level these unsafe actions are analyzed. Control/feedback inadequacies are provided below:

Inadequate feedback - Action on the sulfidation corrosion issues were not taken at executional level

Apparently reliability and maintenance management didn't take enough actions on the issues reported by reliability and maintenance engineers. According to the investigation reports reliability and maintenance management didn't support the recommendations of inspectors or the reliability team to replace the 4 side cut piping despite the fact that reliability and maintenance management had been received communication from ETC about the realization of 100% inspection on high priority piping.

Inadequate control - Use of available resources had not been fully optimized

According to the investigation reports, reliability and maintenance team and inspectors were used many unnecessary tools and processes while no attempt was done by the reliability and maintenance team to consolidate the obtained data and find synergy between these tools and processes. This provided limited information to each small group within the team without having the full picture to find the best and optimized solution.

Refinery management

According to the safety control structure depicted in Figure 34, the refinery manager manages the refinery according to the Company plans, standards and applicable rules and regulations. Refinery management plans all the projects and activities aligned with the Company strategic plan, vision and values. Liaison with authorities and regulators, communication of accidents or events according to requirements are included in the management scope of work. Finally, the ultimate responsible person at refinery level is the refinery manager and acts as the focal point for external stakeholders.

A summary of the refinery management's safety related responsibilities, unsafe decisions and control actions, process model flaws and operational context is provided in Figure 43.

Safety related responsibilities:

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 health safety and environmental 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

Unsafe decisions and control actions:

Did not provided sufficient review/ enforcement of Corporate auditing recommendation

Did not provided sufficient monitoring of effectiveness and quality of work process implementation

Did not provide sufficient emergency guidelines for operation personnel to make decision and failure to detect the dynamic changes, which shifted the operators' safety priority

Failed 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:

Not aware of safety state of the refinery

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

Figure 43 Refinery management level analysis

Refinery management did some unsafe control actions as provided in details in Figure 43. In order to identify inadequacies in the control/feedback at the refinery management level these unsafe actions are analyzed. Control/feedback inadequacies are provided below:

Inadequate Control/Feedback - Corporate audit recommendations were not reviewed or enforced sufficiently

According to the investigation reports it was not obvious how refinery manager enforced the corporate audit recommendations about the sulfidation corrosion within the refinery and how reviewed the outcome with management of maintenance and operation.

Inadequate Feedback/Control - Emergency guidelines were not provided sufficiently for operation personnel to make right decision

Refinery staff while making decision take into account the impact on production, cost and environmental. It is the responsibility of refinery management to prepare adequate guides and instructions to help staff in making decisions. In this specific case, after leak discovery, operation needed to make a decision on shut down taking into account the impact on production and also possible environmental issues because of flaring.

Inadequate Feedback/Control – Different safety studies and reviews executed to improve the risk understanding by different functions were not integrated and optimized

Various process hazard analysis studies, risk based inspections executed with the participation of staff from refinery or ETC. in some cases these works were repeated by different function without been understood with others. If there was an initiative in place to combine these activities or to establish a process involving different functions, they could have a better and common understanding on the risk.

Inadequate Control/detection – There was a lack of adequate emphasis integrity management of equipment

According to CSB investigation reports, there were more than 100 clamps used in the refinery while many of these clamp were not replace even during turnaround which shows a significant issue on the integrity management within refinery.

Inadequate Control - Release of toxic material to the air was not reported immediately

Contra Costa County didn't receive alert from refinery management immediately when the leak started. It took 10 minutes to alert that caused exposure of people to the toxic materials, particles and smoke and resulted in subsequent hospitalization of many people.

Energy Technology Company (ETC)

According to the safety control structure depicted in Figure 34, ETC is the technology center of the Company to develop technical, solutions, products and services in all areas related to the business of the Company. It includes petroleum engineering, reservoir and subsurface, drilling and completion, production and facilities engineering. ETC maintains Company engineering codes and standards according to the updated best practice, industrial codes and standards. It provides technical advices to business units and projects and develops technical instructions and guidelines to improve operational performance and engineering design activities.

A summary of the ETC related responsibilities, unsafe decisions and control actions, process model flaws and context is provided in Figure 44.

Safety related responsibilities:

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

Unsafe decisions and control actions:

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:

ETC had no direct control on monitoring the implementation level of the issued guidelines in the business units

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.

Figure 44 Energy Technology Company (ETC) level analysis

ETC did some unsafe control actions as provided in details in Figure 44. In order to identify inadequacies in the control/feedback at the ETC level these unsafe actions are analyzed. Control/feedback inadequacies are provided below:

Inadequate Control – A clear instruction on the implementation of new guideline was not given

Whether if it was the responsibility of ETC to track and monitor the implementation of its guideline in business units it was not clear in the investigation reports. There was an interpretation that ETC only give technical instruction without having the mechanism to follow up on the implementation of technical advices.

Inadequate Control / Feedback – Missed to issue an official instruction to evaluate the adequacy of isolation valves on old distillation units

Like the carbon steel piping and changes in the new standards, isolation of 4 side cut was not in compliance with the current standard. According to the investigation reports it was not clear the approach of the company and specifically ETC in areas that existing design does not comply with the current industrial standards.

Inadequate Control - Lessons learned from accidents were not captured systematically in process hazard analysis checklist and guidewords

According to CSB investigation reports, apparently sulfidation corrosion was not included in the process hazard analysis. If sulfidation corrosion was integrated by ETC in the process hazard analysis checklist, it could have been highlighted in the process hazard analysis and documented.

Corporate Management

According to the safety control structure depicted in Figure 34, the Corporate management defines vision, values and prepares strategic plans applicable to all business units including exploration & production, transport, refineries, petrochemicals, marketing, fuels and lubricants distributions. Corporate develops management systems and standards to improve operational efficiency in all business units. Zero accident is the target defined by Corporate and policies, processes and tools are provided to achieve it. Corporate carries out governance role by doing audit in all business units. Corporate management also communicate with authorities like EPA, OSHA and agencies in charge of codes and standards.

A summary of the Corporate management related responsibilities, unsafe decisions and control actions, process model flaws and context is provided in Figure 45.

Safety related responsibilities:

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

Unsafe decisions and control actions:

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 not 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 and other initiatives in place were sufficient to prevent process incidents

Context:

Greater challenge to explore and produce crude oil and natural gas in lead to a greater demand to run business flexibly.

Global warming, greenhouse 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

Figure 45 Corporate management level analysis

Corporate management did several unsafe control actions as provided in details in Figure 45. In order to identify inadequacies in the control/feedback at the corporate management level these unsafe actions are analyzed. Control/feedback inadequacies are provided below:

Inadequate control and feedback - Adequate follow up on the findings from the audit was not provided

According to the CSB investigation reports, there was an audit by corporate in Richmond refinery during 2012 addressing corrosion management issue. While, this issue was raised back in 2002. No evidence found on corporate follow up on the findings.

Inadequate control and feedback - ETC recommendation and safety related work processes were not enforced adequately by corporate

After ETC issued sulfidation corrosion recommendations, corporate didn't enforce it in all business units. In the audits done by corporate deficiencies in process hazard analysis or management of change were not found.

Inadequate feedback - Human factor issue that resulted in safety deficiencies was not supervised adequately at corporate level

Safety culture alteration and subsequent impact on staff behavior was not detected and supervised adequately by corporate management.

Codes and standard agencies

According to the safety control structure depicted in Figure 34, the code and standard agencies like American Society of Mechanical Engineers (ASME), National Fire Protection Association (NFPA) or American Petroleum Institute (API) are responsible to prepare codes, standards, and recommended practices help companies in having safe operations and also be aligned with technological change required products. Companies during design, engineering and operations use these codes, standards and recommended practices. Companies and manufacturers are members of codes and standards agencies.

A summary of the code and standard agencies related responsibilities, unsafe decisions and control actions, process model flaws and context is provided in Figure 46.

Safety related responsibilities:

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.

Unsafe decisions and control actions:

Did not mandate minimum specification for silicon content (pre 1985)
Provided voluntary and permissive language in code and standards
API did not provide consistent information in published documents

Process model flaw:

None

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

Figure 46 Codes and standard agencies level analysis

Code and standard agencies did some unsafe control actions as provided in details in Figure 46. In order to identify inadequacies in the control/feedback at the code and standard agencies level these unsafe actions are analyzed. Control/feedback inadequacies are provided below:

Inadequate control/feedback - Did not mandate minimum specification for silicon content (pre 1985)
ASTM A53B regulations issued in 1985 didn't require the minimum silicon content at 0.1% weight. It resulted in steel pipes that were susceptible to high sulfidation corrosion rate. The failed 4 side cut carbon steel pipe was fabricated according to ASTM A53B.

Inadequate control - Standard or recommended practices have a voluntary and permissive language
According to CSB reports, some guidelines like API RP 939-C use permissive and voluntary language. Consequently, companies didn't consider these guidelines as obligatory.

Bay Area Air Quality Management District (BAAQMD)

According to the safety control structure depicted in Figure 34, the BAAQMD is the public agency within counties that surround San Francisco Bay with regulating stationary sources of air pollution. This agency interacts with the EPA and used its resources reduce air pollution in the Bay Area.

A summary of the BAAQMD related responsibilities, unsafe decisions and control actions, process model flaws and context is provided in Figure 47.

Safety related responsibilities:

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

Unsafe decisions and control actions:

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

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

Figure 47 Bay Area Air Quality Management District (BAAQMD) level analysis

The BAAQMD did some unsafe control actions as provided in details in Figure 47. In order to identify inadequacies in the control/feedback at the BAAQMD level these unsafe actions are analyzed. Control/feedback inadequacies are provided below:

Ineffective control – There were inadvertent side effects on operator decisions caused by stringent flaring allowance guidelines

In the area under responsibility of BAAQMD there are numerous companies and facilities sending pollutions to the air, consequently, BAAQMD allows a very limited allowance for flaring in order to guaranty the air quality. Although, flaring is a critical element within safety of a facility like Chevron refinery, the limitation established by BAAQMD is an important items to be considered by operation team during emergency scenarios before pushing the emergency shutdown button.

Richmond City and Contra Costa Health Service's Hazard Material Program (CCHMP)

According to the safety control structure depicted in Figure 34, the Richmond City and Contra Costa Health Service's Hazard Material Program (CCHMP) is a public services to improve viability of local businesses through improvement of prosperity, safety and health local people. Their staff carry out audits in the industry in order to ensure compliance with applicable laws, regulations and standards. They receive industry communication on incidents and inform the situation o local people via established communication channels. They also provide services on emergency preparedness.

The Richmond City and Contra Costa Health Service's Hazard Material Program (CCHMP) maintain the interactions with different parts including Richmond refinery, EPA, Richmond City and Contra Costa, and Cal/OSHA.

A summary of the Richmond City and Contra Costa Health Service's Hazard Material Program (CCHMP) related responsibilities, unsafe decisions and control actions, process model flaws and context is provided in Figure 48.

Safety related responsibilities:

Improve industrial safety by conducting review, inspection, audit

Report audit results to EPA and OSHA

Implementing additional requirements of risk and process safety management at county and city level.

Unsafe decisions and control actions:

Utilized inadequate regulatory checklists in facility audit.

Did not provide quality resource to enforce appropriate safety control action

Process model flaw:

Audit based on current regulatory without comparing with industrial best practices

Believed that the warning system was effective

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

Figure 48 Richmond City and Contra Costa Health Service's Hazard Material Program (CCHMP) level analysis

CCHMP did some unsafe control actions as provided in details in Figure 48. In order to identify inadequacies in the control/feedback at the CCHMP level these unsafe actions are analyzed. Control/feedback inadequacies are provided below:

Inadequate control/ feedback - In facility audits inadequate regulatory checklists were used

There are many regulation that have not been updated since 2000 on regular basis. Despite this fact, CCHMP staff used existing regulations in their checklist for audits which resulted in insufficient risk identifications by them.

Inadequate control/ feedback – Qualified staff to enforce safety control action appropriately was not provided

Words like 'ensure' and 'consider' were used frequently by CCHMP staff in their audit. Consequently, they didn't force Richmond refinery to improve safety by encouraging them in following an inherently safer approach.

Cal/OSHA

According to the safety control structure depicted in Figure 34, the Cal/OSHA enforces safety and health standards. It is in charge to ensure work conditions are safe and healthy. It establishes standards and also delivers training, and assistance.

A summary of the Cal/OSHA related responsibilities, unsafe decisions and control actions, process model flaws and context is provided Figure 49.

Safety related responsibilities:

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.

Unsafe decisions and control actions:

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 lessons learned from incidents and audit findings

Did not provide adequate review of recommended best practices

Process model flaw:

Believe 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

Believe that all facilities are only required to demonstrate their performance within the set requirement instead of reducing risk down to reasonably practical level.

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 which intensifies OSHA's workload

Regulatory regime in USA does not focus on management of change, which is usually one of the accidents causal.

Figure 49 Cal/OSHA level analysis

Cal/OSHA did several unsafe control actions as provided in details in Figure 49. In order to identify inadequacies in the control/feedback at the Cal/OSHA level these unsafe actions are analyzed. Control/feedback inadequacies are provided below:

Inadequate control/feedback – Didn't review company's process safety analysis adequately to identify quality of hazard analysis works

Process hazard analysis is one of the elements of the OSHA PSM and it has to be reviewed every 5 years. Cal/OSHA is responsible to enforce OSHA PSM, however, Cal/OSHA didn't review company's process hazard analysis within its normal and routine oversight of process safety management.

Inadequate control / feedback - Lessons learned from incidents or audit findings were not considered systematically to improve regulation requirements

Normally, it takes a long time for OSHA to revise its CFR and related regulatory requirement. This results in having regulations and requirements not up to dated that are used by auditors and local inspectors.

Inadequate control- Recommended best practices were not reviewed adequately

There are many recommended best practices in the industry, however, regulatory agencies like OSHA didn't include these best practices in their regulations. Additionally, OSHA didn't review recommended practices like API RP 939-C to ascertain if its provisions are enough to minimize the risks related to sulfidation corrosion.

EPA

According to the safety control structure depicted in Figure 34, the EPA has the highest responsibility in regulating, and enforcing environmental laws, environmental licensing, monitoring, analyzing and reporting in order to ensure that environment is protected. However, environment protection is a common responsibility among government, industry and public.

A summary of the EPA related responsibilities, unsafe decisions and control actions, process model flaws and context is provided in Figure 50.

Safety related responsibilities:

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 on the release of toxic material into the air from operating chemical facilities and others

Cite facilities for failure to comply with Recognized and Generally Accepted Good Engineering Practice (RAGAGEP) or CFRs.

Unsafe decisions and control actions:

Did not implement CSB recommendations and learning from past industrial incidents

Did not conduct sufficient on-site inspection or audit

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

Process model flaw:

Believe that activity base model is sufficient to manage risk for refinery and chemical industry

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.

Context:

Lengthy rule making process due to various impact assessments leading to static regulations for decades

Industry standards, technologies and practice continue to change and advance

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

Figure 50 EPA level analysis

EPA did several unsafe control actions as provided in details in Figure 50. In order to identify inadequacies in the control/feedback at the EPA level these unsafe actions are analyzed. Control/feedback inadequacies are provided below:

Inadequate control – CBS recommendations and learning on industrial incidents were not implement

Despite CSB had sent some improvement points to points to EPA for inclusion in the PSM and RMP regulations, these regulations were not updated.

Inadequate control/ feedback – Limited site inspection or audit conducted

According to the Office of Inspector General, in 2009, 65% of active RMP facilities didn't receive a site inspection or audit which means that EPA didn't receive enough feedback on how RMP was implemented in the facilities.

Inadequate control – ALARP concept is not included in RMP requirement and its oversight by EPA

RMP has to be developed and submitted by each facility to EPA. A high level hazard analysis report has to be included in the RMP. However, it doesn't require a detailed process hazard analysis report that provides information on the controls and mitigation measures in place. Consequently, there is no obligation for facilities to demonstrate how the risk is minimized and verify sufficient safety controls and mitigation measures are in place. On top of this, EPA does not have enough qualified staff to carry out audits and assess if the facility risks are reduced to As Low As Reasonably Practical (ALARP) level.

STEP 7: Review contributions of coordination or communication failures

In previous step of the CAST analysis, each component was analyzed separately. In this step the overall coordination and communications among different controllers of the system are examined to identify areas where coordination and communication between controllers resulted in the hazardous situation or contributed to the 4 crude unit fire accident. This analysis demonstrated that in different occasion interaction between different controllers were missing sufficient coordination and communication. It has been already discussed in Step 6 at component level and here it will be discussed at system level.

Inadequate coordination and communication in taking decisions and actions when the leak was discovered: According to the CSB reports, emergency response team including supervisors, operators, firefighting personnel and engineers didn't react to the emergency in well-organized way. Different people involved in the emergency did activities without being coordinated with the rest. There was no coordination meeting to let all people work under a unified and well communicated structure. Consequently, they didn't assess the risk correctly and missed to consider pipe rupture as a valid scenario.

Conflicted communication and delay in activation of emergency shutdown: There were controls in place to ensure safety of operation while attending emergency situations. Similarly, for normal shutdown of the crude unit. Despite flaring is considered as a safe way to release combustible material quickly from the process during emergency situation, because of its environmental impacts BAAQMD established some limitations on emissions and required communications regarding pollution emission. These limitations potentially impacted on operator decision regarding shut down and its subsequent flaring.

Conflicted coordination or inadequate communication between different teams resulted in not replacing 4 side cut prior to its failure: The only opportunity to replace pipes or install corrosion monitoring probes is during turnaround that happened normally every 4 to 5 years. This is the available time frame for reliability engineers and inspectors. Consequently, turnaround has to be planned very carefully and it is the responsibility of the turnaround team to determine the priority of work included in the turnaround list. Reliability engineer and inspector on different occasions proposed 4 side cut replacement to be included in the turnaround worklist, however, it was not approved by the turnaround team. Reliability engineer and inspector didn't work together to convince the turnaround to approve the 4 side cut replacement.

Inadequate coordination between ETC and maintenance management to manage the replacement of 4 side cut: Taking into account accidents occurred due to sulfidation in the industry and the fire occurred in Richmond refinery in 2007, ETC prepared different guidelines to mitigate sulfidation corrosion. These guidelines was sent to reliability and maintenance management and also inspectors for action and implementation. However, ETC had no direct influence on business units. Consequently, implementation of ETC guideline was depended to the local maintenance team.

Inadequate coordination and communication on managing gaps in the facilities due to change in the industrial codes and standards: normally agencies responsible for preparation of codes and standards update the standards, guidelines and recommended practices on regular basis in order to capture new technology, lessons learned from accidents and changes that happened and impact the publication. Updates are mainly simple to be applied in new projects in design or construction, but in case of existing facility there will be gap between their design and the updated version. According to the investigation reports, the way these gaps are handles and coordinated is not clear.

Inadequate coordination and communication on the process of keeping updated facilities manager about the compliance with changes in the codes and standards: Agencies like ANSI, NFPA, ASME, API and CCPS publish new codes, standards or recommended practice timely or update existing ones modifying their requirements. In many cases for a facility it is not easy to be aware of these changes and continuously verify compliance with these codes, standards and recommended practices. OSHA as regulatory body does not consolidate applicable ones to each facility for different steps of life cycle. This could potentially cause less effectiveness in managing risk.

Lack of coordination and inadequate communication among reliability team, maintenance team and inspections department to assess the integrity of 4 side cut: For a period of time from 2002 up to the time of accident, many inspections, reviews and corrosion studies took place in the refinery on the 4 side cut. Nevertheless, inspectors, reliability engineers and maintenance engineers didn't consolidate all the available information between them to assess the status and there was no focal point in charge of the issue coordinating between all and keep a constant communication to resolve the issue.

After a careful analysis many issues had been identified regarding coordination and communication between different controllers that move the operation toward greater risk and finally caused the accident. A part of the items discussed before, failure to communicate the process condition like temperature, pressure and characteristics of product to emergency team, inadequate communication of sulfidation corrosion issue to the refinery management, unclear communication between ETC and decision makers, improper internal communication in API and subsequent inconsistency of information within API publications and finally inadequate coordination between EPA and OSHA on process safety conditions and in some cases redundancy of requirements can also be mentioned.

STEP 8: Determine the dynamics and changes in the system and the safety control structure relating to the loss and any weakening of the safety control structure over time

Generally speaking in the world of oil and gas and especially in the refinery and petrochemical sector, considering safety as a top priority is well established. Chevron made many efforts like developing management systems and providing tools and training employee to improve safety in operations. Despite all these efforts with the purpose to operate the refinery safely, in 2012 the fire accident happened in the refinery. Similarly, at the industry level many accidents happen in the face of all efforts companies are doing to improve safety.

Safety is considered as an emergence property of the systems. It emerges from the interactions of system's components. Each component within a system needs to play its role in providing adequate control and communicating correctly with other components. According to Rasmussen most the major accidents happen when a system migrate toward safety margins over time. Richmond refinery fire case was a similar one as maintaining the integrity of such amount of piping components is challenging and can result in a migration toward unsafe piping.

According to the CSB investigation reports, the use of clamps on various piping had become more common over time in the refinery and in some cases clamps were not removed even in turnaround. This examples shows how a system can migrate to an unsafe state over time gradually. Other aspects like modifications in corporate structure and planning, regulatory updates and enforcements, commercial requirements, community perceptions, etc. change from one point time to another point and in either way, directly or indirectly migrate the status of the system from one point to another point which could impacts on the safety of the installations and in this specific case of the physical integrity of the equipment and piping.

In case of Chevron refinery the team present in the refinery at the time of 4 side cut leak discovery came to a conclusion to make a temporary repair using clamp. The reason behind this decision could be time or resource constraints or any other issue. However, any of these factors or the pressure from regulatory or community had caused this decision to be taken. The point is that safety state of the refinery and personnel perception about the safety had been changed over time.

Another point is the removal of sulfur recovery equipment from the 4 side cut circuit when this circuit was built from carbon steel and was not designed to tolerate sulfur content more than a certain amount. However, the impact of sulfur recovery equipment removal was not assessed properly and it impacted 4 side cut piping. This means the change that could occur over time because of sulfidation was not managed adequately. There were other changes in the crude and management of change was carried out. However, the management change was assessing the impact of these changes on operational conditions without covering the impact of these changes on the sulfidation corrosion.

When ETC launched the initiative on prevention of sulfidation called 'Sulfidation Failure Prevention Initiative' important change happened in the FER BIN. The person who led FER BIN retired 2010 when initiative was not fully developed yet and consequently not implemented. This individual had a very close working relationship with ETC and specifically with those who were involved in preparation of the ETC Sulfidation Failure Prevention Initiative. During 2010 there were other organizational changes affecting the FER BIN role and reporting channels. The position of retired leader was not filled during four months and due to the changes new FER BIN leader had limited power to enforce the implementation of the ETC initiative on sulfidation in refineries.

In order to realize that the refinery as a system is migrating to a hazardous situation, it is necessary to study the refinery operations entirely as a system and not focus only physical equipment and proximate events. For this, the entire refinery process including all internal and external controllers have to be analyzed. It is necessary to include different contextual factors or changes and movements that could affect or make influence on controllers or their behavior. Since normally in refineries the decision process is not simple and requires coordination and communication between different stake holders, an accurate work process and information channels is very important. Specifically when it comes to process safety and prevention of major accidents these are highlighted and their important become more obvious.

STEP 9: Generate recommendations

Doing investigation based on the previous investigation report has its own complexities. Specifically, when there is no access to refinery documents and there is no chance to make interview with those who were involved in the accident and had a role in the safety control structure. This limit the capacity in generating recommendation. Nevertheless, in this study CAST analysis is applied and it was possible to identify inadequacies in control and feedback for each controller. The study covered different controllers at different levels of the safety control structure. It highlighted the contribution of each controller in failing to prevent the release of hydrocarbon, fire and its subsequent impact on local residents in the area. Taking into consideration the failures or inadequate controls identified in previous Steps of CAST different recommendations were generated that are classified under in three levels: Chevron USA, Standard and Code producer bodies like API and ASME and Regulatory bodies like EPA and OSHA. A summarized of these recommendations is provided below:

Chevron USA:

- Review the MOC procedure in order to ensure that it is comprehensive and includes all types of changes. And improve its implementation by ensuring that the roles and responsibilities are adequately assigned and responsible persons are competent. MOC was not done properly when sulfur removal unit was taken out of service and when there were changes in feed and operating condition.
- Detect the areas impacted by sulfidation corrosion across all units following the industry best practice recommendation and ETC initiative on either 100 % inspection on carbon steel pipes susceptible to sulfidation corrosions or replacement of the carbon steel pipes with low silicon content susceptible to sulfidation corrosions.
- Evaluate the possibility of 4-sidecut section isolation from column in case of rupture and also the other circuits similar to 4-sidecut that has the potential to release huge volume of hazardous materials in case of rupture.
- Prepare a leak response policy in order to avoid similar operational decisions in case of occurrence of other leaks with potential escalation if not shutting down the plant.
- Include the requirement of multidisciplinary risk assessment and evaluation of response actions before taking major decisions in case of an emergency in the Emergency Response Documents.
- Review the turnaround process in a manner that the rejected works are reviewed by refinery manager (installation responsible) and also the process and especially the rejected works are auditable.
- Enforce the compliance with duties and responsibilities through competency assurance, training, code and ethics policy.

- Design a system that guaranty an adequate leadership at installation management level and their involvement in safety issues.
- Facilitate the ETC with monitoring authority on the implementation level of the issued guidelines in the business units. And ETC to provide an implementation plan associated with new guidelines.

Standard and Code producer bodies like API and ASME:

- Have consistent technical information and guidance in their publications. In this case on sulfidation corrosion in API RP 571, API 570, API RP 578, API RP 574 and API RP 939-C.
- Avoid voluntary and permissive language in code and standards as much as possible.

Regulatory bodies like EPA and OSHA:

- EPA to provide more requirement and oversight of RMP and increase on-site inspections or audits. Also to implement CSB recommendations and apply past accident lessons in its management.
- California OSHA to provide adequate review of company's PHA, develop means to detect the state of process safety in each facility, improve the regulation requirements considering lesson leant from accidents, audit findings and industry best practices.
- California EPA to adopt a risk based approach rather that prescriptive approach which in some situations may increase the risk instead of reduction.
- California State Governor, Richmond Mayor and City Council to improve the quality of facility audits and also the enforcement of resources.
- CCC to have prepared officers for possible emergency scenarios in the area. And also to provide inherent safer system requirements for existing facilities and to improve the quality of audits taking into account industrial best practices.

5.3. Chevron Richmond Refinery Accident analysis using FRAM method

To apply FRAM methodology it is required to describe the system within which accident happened through functions and corresponding aspects. In a generic manner Chevron Company system, including its business units and refineries, has to be understood and more specifically Richmond refinery and its activities. Undoubtedly describing this vast system requires its time, effort and access to the information that is not available for this work, and in order to carry out this study it is more reasonable to apply the FRAM methodology on those functions of the system that have some interactions with the accident.

5.3.1 Creating FRAM Model – Functions and aspects

Accident description is used to characterize the normal working operations in Chevron and more precisely in Richmond refinery. This result in having system description through a series of interrelated functions

These functions can be classified in three categories:

1. Functions related to emergency operations in Richmond refinery
2. Functions related to the Richmond refinery operations
3. Functions related to Chevron organizational operations

All the operations carried out to mitigate the incident are captured in the first category. They are mainly done as reaction to the release. It is understood that what happened on the day of incident is normal on this kind of situations, and it is reflected in the proposed functions and their aspects. This category includes the following functions:

- Call fire brigade department: normal operation against release notice
- Create an action group: a function developed by the firefighters, operational and inspection personnel
- Establish hot zone: function carried out by firefighters before commencing any other activities
- Repair leak by Clamp: activity carried out to repair piping with small damage
- Remove insulation: operation carried out by firefighters as a response to releases with the objective of being able to observe the leak point and repair it

It is considered that the abovementioned functions are the related functions to the emergency operations of the system that their variation and interaction contributed in the accident, although the analysis on how they could contribute will be developed at the end of this section after having all the considered functions described.

The function ‘call fire brigade department’ is human type and present the following aspects:

- Input: leak discovery
- Output: firefighters

For description of the functions, only those aspects related to the accidents are considered. With this approach the model is not going to be complicate and it prevent to include not properly known information that could lead to less effective application of the methodology.

The output variability is characterized as just in time and precise. Regarding the time, it is an operation that is executed against certain emergency situations which usually does not occur late, and attending to the precision presents a very small margin of error, being a simple operation.

The function ‘*create an action group*’ is an organizational function, to understand the interaction of several agents, although there is no written organizational procedure on how to establish this group, considering that the establishment of the group depends on the different situations in which it forms. Its aspects are the followings:

- Input: leak discovery
- Output: decisions of the action group.
- Precondition: firefighters.
- Resource: information from the database.

In relation to the time the output does not present a significant variability, considering that the function is given usually just in time. In turn, since it is a function in which different people and agents take part, the output shows an acceptable precision, which means that they have some variability, which can be manifested in the decisions of the action group in making the decisions appropriate to the circumstance, and to the action group that its members are not appropriate.

The function of '*establish hot zone*' is a function of the human type, whose aspects are as followings:

- Input: leak discovery
- Output: hot zone (or cold zone)
- Resource: firefighters (it has been considered a resource because it is necessary for the function to be executed and establish the control of the same).

Its Output, with respect to the time, is given too soon, because the function is executed as soon as firefighters arrive and only with the preliminary information on the circumstances. About the precision is considered acceptable, because specialized professionals develop it.

The function '*repair leak by clamp*' is of the human type and presents the following aspects:

- Input: decision of the action group.
- Output: pipe in good condition.
- Precondition: uninsulated piping; information about the status of the piping.
- Control: firefighters; action group; hot zone.

About time, as it is a repair on an existing leak and the decision on repair (including how to do it) and the repair itself consume a significant time, it is considered that the output is given too late. In turn, the accuracy is qualified as acceptable, since it is not an excessively complicated operation, assuming the highest degree of complication that is performed on a pipe in process.

The function '*remove insulation*' is considered as a human type function and is characterized by the following aspects:

- Input: decision of the action group.
- Output: uninsulated pipe.
- Precondition: insulated pipe; information about the status of the pipe.

- Control: firefighters.

Regarding the time this function does not impose any variability on its output as usually it occurs on time without further delay when the function is activated and the preconditions exist. In a similar way, its output is also precise, because it is a simple operation that can be carried out by different methods, so that if one fails or the action cannot be completed through it there are others to achieve the same output.

The second category includes those activities that are carried out in the day-to-day of the Richmond refinery, among them, for the present analysis the following have been considered:

- Check piping and equipment: periodic activity according to operating procedure.
- Report piping status: action taken by inspectors when information on the status of pipes and components is required.
- Fill in the thickness database: activity developed by the inspectors who carry out inspections of the pipes according to an operational procedure
- Recommend activities for the turnaround: activity developed by any operator based on their own knowledge.
- Execute the activities of the turnaround: a function that includes all the tasks developed during the maintenance turnaround.

The function '*check piping and equipment*' is of the human type and its aspects are the following:

- Inputs: Work Order (WO) generated periodically; WO generated from a recommendation.
- Outputs: observations of checks.
- Control: check route; register form.

About time, the output of the function can occur regularly too late. About precision, an acceptable variability has been taken, since the operator normally reports the observations he/she makes, without modifying them.

The function '*report piping status*' is a human function whose aspects are:

- Inputs: observations of checks.
- Output: information about the status of the piping.
- Control: information from the database.

In a similar way to the previous function, the output with respect to time may be too late, and this output can only be used to correct problems but not to prevent them. Regarding the precision, it has been considered as acceptable, since it is a simple function which consists of reproducing information that has been previously obtained.

'Fill in the thickness database' is a human function and presents the following aspects:

- Inputs: WO generated from a recommendation; WO generated periodically; Activities developed during the turnaround.
- Output: information in the database.
- Control: operating procedure to take thickness.

Regarding the time the function output is always given in the right time, there is always updated information on the thickness of the pipes in the database. In turn, the output of the function is imprecise, although this imprecision does not derive from the thicknesses that are collected in the database itself, but it comes from the recorded thicknesses which are measured according to the control aspect *operating procedure to take thickness*.

The function *'recommend activities for turnaround'* is a human function and presents the following aspects:

- Inputs: ETC reports; corrosion mitigation plans; trainings; corporate procedures; Information about the status of the pipes.
- Output: proposed activities for turnaround

In relation to the time, the output usually occurs in the right time, which means that the activities for the turnaround are presented to the IMPACT team when they make sense and can serve to avoid what they are proposed for. Regarding precision it has been considered acceptable.

The function *'execute the activities of the turnaround'* is of human type and only two aspects are necessary to define it in the terms of the proposed scope:

- Input: activities developed during the turnaround.
- Output: piping in good condition.

Regarding the time, the output is given in the right time, which is precisely after the completion of the maintenance turnaround when it is ensured that the necessary activities to have pipes in good condition are performed. However, this output cannot be considered as precise, but only acceptable, because the performed activities are limited, and are not always carried out completely, due to the time limitation, therefore it cannot be ensured 100% that after the maintenance turnaround the pipes are in perfect condition, although if the system works correctly this is the most likely.

In the third category, functions related to Chevron's organizational operations cover those functions that integrate the Company organizational activities that affect the operations and safety of the Richmond refinery. The functions considered in this category are the following:

- Maintenance preparation: activity performed to determine the operations necessary to carry out the maintenance.
- Develop technological solutions: ETC activity.

- Homogenize reliability activities: FER BIN activity.
- Preparation of the inspection guide for the refinery piping: Activity consisting in writing and keeping updated the reference guide used both to calculate the required minimum thickness and to determine the points subject to inspection.
- Plan the activities of the turnaround: an activity developed by a dedicated team to determine what maintenance activities have to be performed during the turnaround.
- Prepare the framing document: an activity carried out by a team dedicated years before the turnaround for which the framing document will be used.
- Turnaround planning team training: activity consisting in training the IMPACT team and a dedicated team to develop the framing document.

In this category, most of the functions are considered as original and consequently they are not analyzed since it is understood that their variability is insignificant and they don't provide resonance to the system. They are only provided to be able to close the model.

'Homogenizing the activities of the FER BIN' is an organizational function that has been described through the unique use of 2 aspects, an input and an output:

- Input: ETC reports.
- Output: WO generated from a recommendation.

There are other aspects that could have been included in this function. At global level, the function is not properly defined only with these two aspects, however, as already stated, for the analysis these are enough and it is not necessary to use others that would only increase the magnitude of the model without providing significant information.

The output of this function has been considered precise, but slow, in terms of time is given too late. This is because the function requires a careful study by an independent unit such as the FER BIN that has to use specific channels to get their recommendation, which is a considerable time delay.

The function *'plan the activities of the turnaround'* is of the organizational type and presents the following aspects:

- Inputs: planned turnaround; proposed activities for the turnaround.
- Outputs: activities developed during the turnaround.
- Control: framing document; IMPACT group; information of the database; minimum required thickness.

About the time, the output of the function has been considered as on time as the plan is prepared for turnaround. Because of the complexity of the selection process it is possible that some necessary activities are left out and consequently the output is not considered as precise, but acceptable.

Finally, there are three functions that do not fall into any of the above categories, and do not share aspects of each other to form a new category, and defining a category to locate each one of them is meaningless. These functions are:

- Contain the fluid: technical function performed by the pipes through which the hydrocarbons are transported.
- Calculate the minimum required thickness: activity performed when a minimum thickness of alert has been found.
- Design the pipe: function by which the requirements of the pipe are established.

As it appears in its definition, the function '*contain the fluid*' is a function of the technical type and presents the following aspects:

- Input: pipe requirements.
- Outlet: isolated pipe.
- Control: pipe in good condition.

The output of the function occurs in the right time, there being no variability of the same with respect to time, although in terms of precision there is some variability, which is qualified as acceptable.

'*Calculate the minimum required thickness*' is a human function and is characterized by:

- Input: information from the database.
- Output: minimum required thickness.
- Control: inspection guide for Chevron refinery lines.

Regarding the time, variability has not been considered, resulting in output in the right time. However, regarding precision, it has been qualified as imprecise, because the complex nature of the calculation it is not very likely that the calculated thickness is not adequate. In addition, by using information from the database as input, the calculated thickness should be applied only to the sections corresponding to those collected by the database, and yet the result is also used for similar sections, even if their data are not used.

Figure 51 shows graphically the FRAM model developed to analyze the Chevron refinery accident. The couplings between the different functions that have been used to develop the model can be seen in the figure. This level of interaction is predictable for the analyzed system, in which there are very diverse agents whose work is strongly related, although they are not aware of this interaction.

Figure 51 FRAM model developed to analyze the Chevron refinery accident

5.3.2 Analysis – Instantiation

Once the model of the system is developed, an instantiation of the model is done, analyzing variability of the functions and consequently “*Contain the fluid*” function is identified as the one where the variability increased throughout the system and exceeded the critical level which resulted in the accident. The reason for having such variability in a technical function is due to coupling with the following functions:

- “*Design the pipe*” (output-input coupling)
- “*Repair the leak by clamp*” (output-control couplings)
- “*Execute the activities of turnaround*” (output-control couplings)

Their outputs were not as expected and consequently affected the “*Contain the fluid*” function negatively. There are also other couplings between these three functions and other functions allowing the variability to increase throughout the system. “*Plan the activities of turnaround*” is identified as the function with more couplings among the ones which have influence in the accident. “*Contain the fluid*” and “*Plan the activities of turnaround*” functions are analyzed below.

“*Contain the fluid*” is the function in which the accidental output resulted in release of hydrocarbon, or accident, instead of “*Isolated pipe*”. Table 1 includes this function and its aspects. Although this function is a technical one and the intrinsic variability is small, due to functional couplings the variability of this function was amplified very significantly.

Table 1 “*Contain the fluid*” function and its aspects

Function: Contain the fluid	
Aspect	Aspect description
Input	Pipe requirements
Output	Isolated pipe
Control	Pipe in good condition

There are two types of couplings that directly affect this function; output-input and output-control. The first one is part of a background function, “*Design the pipe*”, which initially should not present any variability, however, considering particularity of the case study, the issue is that the pipe was not designed adequately to withstand the sulfidation corrosion, so this is the first factor influencing the variability of the output. The second coupling type is still more important, because it is on the control of the function, which is the aspect that controls the output of the function to be the expected one. This aspect is “*Pipe in good condition*” and is the output of two different functions; “*Execute the activities of turnaround*” and “*Repair the leak by clamp*”. These are human functions that have potential variability. Additionally, both functions have functional couplings, which caused that the variability of their output was greater, resulting that the “*Pipe in good condition*” aspect in the case study was not given and rather resulted in pipe in bad condition. The analysis of these functional couplings provides a better understanding of why the accident occurred.

The function “*Repair the leak by clamp*” serves to repair small leaks where the pipe has structural integrity to support a clamp. In the case of the accident the cause of the leak was sulfidation corrosion which implies that the leak cannot be repaired with a clamp. Thus, the clamp should not have been used, but due to the decision of the action group it was used, which in turn is the output of the “*Create an action group*” function. This function would present information of different nature as resource, but in this case only the “*Information of the database*” was presented. This information was not so representative of the corroded pipe and was used in making the decision to repair the leak using a clamp, therefore for this function followings are present: the influence of an output-input coupling between the functions “*Create an action group*” and “*Repair leak by clamp*”, and the output-resource coupling between the functions “*Fill in the thickness database*” and “*Create an action group*”.

On the other hand, the aspect “*Pipe in good condition*” is the output of the function “*Execute the activities of turnaround*”. This function does not present more aspects than its input, and its potential variability is not great, however, in the instantiation, its output did not turn out to be the expected. This is because some of the necessary maintenance activities for the damaged pipe were not carried out completely, which prevented taking the necessary measures to ensure the good condition of the pipe. In addition, this function represents only the execution of those activities which are programmed for the turnaround (input of the function), so if the necessary activities to ensure the good condition of the pipe are not programmed, as is the case here, therefore the pipe is in poor condition.

The explanation of the last one is found in the variability of the aspect *“Activities programmed for turnaround”* that is the output of the function *“Plan the activities of turnaround”*, and that has numerous couplings, consequently it can be considered as one of the more complex functions of the system. The control of this function is marked by aspects such as *“Information of the database”*, which has been discussed already, *“Framing document”*, *“Inspection guide for Chevron refinery lines”*, *“Regulations”*, *“Codes and standards”* and *“Minimum required thickness”*, which is output from a human type function, and its potential variability is not large, but it exists and in the case of instantiation the minimum thickness used for the decision making of maintenance activities on the damaged pipe was incorrect, which led to the elimination of the necessary activities. In this case requirements of various codes and standards were not consistent which resulted in a variability in this control aspect and consequently in the output of the function. *“Codes and standards”* is the output of a function called: *“Develop standard and guideline for the industry (API, ASTM, NFPA, etc.)”* which has output-input and output-control couplings with following functions: *“Design the pipe”*, *“Develop technological solutions (by ETC)”*, *“Preparation of the inspection guide for the refinery piping”*, *“Prepare the framing document”*, *“Plan the activities of turnaround”*, *“Audit/Inspect the industry by governmental bodies on regulatory compliance”*. Consequently, any variability in its output impacts all these mentioned functions.

Lastly, there is also an output-input coupling which is *“Proposed activities for turnaround”* aspect as output of *“Recommend activities for turnaround”* function whose inputs are all those aspects that can result, in one form or another, in a formal proposal of an activity. In the case study there was not a great variability on this aspect, since there were many activities aimed at improving the condition of the damaged section, but because of the complexity of the function *“Plan the activities of turnaround”* due to its multiple aspects, these proposals did not work and ultimately resulted in a pipe in bad condition, which caused the accident.

5.3.3 Recommendations

As a result of the provided analysis following functions are identified as the ones that influenced in the accident: *“Contain the fluid”*, *“Create an action group”*, *“Repair the leak by clamp”*, *“Fill in the thickness database”*, *“Execute the activities of turnaround”*, *“Prepare the framing document”*, *“Plan the activities of turnaround”*, *“Recommend activities for turnaround”*, *“Preparation of the inspection guide for the refinery piping”*, *“Develop technological solutions (by ETC)”*, *“Develop standard and guideline for the industry (API, ASTM, NFPA, etc.)”*. And below is a summary of the recommendations:

- Pipes are not designed adequately to withstand the sulfidation corrosion, therefore either replace them fully or ensure that they can withstand up to programmed replacement date by proper inspections and maintenance program.
- For critical decisions involve all the related disciplines. Within operational procedures or emergency response plan define the disciplines to be involved.
- Modify the turnaround programming to ensure necessary activities are included in turnaround program. Take into account *“Inspection guide for Chevron refinery lines”*, *“Regulations”*, *“Codes and standards”* and *“Minimum required thickness”* amongst others.
- Ensure that the requirements of codes and standards (API, ASTM, NFPA, etc.) are consistent.

5.4. Chevron Richmond Refinery Accident analysis by CCPS using AcciMap method

An AcciMap of the Chevron accident has been developed by CSB investigation team which is showed in Figure 52. The AcciMap depicts immediate causes as well as higher level contributing causes at the corporate, governmental, and regulatory levels. This diagram includes five levels:

1. Outcomes: the impact of the August 6, 2012, event to workers present and the surrounding community
2. Physical Events and Conditions: the immediate causes of the incident as displayed in a traditional logic tree
3. Chevron: company rules and policies; conduct of turnarounds; risk management; identification of hazards and evaluation of safeguards; adoption of internal recommendations; safety programs; and emergency response
4. Industry Codes and Standards: good practice guidelines that provide safety requirements and recommendations on topics including mechanical integrity and emergency response; and
5. Government: laws and legislation developed to regulate process safety at refineries.

Figure 52 AcciMap of the Chevron accident (U.S. Chemical Safety and Hazard Investigation Board (CSB), Final Investigation Report, Report No. 2012-03-I-CA, 2015)

The contributing factors are discussed in the CSB Chevron investigation reports; 2013 Chevron Interim Report (U.S. Chemical Safety and Hazard Investigation Board (CSB), Interim Investigation Report, 2013), 2014 Chevron Regulatory Report (U.S. Chemical Safety and Hazard Investigation Board (CSB), Regulatory Report, Report No. 2012-03-I-CA, 2014) and 2015 Chevron Final Investigation Report (U.S. Chemical Safety and Hazard Investigation Board (CSB), Final Investigation Report, Report No. 2012-03-I-CA, 2015).

The CSB investigation reports identify findings in various areas: Technical, Organizational, Emergency Response, Safety Culture, Industry Codes and Standards, and Regulatory. These reports include recommendations to different bodies:

API: Revise the following publications to improve sulfidation corrosion management and leak response: API RP 939-C, API RP 571, API 570, API RP 578, API RP 574 and API RP 2001

ASME: Refer users to follow the leak response guidance developed by the American Petroleum Institute prior to conducting leak repairs

Chevron USA:

Perform a documented damage mechanism hazard review at all Chevron U.S. refineries. Report leading and lagging process safety indicators. Develop an accountability method at Chevron to identify and track effective implementation of Chevron or industry best practices to ensure process safety or employee personal safety. Develop an auditable process for all recommended turnaround work items related to inspection or mechanical integrity recommendations that are denied or deferred. This process shall provide the submitter of the denied or deferred recommendation with a mechanism to further elevate and discuss the recommendation with higher level management. Develop an approval process that includes a technical review that must be implemented prior to resetting the minimum alert thickness to a lower value in the inspection database.

EPA:

Jointly plan and conduct inspections with Cal/OSHA, California EPA and other state and local regulatory agencies with chemical accident prevention responsibilities to monitor the effective implementation of the damage mechanism hazard review

California State Legislature, Governor of California, Mayor and City Council-City of Richmond- California and Board of Supervisors- Contra Costa County- California:

Enhance and restructure California's process safety management (PSM) regulations by including the goal-setting attributes for petroleum refineries in the state of California.

Establish or cause to be established a compensation system to ensure regulator capability in process safety oversight and policy development in Richmond, California.

Revise the Industrial Safety Ordinance (ISO) regulations for petroleum refineries to require the development of an oversight committee comprised of the regulator, the company, the workforce and

their representatives, and community representatives. Among the duties of this committee shall be to oversee the development and implementation of action items created as a result of safety culture assessment findings.

Revise the Industrial Safety Ordinance (ISO) to require that Process Hazard Analyses include documentation of the recognized methodologies, rationale and conclusions used to claim that safeguards intended to control hazards will be effective.

Revise the Industrial Safety Ordinance (ISO) to require the documented use of inherently safer systems analysis and the hierarchy of controls to the greatest extent feasible in establishing safeguards for identified process hazards.

Ensure the effective implementation of the damage mechanism hazard review program. Monitor and confirm the effective implementation of the damage mechanism hazard review program.

Identify and require the reporting of leading and lagging process safety indicators.

Establish a multi-agency process safety regulatory program for all California oil refineries to improve the public accountability, transparency, and performance of chemical accident prevention and mechanical integrity programs

5.5. Discussion

FRAM and CAST are developed as part of this study based on understanding obtained from the CBS reports and also from general knowledge of the process in general. In both cases the information provided in the accident description section of the CBS reports was used without previously reading the recommendations of the reports. Then the outcome and obtained recommendations were compared with the recommendations provided in the CBS reports. It is understood that the outcome could be improved, but it is adequate for demonstration, analysis and comparison. A summary of this comparison is provided in Table 2. If a recommendation is provided by a method, it is marked with a tick in the column corresponding to the method. The comparison is based on the concept of each recommendation, as the wordings are not exactly similar.

Table 2 Summary of comparison made between recommendations generated by AcciMap, FRAM and CAST

Recommendations	AcciMap	FRAM	CAST
Regulatory bodies (EPA, California State Legislature, Governor of California, Mayor and City Council-City of Richmond- California and Board of Supervisors- Contra Costa County- California):			
Jointly plan and conduct inspections with Cal/OSHA, California EPA and other state and local regulatory agencies with chemical accident prevention responsibilities to monitor the effective implementation of the damage mechanism hazard review.	√		
Establish or cause to be established a compensation system to ensure regulator capability in process safety oversight and policy development in Richmond, California.	√		

Revise the Industrial Safety Ordinance (ISO) regulations for petroleum refineries to require the development of an oversight committee comprised of the regulator, the company, the workforce and their representatives, and community representatives. Among the duties of this committee shall be to oversee the development and implementation of action items created as a result of safety culture assessment findings.	√		
Adequate review company's PHA and ensure it includes documentation of the recognized methodologies, rationale and conclusions used to claim that safeguards intended to control hazards will be effective.	√		√
Ensure the effective implementation of the damage mechanism hazard review program. Monitor and confirm the effective implementation of the damage mechanism hazard review program.	√		
Develop means to detect the state of process safety in each facility including identification and reporting of leading and lagging process safety indicators.	√		√
Establish a multi-agency process safety regulatory program for all California oil refineries to improve the public accountability, transparency, and performance of chemical accident prevention and mechanical integrity programs	√		
EPA to provide more requirement and oversight of RMP and increase on-site inspections or audits. Also to implement CSB recommendations and apply past accident lessons in its management.			√
California OSHA to improve the regulation requirements considering lesson learnt from accidents, audit findings and industry best practices.			√
California regulator to adopt a risk based approach rather than prescriptive approach which in some situations may increase the risk instead of reduction.	√		√
California State Governor, Richmond Mayor and City Council to improve the quality of facility audits and also the enforcement of resources.			√
CCC to have prepared officers for possible emergency scenarios in the area.			√
CCC to provide inherent safer system requirements for existing facilities and to improve the quality of audits taking into account industrial best practices.	√		√
Standard and Code producer bodies like API and ASME:			
ASME: Refer users to follow the leak response guidance developed by the American Petroleum Institute prior to conducting leak repairs	√		
Have consistent technical information and guidance in their publications. In this case on sulfidation corrosion in API RP 571, API 570, API RP 578, API RP 574 and API RP 939-C.	√	√	√
Avoid voluntary and permissive language in code and standards as much as possible.			√
Chevron USA:			
Perform a documented damage mechanism hazard review at all Chevron U.S. refineries.	√		
Report leading and lagging process safety indicators.	√		
Develop an accountability method at Chevron to identify and track effective implementation of Chevron or industry best practices to ensure process safety or employee personal safety.	√		√

Develop an auditable process for all recommended turnaround work items related to inspection or mechanical integrity recommendations that are denied or deferred. This process shall provide the submitter of the denied or deferred recommendation with a mechanism to further elevate and discuss the recommendation with higher level management.	√	√	√
Develop an approval process that includes a technical review that must be implemented prior to resetting the minimum alert thickness to a lower value in the inspection database.	√		
Review the MOC procedure in order to ensure that it is comprehensive and includes all types of changes. And improve its implementation by ensuring that the roles and responsibilities are adequately assigned and responsible persons are competent. MOC was not done properly when sulfur removal unit was taken out of service and when there were changes in feed and operating condition.			√
Detect the areas impacted by sulfidation corrosion across all units following the industry best practice recommendation and ETC initiative on either 100 % inspection on carbon steel pipes susceptible to sulfidation corrossions or replacement of the carbon steel pipes with low silicon content susceptible to sulfidation corrossions.		√	√
Evaluate the possibility of 4-sidecut section isolation from column in case of rupture and also the other circuits similar to 4-sidecut that has the potential to release huge volume of hazardous materials in case of rupture.			√
Prepare a leak response policy in order to avoid similar operational decisions in case of occurrence of other leaks with potential escalation if not shutting down the plant.			√
Include the requirement of multidisciplinary risk assessment and evaluation of response actions before taking major decisions in case of an emergency in the Emergency Response Documents.		√	√
Enforce the compliance with duties and responsibilities through competency assurance, training, code and ethics policy.			√
Facilitate the ETC with monitoring authority on the implementation level of the issued guidelines in the business units. And ETC to provide an implementation plan associated with new guidelines.			√

AcciMap identified contributing factors both close to the accident and far from the accident. Consequently, it generated recommendations for different levels of control structure: Chevron USA, standard bodies and regulatory bodies. CAST identified the control and feedback inadequacies for each component/controller at different levels of the safety control structure that failed to prevent the accident and/or to protect the local residents from the released hazard. It identified contributing factors in different level of safety control structure with recommendations for each level: Chevron USA, standard bodies and regulatory bodies. FRAM identified functions that their variability increased significantly due to functional couplings that resulted in the accident. It identified contributing factors that are both close to the accident and far from the accident but their locations in control structure level were not been determined. In fact, FRAM does not define the control structure in a hierarchical level similar to AcciMap and CAST, but it could reach different levels even far from the accident depending on the functions that are identified. It generated recommendations related to the Chevron USA and standard bodies.

When models are developed, CAST is likely to be more instrumental and comprehensive in generation of recommendations because it already captured failures/inadequate controls, unsafe decisions/control actions and process model flaws.

Although there were some shortages on information while applying CAST and FRAM in this study comparing with the AcciMap done by CSB, the generated recommendations by CAST are comparable with the ones of AcciMap. Since CAST develops and analyzes the system hierarchical control structure, it provides a context leading to a more complete understanding of the causes of the accident, enhancing the ability to identify system improvements.

A summary of this chapter published in Process Safety Progress Journal DOI 10.1002/prs.12002.

Chapter 6: Case Study: Applying STPA on a process plant and comparing the outcome with the result of HAZOP

In this chapter, STPA is applied to a gas process plant. The outcome of the STPA application is compared with the recommendations generated by the HAZOP study (Hazard and Operability study) of the plant carried out during the engineering phase.

HAZOP is a structured and disciplined examination for identification of potential hazards and operational problems in a process. This study is carried out by a multidisciplinary team when the P&IDs (piping and instrument diagrams) become available. It divides the plant in sections or nodes and analyses the deviations from normal operating conditions. Guide words and process parameters are combined to generate deviations. For each deviation possible causes are identified and consequences are determined. It is necessary to identify existing safeguards and assess the risk. If the risk is not acceptable recommendations are generated in order to reduce the risk. A list of some guide words, parameters and examples of deviations are provided in Table 3.

Table 3 A list of guide words, parameters and examples of deviations

Guide word	Parameter	Deviation
No	Level	More level
More	Flow	No flow
Less	Pressure	High pressure
Other than	Temperature	Less pressure
Reverse	Composition	Reverse flow
Part of	Services	Etc.

This approach is applied to each node until the entire scope of the study is covered. An example of the HAZOP sheet including the abovementioned information is provided in Table 4.

Table 4 A model of HAZOP sheet

Company Name & Logo					HAZOP Worksheet							
Node:					Node Description:							
Parameter:					Project:				P&ID:			
Guide word	Deviation	Causes	Consequences	Safeguards	Risk				Actions	By	Date	
					C	E	L	R				

HAZOP was developed originally by ICI (Imperial Chemical Industries) in the 1960s. It is a standardized best practice which is widely used in the process industry and there are numerous papers, publications, guides and references on HAZOP. International Electrotechnical Commission (IEC) standard on HAZOP (IEC 61882 standard, 2016) is an example of numerous publications on HAZOP.

Figure 53 A train of air cooler and separator

6.2. Application of STPA

STPA is applied on the described process in accordance with STPA Handbook (Leveson & Thomas, STPA Handbook, 2018) following steps shown in Figure 29 and described below:

Step 1) Define purpose of the analysis

- Identify system boundary
- Identify possible accidents (losses) that may occur in the system
- Identify the hazards in the system
- Identify system-level safety constraints

Step 2) Model the control structure

- Draw the control structure for the system under study
- Create the process model and identify the variables of this model

Step 3) Identify unsafe control actions

- Identify control actions
- Postulate control action behaviors: control action is provided, not provided, provided too early or too late, or stopped too soon
- Determine if control action behaviors are unsafe for each scenario
- Define constraints on the behavior of controllers

Step 4) Identify loss scenarios

- Identify possible causes of unsafe control actions or improper execution of control actions causing hazards (loss scenarios)
- Eliminate or mitigate hazard through the establishment of recommendations

6.2.1 Define purpose of the analysis

Identifying losses: in order to identify losses, the definition of loss is provided here: A loss involves something of value to stakeholders. Losses may include a loss of human life or human injury, property damage, environmental pollution, loss of mission, loss of reputation, loss or leak of sensitive information, or any other loss that is unacceptable to the stakeholders. Following losses are identified for the system under study:

L-1: Loss of human life or injury to people

L-2: Environmental loss

L-3: Loss of or damage to asset

System and boundaries: Production facilities from the plant inlet to the outlet before connecting to the existing facilities.

Identifying system-level hazards: in order to identify hazards, the definition of hazard is provided here: A hazard is a system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to a loss. Following hazards are identified for the system under study:

H-1: Uncontrolled or unplanned release of hydrocarbon ignited (L-1, L-3)

H-2: Uncontrolled or unplanned release of liquid hydrocarbon reaching the environment (L-2)

Defining system-level constraints: in order to identify constraints, the definition of constraint is provided here: A system-level constraint specifies system conditions or behaviors that need to be satisfied to prevent hazards (and ultimately prevent losses). Following system-level safety constraints are identified for the system under study:

SC-1: Uncontrolled or unplanned release of hydrocarbon must be prevented, stopped and contained (H-1)

SC-2: Ignition of uncontrolled or unplanned release of hydrocarbon must be prevented (H-1)

SC-3: Ignited uncontrolled or unplanned release of hydrocarbon must not cause human loss and asset damage (H-1)

SC-4: Uncontrolled or unplanned release of liquid hydrocarbon must not reach the environment (H-2)

No.	Hazard	Related loss	Relevant safety constraint
H1	Uncontrolled or unplanned release of hydrocarbon ignited	L-1, L-3	SC-1: Uncontrolled or unplanned release of hydrocarbon must be prevented, stopped and contained (H-1) SC-2: Ignition of uncontrolled or unplanned release of hydrocarbon must be prevented (H-1) SC-3: Ignited uncontrolled or unplanned release of hydrocarbon must not cause human loss and asset damage (H-1)
H2	Uncontrolled or unplanned release of liquid hydrocarbon reaching the environment	L-2	SC-4: Uncontrolled or unplanned release of liquid hydrocarbon must not reach the environment (H-2)

6.2.2 Model the control structure

The next step in STPA is to model the hierarchical control structure.

A Hierarchical control structure is a system model that is composed of feedback control loops. An effective control structure will enforce constraints on the behavior of the overall system. In general, a controller may provide control actions to control some process and to enforce constraints on the behavior of the controlled process. The control algorithm represents the controller's decision making process, it determines the control actions to provide. Controllers also have process models that represent the controller's internal beliefs used to make decisions. Process models may include understanding about the process under control or other relevant aspects of the system or the environment. Process models may be updated in part by feedback receiving from the controlled process.

The control structure is provided in the Figure 54.

Figure 54 Safety Control Structure of the gas plant

6.2.3 Identify Unsafe Control Actions

Once the control structure has been modeled, the next step is to identify Unsafe Control Actions (UCA). UCA is defined as below:

An Unsafe Control Action is a control action that, in a particular context and worst-case environment, will lead to a hazard.

Every UCA contains five parts: <Source> <Type> <Control Action> <Context> <Link to Hazards>

For example for the Basic Process Control (BPC) function as a control action three UCAs can be considered as following:

UCA-1: <Automated process control> <does not provide> <the BPC function> <when the process is out of normal conditions> <[H1, H2]>

UCA-2: <Automated process control> <provides the BPC function too late> <when the process is out of normal conditions> <[H1, H2]>

UCA-3: <Automated process control> <stops providing the BPC function too soon> <when the process is still out of normal conditions> <[H1, H2]>

For this study unsafe control actions up to operations and maintenance in the control structure are identified and summarized in Table 5.

Table 5 Identified Unsafe Control Actions

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Automated process control (BPC) function	UCA-1: Automated process control does not provide the BPC function when the process is out of normal conditions [H1, H2]		UCA-2: Automated process control provides the BPC function too late when the process is out of normal conditions [H1, H2]	UCA-3: Automated process control stops providing the BPC function too soon when the process is still out of normal conditions [H1, H2]
Disable BPC		UCA-4: Operators disables BPC when BPC is required to maintain the process within the normal conditions [H1, H2]		
Manual process control	UCA-5: Operators do not provide intervention when manual process control (intervention by operator) is required [H1, H2]		UCA-6: Operators provide intervention too late when manual process control (intervention by operator) is required [H1, H2]	
Repair and maintain equipment and instruments	UCA-7: Maintenance team do not provide the required repair and maintenance of the equipment and instrument [H1, H2]		UCA-8: Maintenance team provide the required repair and maintenance of equipment and instrument too late [H1, H2]	

Once UCAs have been identified, they can be translated into constraints on the behavior of each controller. A Controller Constraint is defined as below: A controller constraint specifies the controller behaviors that need to be satisfied to prevent UCAs. Table 6 shows the controller constraints of the identified UCAs.

Table 6 Defined constraints on the behavior of controllers

Unsafe Control Actions	Controller Constraints
UCA-1: Automated process control does not provide the BPC function when the process is out of normal conditions [H1, H2]	C-1: Automated process control must provide the BPC function when the process is out of normal conditions [UCA 1]
UCA-2: Automated process control provides the BPC function too late when the process is out of normal conditions [H1, H2]	C-2: Automated process control must not provide the BPC function too late when the process is out of normal conditions [UCA-2]

UCA-3: Automated process control stops providing the BPC function too soon when the process is still out of normal conditions [H1, H2]	C-3: Automated process control must not stop providing the BPC function too soon when the process is still out of normal conditions [H1, H2]
UCA-4: Operators disables BPC when BPC is required to maintain the process within the normal conditions [H1, H2]	C-4: Operators must not disable BPC when BPC is required to maintain the process within the normal conditions [H1, H2]
UCA-5: Operators do not provide intervention when manual process control (intervention by operator) is required [H1, H2]	C-5: Operators must provide intervention when manual process control (intervention by operator) is required [H1, H2]
UCA-6: Operators provide intervention too late when manual process control (intervention by operator) is required [H1, H2]	C-6: Operators must not provide intervention too late when manual process control (intervention by operator) is required [H1, H2]
UCA-7: Maintenance team do not provide the required repair and maintenance of the equipment and instrument [H1, H2]	C-7: Maintenance team must provide the required repair and maintenance of the equipment and instrument [H1, H2]
UCA-8: Maintenance team provide the required repair and maintenance of equipment and instrument too late [H1, H2]	C-8: Maintenance team must not provide the required repair and maintenance of equipment and instrument too late [H1, H2]

6.2.4 Identify Loss Scenarios

Once unsafe control actions have been identified, the next step is to identify loss scenarios.

Definition of loss scenario is provided below: A loss scenario describes the causal factors that can lead to the unsafe control actions and to hazards.

Two types of loss scenarios must be considered:

- Why would Unsafe Control Actions occur?
- Why would control actions be improperly executed or not executed, lead to hazards?

Identifying scenarios that lead to Unsafe Control Actions

In general, scenarios that lead to Unsafe Control Actions may involve:

- Failures related to the controller (for physical controllers)

2. Inadequate control algorithm
3. Unsafe control input
4. Inadequate process model

Considering the identified UCAs, following loss scenarios are identified in Table 7:

Table 7 Identified loss scenarios for UCAs

Unsafe Control Actions	Loss scenarios
UCA-1: Automated process control does not provide the BPC function when the process is out of normal conditions [H1, H2]	Scenario 1 for UCA-1: Process is out of normal conditions but automated process control does not detect it because sensors are not capable to detect the abnormal conditions (not the right sensors selected) [UCA 1]. As a result, hydrocarbon may be released from the process [H1,H2] Scenario 2 for UCA-1: Process is out of normal conditions but automated process control does not detect it because sensors are faulty due inadequate testing and maintenance [UCA 1]. As a result, hydrocarbon may be released from the process [H1,H2] Scenario 3 for UCA-1: Process is out of normal conditions but automated process control does not detect it because set point of sensors were not correctly established in the design [UCA 1]. As a result, hydrocarbon may be released from the process [H1,H2] Scenario 4 for UCA-1: Process is out of normal conditions but automated process control does not detect it because set point of sensors are modified wrongly in the operation [UCA 1]. As a result, hydrocarbon may be released from the process [H1,H2] Scenario 5 for UCA-1: Process is out of normal conditions and automated process control detects it but ignores it because it is not defined as abnormal condition in the process model [UCA 1]. As a result, hydrocarbon may be released from the process [H1,H2] Scenario 6 for UCA-1: Process is out of normal conditions and automated process control detects it but does not provide correct BPC function because BPC function is not defined correctly in the process model [UCA 1]. As a

	result, hydrocarbon may be released from the process [H1,H2] Scenario 7 for UCA-1: Process is out of normal conditions and automated process control detects it but does not provide BPC function because actuators are faulty or incapable to control the process due to inadequate testing and maintenance [UCA 1]. As a result, hydrocarbon may be released from the process [H1,H2]
UCA-2: Automated process control provides the BPC function too late when the process is out of normal conditions [H1, H2]	Scenario 1 for UCA-2: Process is out of normal conditions, but automated process control provided the BPC function too late because feedback about the abnormal conditions is delayed due to sensors maintenance and calibration problems [UCA-2]. As a result, hydrocarbon may be released from the process [H1,H2] Scenario 2 for UCA-2: Process is out of normal conditions, but automated process control provided the BPC function too late because feedback about the abnormal conditions is delayed due to sensors' wrong set point from design [UCA-2]. As a result, hydrocarbon may be released from the process [H1,H2] Scenario 3 for UCA-2: Process is out of normal conditions, but automated process control provided the BPC function too late because feedback about the abnormal conditions is delayed due to sensors' wrong set point from operation (modifications) [UCA-2]. As a result, hydrocarbon may be released from the process [H1,H2] Scenario 4 for UCA-2: Process is out of normal conditions, but automated process control provided the BPC function too late because process model is not correct and wrongly requires late response [UCA-2]. As a result, hydrocarbon may be released from the process [H1,H2] Scenario 5 for UCA-2: Process is out of normal conditions, but automated process control provided the BPC function too late because there is a delay in the final element actuation due to the design of final element [UCA-2]. As a result, hydrocarbon may be released from the process [H1,H2]

	Scenario 6 for UCA-2: Process is out of normal conditions, but automated process control provided the BPC function too late because there is a delay in the final element actuation since it is not being maintained and tested adequately [UCA-2]. As a result, hydrocarbon may be released from the process [H1,H2]
UCA-3: Automated process control stops providing the BPC function too soon when the process is still out of normal conditions [H1, H2]	Scenario 1 for UCA-3: Process is still out of normal conditions, but BPC function stops too soon because the final element fails to continue providing the control action due to not adequate maintenance [UCA-3]. As a result, hydrocarbon may be released from the process [H1,H2] Scenario 2 for UCA-3: Process is still out of normal conditions, but operator stops the control action too soon by error due to not having adequate skills and trainings [UCA-3]. As a result, hydrocarbon may be released from the process [H1,H2]
UCA-4: Operators disables BPC when BPC is required to maintain the process within the normal conditions [H1, H2]	Scenario 1 for UCA-4: BPC is required to maintain the process within the normal conditions, but operators disable the BPC due to faulty alarms because of lack of maintenance/calibration of alarms [UCA-4]. As a result, hydrocarbon may be released from the process [H1,H2] Scenario 2 for UCA-4: BPC is required to maintain the process within the normal conditions, but operators disable the BPC due to its malfunctioning because of lack of maintenance/calibration of initiator, logic solver or final elements [UCA-4]. As a result, hydrocarbon may be released from the process [H1,H2]
UCA-5: Operators do not provide intervention when manual process control (intervention by operator) is required [H1, H2]	Scenario 1 for UCA-5: Manual process control is required, but operators do not provide intervention because they are overwhelmed with the process requirements due to not adequate alarm management [UCA-5]. As a result, hydrocarbon may be released from the process [H1, H2] Scenario 2 for UCA-5: Manual process control is required, but operators do not provide intervention or provide a wrong function because lack of competency or awareness [UCA-5]. As a result, hydrocarbon may be released from the process [H1, H2]

UCA-6: Operators provide intervention too late when manual process control (intervention by operator) is required [H1, H2]	Scenario 1 for UCA-6: Manual process control is required, but operators provide intervention too late because they are overwhelmed with the process requirements due to not adequate alarm management [UCA-6]. As a result, hydrocarbon may be released from the process [H1, H2]
UCA-7: Maintenance team do not provide the required repair and maintenance of the equipment and instrument [H1, H2]	Scenario 1 for UCA-7: Maintenance of the equipment and instrument is required, but maintenance team do not provide the required repair and maintenance because of lack of spares and tools [UCA-7]. As a result, hydrocarbon may be released from the process [H1, H2] Scenario 2 for UCA-7: Maintenance of the equipment and instrument is required, but maintenance team do not provide the required repair and maintenance because of backlog due to inadequate maintenance planning resulted from lack of competency of maintenance team or not enough workers in the maintenance team [UCA-7]. As a result, hydrocarbon may be released from the process [H1, H2]
UCA-8: Maintenance team provide the required repair and maintenance of equipment and instrument too late [H1, H2]	Scenario 1 for UCA-8: Maintenance of the equipment and instrument is required, but maintenance team provide the required repair and maintenance too late because of lack of spares and tools in the warehouse [UCA-8]. As a result, hydrocarbon may be released from the process [H1, H2] Scenario 2 for UCA-8: Maintenance of the equipment and instrument is required, but maintenance team provide the required repair and maintenance too late because of backlog due to inadequate maintenance planning resulted from lack of competency of maintenance team or not enough workers in the maintenance team [UCA-8]. As a result, hydrocarbon may be released from the process [H1, H2]

Identifying scenarios in which control actions are improperly executed or not executed

Hazards can be caused by UCAs, but they can also be caused without a UCA if control actions are improperly executed or not executed. To create these scenarios, we must consider:

1. Scenarios involving the control path (Control action not executed, Control action improperly executed)
2. Scenarios related to the controlled process

Further loss scenarios are identified in Table 8 taking into account the control actions:

Table 8 Identified further loss scenarios for control actions

Control Action	Loss scenarios
CA-1: Automated process control (BPC) function	Scenario 1 of CA-1: Automated process control command is provided, but the process control function is not executed properly due to actuator failure. As a result, hydrocarbon may be released from the process [H1,H2] Scenario 2 of CA-1: Controlled process is not out of normal condition, but automated process control functions improperly due to faulty detections. As a result, hydrocarbon may be released from the process [H1,H2]
CA-2: Disable BPC	BPC disabled while required is already captured as an UCA (UCA-4)
CA-3: Manual process control	Scenario 1 of CA-3: Operator provides manual process control, but it is not executed because of actuator failure due to lack of adequate inspection and maintenance of actuator. As a result, hydrocarbon may be released from the process [H1,H2] Scenario 2 of CA-3: Operator provides manual control improperly when it is not required due to lack of competency. As a result, hydrocarbon may be released from the process [H1,H2]
CA-4: Repair and maintain equipment and instruments	Scenario 1 for CA-4: Repair and maintenance of the equipment and instrument is not executed properly due to: - lack of competency of maintenance team, - inadequate spares and tools, or - lack of proper supervision on maintenance works. As a result, hydrocarbon may be released from the process [H1, H2]

At the end, new safety measures have to be defined to prevent loss scenarios being converted to hazards. List of safety measures corresponding to loss scenarios is provided in Table 9.

Table 9 Safety measure recommended by STPA

Loss scenarios	Safety Measures
Scenario 1 for UCA-1: Process is out of normal conditions but automated process control does not detect it because sensors are not capable to detect the abnormal conditions (not the right sensors selected) [UCA 1]. As a result,	Ensure that right sensor is selected for each process parameter that will be capable to detect the abnormal conditions.

hydrocarbon may be released from the process [H1,H2]	
Scenario 2 for UCA-1: Process is out of normal conditions but automated process control does not detect it because sensors are faulty due inadequate testing and maintenance [UCA 1]. As a result, hydrocarbon may be released from the process [H1,H2]	Test and maintain process parameter sensors adequately. (Prepare a manual for testing and maintenance of process parameter sensors, and ensure that maintenance team is competent and act according to this manual. Design and implement a competency assurance system for maintenance team).
Scenario 3 for UCA-1: Process is out of normal conditions but automated process control does not detect it because set point of sensors were not correctly established in the design [UCA 1]. As a result, hydrocarbon may be released from the process [H1,H2]	Verify that the set point of process parameter sensors are established correctly.
Scenario 4 for UCA-1: Process is out of normal conditions but automated process control does not detect it because set point of sensors are modified wrongly in the operation [UCA 1]. As a result, hydrocarbon may be released from the process [H1,H2]	Prepare a manual for modifying process parameter sensors' set point during operation, and ensure that operation team is competent and act according to the manual. Design and implement a competency assurance system for operators.
Scenario 5 for UCA-1: Process is out of normal conditions and automated process control detects it but ignores it because it is not defined as abnormal condition in the process model [UCA 1]. As a result, hydrocarbon may be released from the process [H1,H2]	Ensure that appropriate function is defined for each abnormal condition in the process control system.
Scenario 6 for UCA-1: Process is out of normal conditions and automated process control detects it but does not provide correct BPC function because BPC function is not defined correctly in the process model [UCA 1]. As a result, hydrocarbon may be released from the process [H1,H2]	Ensure that appropriate function is defined for each abnormal condition in the process control system.
Scenario 7 for UCA-1: Process is out of normal conditions and automated process control detects it but does not provide BPC function because actuators are faulty or incapable to control the process due to inadequate testing and maintenance [UCA 1]. As a result, hydrocarbon may be released from the process [H1,H2]	Test and maintain control system's actuators adequately. (Prepare a manual for testing and maintenance of control system's actuators, and ensure that maintenance team is competent and act according to this manual. Design and implement a competency assurance system for maintenance team).
Scenario 1 for UCA-2: Process is out of normal conditions, but automated process control provided the BPC function too late because feedback about the abnormal conditions is delayed due to sensors maintenance and calibration problems [UCA-2]. As a result, hydrocarbon may be released from the process [H1,H2]	Maintain and calibrate process parameter sensors adequately. (Prepare a manual for testing and maintenance of sensors, and ensure that maintenance team is competent and act according to this manual. Design and implement a competency assurance system for maintenance team).
Scenario 2 for UCA-2: Process is out of normal conditions, but automated process control	Ensure that the set point of process parameter sensors are established correctly.

provided the BPC function too late because feedback about the abnormal conditions is delayed due to sensors' wrong set point from design [UCA-2]. As a result, hydrocarbon may be released from the process [H1,H2]	
Scenario 3 for UCA-2: Process is out of normal conditions, but automated process control provided the BPC function too late because feedback about the abnormal conditions is delayed due to sensors' wrong set point from operation (modifications) [UCA-2]. As a result, hydrocarbon may be released from the process [H1,H2]	Prepare a manual for modifying process parameter sensors' set point during operation, and ensure that operation team is competent and act according to the manual. Design and implement a competency assurance system for operators.
Scenario 4 for UCA-2: Process is out of normal conditions, but automated process control provided the BPC function too late because process model is not correct and wrongly requires late response [UCA-2]. As a result, hydrocarbon may be released from the process [H1,H2]	Ensure that appropriate function is defined for each abnormal condition in the process control system.
Scenario 5 for UCA-2: Process is out of normal conditions, but automated process control provided the BPC function too late because there is a delay in the final element actuation due to the design of final element [UCA-2]. As a result, hydrocarbon may be released from the process [H1,H2]	Ensure that final elements are designed correctly as required by defined functions.
Scenario 6 for UCA-2: Process is out of normal conditions, but automated process control provided the BPC function too late because there is a delay in the final element actuation since it is not being maintained and tested adequately [UCA-2]. As a result, hydrocarbon may be released from the process [H1,H2]	Test and maintain control system's actuators adequately. (Prepare a manual for testing and maintenance of control system's actuators, and ensure that maintenance team is competent and act according to this manual. Design and implement a competency assurance system for maintenance team).
Scenario 1 for UCA-3: Process is still out of normal conditions, but BPC function stops too soon because the final element fails to continue providing the control action due to not adequate maintenance [UCA-3]. As a result, hydrocarbon may be released from the process [H1,H2]	Test and maintain control system's actuators adequately. (Prepare a manual for testing and maintenance of control system's actuators, and ensure that maintenance team is competent and act according to this manual.
Scenario 2 for UCA-3: Process is still out of normal conditions, but operator stops the control action too soon by error due to not having adequate skills and trainings [UCA-3]. As a result, hydrocarbon may be released from the process [H1,H2]	Ensure operators are competent in operating the plant. Design and implement a competency assurance system for operators.
Scenario 1 for UCA-4: BPC is required to maintain the process within the normal conditions, but operators disable the BPC due to faulty alarms because of lack of maintenance/calibration of alarms [UCA-4]. As	Maintain and calibrate process alarms adequately. (Prepare a manual for testing and maintenance of process alarms, and ensure that maintenance team is competent and act according to this manual. Design and implement

a result, hydrocarbon may be released from the process [H1,H2]	a competency assurance system for maintenance team).
Scenario 2 for UCA-4: BPC is required to maintain the process within the normal conditions, but operators disable the BPC due to its malfunctioning because of lack of maintenance/calibration of initiator, logic solver or final elements [UCA-4]. As a result, hydrocarbon may be released from the process [H1,H2]	Test, maintain and calibrate process control elements (initiator, logic solver and final element) adequately. [Prepare a manual for testing, maintenance and calibration of process control elements (initiator, logic solver and final element), and ensure that maintenance team is competent and act according to this manual. Design and implement a competency assurance system for maintenance team].
Scenario 1 for UCA-5: Manual process control is required, but operators do not provide intervention because they are overwhelmed with the process requirements due to not adequate alarm management [UCA-5]. As a result, hydrocarbon may be released from the process [H1, H2]	Carry out an alarm management to ensure that operators are not overwhelmed with the process requirements.
Scenario 2 for UCA-5: Manual process control is required, but operators do not provide intervention or provide a wrong function because lack of competency or awareness [UCA-5]. As a result, hydrocarbon may be released from the process [H1, H2]	Ensure operators are competent in operating the plant. Design and implement a competency assurance system for operators.
Scenario 1 for UCA-6: Manual process control is required, but operators provide intervention too late because they are overwhelmed with the process requirements due to not adequate alarm management [UCA-6]. As a result, hydrocarbon may be released from the process [H1, H2]	Carry out an alarm management to ensure that operators are not overwhelmed with the process requirements.
Scenario 1 for UCA-7: Maintenance of the equipment and instrument is required, but maintenance team do not provide the required repair and maintenance because of lack of spares and tools [UCA-7]. As a result, hydrocarbon may be released from the process [H1, H2]	Design and implement a maintenance management system to ensure adequate maintenance including not facing with lack of required spares and tools for maintenance.
Scenario 2 for UCA-7: Maintenance of the equipment and instrument is required, but maintenance team do not provide the required repair and maintenance because of backlog due to inadequate maintenance planning resulted from lack of competency of maintenance team or not enough workers in the maintenance team [UCA-7]. As a result, hydrocarbon may be released from the process [H1, H2]	Design and implement a competency assurance system for maintenance team. Review the maintenance workload and maintenance team dimension and ensure that there are enough workers in the maintenance team for the assigned tasks.
Scenario 1 for UCA-8: Maintenance of the equipment and instrument is required, but maintenance team provide the required repair and maintenance too late because of lack of spares and tools in the warehouse [UCA-8]. As a	Design and implement a maintenance management system to ensure adequate maintenance including not facing with lack of required spares and tools for maintenance.

result, hydrocarbon may be released from the process [H1, H2]	
Scenario 2 for UCA-8: Maintenance of the equipment and instrument is required, but maintenance team provide the required repair and maintenance too late because of backlog due to inadequate maintenance planning resulted from lack of competency of maintenance team or not enough workers in the maintenance team [UCA-8]. As a result, hydrocarbon may be released from the process [H1, H2]	Design and implement a competency assurance system for maintenance team. Review the maintenance workload and maintenance team dimension and ensure that there are enough workers in the maintenance team for the assigned tasks.
Scenario 1 of CA-1: Automated process control command is provided, but the process control function is not executed properly due to actuator failure. As a result, hydrocarbon may be released from the process [H1,H2]	Test and maintain control system's actuators adequately. (Prepare a manual for testing and maintenance of control system's actuators, and ensure that maintenance team is competent and act according to this manual. Design and implement a competency assurance system for maintenance team).
Scenario 2 of CA-1: Controlled process is not out of normal condition, but automated process control functions improperly due to faulty detections. As a result, hydrocarbon may be released from the process [H1,H2]	Test and maintain process parameter sensors adequately. (Prepare a manual for testing and maintenance of process parameter sensors, and ensure that maintenance team is competent and act according to this manual. Design and implement a competency assurance system for maintenance team).
Scenario 1 of CA-3: Operator provides manual process control, but it is not executed because of actuator failure due to lack of adequate inspection and maintenance of actuator. As a result, hydrocarbon may be released from the process [H1,H2]	Test and maintain control system's actuators adequately. (Prepare a manual for testing and maintenance of control system's actuators, and ensure that maintenance team is competent and act according to this manual. Design and implement a competency assurance system for maintenance team).
Scenario 2 of CA-3: Operator provides manual control improperly when it is not required due to lack of competency. As a result, hydrocarbon may be released from the process [H1,H2]	Ensure operators are competent in operating the plant. Design and implement a competency assurance system for operators.
Scenario 1 for CA-4: Repair and maintenance of the equipment and instrument is not executed properly due to: - lack of competency of maintenance team, - inadequate spares and tools, or - lack of proper supervision on maintenance works. As a result, hydrocarbon may be released from the process [H1, H2]	Ensure maintenance team is competent in maintaining the equipment and instrument. Design and implement a competency assurance system for maintenance team. Design and implement a maintenance management system to ensure adequate maintenance including not facing with lack of required spares and tools for maintenance. Properly supervise maintenance works.

Considering the high level control structure of the gas plant (Figure 54), these safety measures (Table 9) are recommended. A summary of these safety measures is provided in Table 10.

Table 10 STPA recommendations using general control structure

	Recommendations
1	Ensure that for each abnormal condition an appropriate function is defined in the process control system. And ensure that final elements are designed correctly as required by defined functions.
2	Ensure that right sensor is selected for each process parameter and it will be capable to detect the abnormal conditions. Verify that the set point of process parameter sensors are established correctly.
3	Test, maintain and calibrate process control elements (sensor/initiator, logic solver and actuator/final element) adequately. Prepare a manual for testing, maintenance and calibration of process control elements and ensure that it is included in the competency program of maintenance team.
4	Carry out an alarm management to ensure that operators are not overwhelmed with the process requirements.
5	Design and implement a maintenance management system to ensure adequate maintenance including not facing with lack of required spares and tools for maintenance.
6	Review the maintenance workload and maintenance team dimension and ensure that there are enough workers in the maintenance team for the assigned tasks.
7	Ensure maintenance team is competent in maintaining the equipment and instrument. Design and implement a competency assurance system for maintenance team. Properly supervise maintenance works.
8	Design and implement a competency assurance system for maintenance team.

In order to have more detailed safety measures it is necessary to develop a refined control structure. For this, a section of the gas plant (air cooler and separator) is selected and control structure is prepared (Figure 55)

Figure 55 Detailed Safety Control Structure for air cooler and separator

STPA is applied to this refined safety control structure. Consequently, refined control actions are analyzed to identify UCAs (Table 11).

Table 11 Identified Unsafe Control Actions from the refined control structure

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
BPC Opens Produced water valve	BPC does not provide Open valve function when water level is high in the separator, causing water enter to the condensate stream. N/A	UCA-1: BPC provide Open produced water valve function when water level is low, causing hydrocarbon enter to the water stream and potentially release from the process [H1, H2]		UCA-2: BPC maintain Open produced water valve function for too long causing hydrocarbon enter to the water stream and potentially release from the process [H1, H2]
BPC Closes Produced water valve	UCA-3: BPC does not provide Close produced water valve function when water level is low, causing hydrocarbon enter to the water stream and potentially release	BPC provide Close valve function when water level is high in the separator, causing water enter to the condensate stream. N/A	UCA-4: BPC provides Close produced water valve function too late while water level is low, causing hydrocarbon enter	

	from the process [H1, H2]		to the water stream and potentially release from the process [H1, H2]	
BPC Opens condensate valve	UCA-5: BPC does not provide Open valve function when condensate level is high in the separator, causing high pressure in the separator and condensate enter to gas stream. [H1, H2]	UCA-6: BPC provide Open valve function when condensate level is low in the separator, causing gas enter to condensate stream. [H1, H2]	UCA-7: BPC provide Open valve function too late when condensate level is high in the separator, causing high pressure in the separator and condensate enter to gas stream. [H1, H2]	
BPC Closes condensate valve	UCA-8: BPC does not provide Close valve function when condensate level is low, causing gas enter to condensate stream (blow by) and potentially release from the process [H1, H2]	UCA-9: BPC provide Close valve function when condensate level is high in the separator, causing high pressure in the separator and condensate enter to gas stream. [H1, H2]	UCA-10: BPC provides Close valve function too late while condensate level is low, causing gas enter to the condensate stream (blow by) and potentially release from the process [H1, H2]	
BPC Increases fan speed	N/A	BPC does not provide increase fan speed when the fluid temperature is high causing difficulties for separation. N/A	N/A	N/A
BPC Decrease fan speed	BPC provide decrease fan speed when the fluid temperature is high causing difficulties for separation. N/A	N/A	N/A	N/A
Operators Disable BPC		UCA-11: Operators disables BPC when BPC is required to maintain the process within the normal conditions [H1, H2]		
Operators respond to alarms	UCA-12: Operators do not provide response to alarms when process is out of normal conditions [H1, H2]		UCA-13: Operators provide response to alarms too late when process is out of	

			normal conditions [H1, H2]	
Operators operate valves	UCA-14: Operators do not operate valves when BPC is disabled and manual process control is required [H1, H2]	UCA-15: Operators operates valves when it is not required causing process parameters out of safe envelope [H1, H2]	UCA-16: Operators operate valves too late when BPC is disabled and manual process control is required [H1, H2]	
Operators change fan speed	Operators do not change fan speed when BPC is disabled and manual process control is required causing high fluid temperature and difficulties for separation. N/A	Operators change fan speed when manual process control (intervention by operator) is not required causing high fluid temperature and difficulties for separation. N/A		
Operators modify set points	N/A	Operators modify set points		

After identification of UCAs, constraints on the behavior of each controller are defined (Table 12):

Table 12 Controller constraints of the UCAs for air cooler and separator

Unsafe Control Actions	Controller Constraints
UCA-1: BPC provide Open produced water valve function when water level is low, causing hydrocarbon enter to the water stream and potentially release from the process [H1, H2]	C-1: BPC must not provide Open produced water valve function when water level is low, causing hydrocarbon enter to the water stream and potentially release from the process.
UCA-2: BPC maintain Open produced water valve function for too long causing hydrocarbon enter to the water stream and potentially release from the process [H1, H2]	C-2: BPC must not maintain Open produced water Valve function for too long, causing hydrocarbon enter to the water stream and potentially release from the process.
UCA-3: BPC does not provide Close produced water valve function when water level is low, causing hydrocarbon enter to the water stream and potentially release from the process [H1, H2]	C-3: BPC must provide Close valve function when water level is low, causing hydrocarbon enter to the water stream and potentially release from the process
UCA-4: BPC provides Close produced water valve function too late while water level is low, causing hydrocarbon enter to the water stream and potentially release from the process [H1, H2]	C-4: BPC must not provide Close valve function too late while water level is low, causing hydrocarbon enter to the water stream and potentially release from the process
UCA-5: BPC does not provide Open valve function when condensate level is high in the separator, causing high pressure in the separator and condensate enter to gas stream. [H1, H2]	C-5: BPC must provide Open valve function when condensate level is high in the separator, causing high pressure in the separator and condensate enter to gas stream.

UCA-6: BPC provide Open valve function when condensate level is low in the separator, causing gas enter to condensate stream. [H1, H2]	C-6: BPC must not provide Open valve function when condensate level is low in the separator, causing gas enter to condensate stream
UCA-7: BPC provide Open valve function too late when condensate level is high in the separator, causing high pressure in the separator and condensate enter to gas stream. [H1, H2]	C-7: BPC must not provide Open valve function too late when condensate level is high in the separator, causing high pressure in the separator and condensate enter to gas stream.
UCA-8: BPC does not provide Close valve function when condensate level is low, causing gas enter to condensate stream (blow by) and potentially release from the process [H1, H2]	C-8: BPC must provide Close valve function when condensate level is low, causing gas enter to condensate stream (blow by) and potentially release from the process
UCA-9: BPC provide Close valve function when condensate level is high in the separator, causing high pressure in the separator and condensate enter to gas stream. [H1, H2]	C-9: BPC must not provide Close valve function when condensate level is high in the separator, causing high pressure in the separator and condensate enter to gas stream.
UCA-10: BPC provides Close valve function too late while condensate level is low, causing gas enter to the condensate stream (blow by) and potentially release from the process [H1, H2]	C-10: BPC must not provide Close valve function too late while condensate level is low, causing gas enter to the condensate stream (blow by) and potentially release from the process
UCA-11: Operators disables BPC when BPC is required to maintain the process within the normal conditions [H1, H2]	C-11: Operators must not disables BPC when BPC is required to maintain the process within the normal conditions
UCA-12: Operators do not provide response to alarms when process is out of normal conditions [H1, H2]	C-12: Operators must provide response to alarms when process is out of normal conditions [H1, H2]
UCA-13: Operators provide response to alarms too late when process is out of normal conditions [H1, H2]	C-13: Operators must not provide response to alarms too late when process is out of normal conditions
UCA-14: Operators do not operate valves when BPC is disabled and manual process control is required [H1, H2]	C-14: Operators must operate valves when BPC is disabled and manual process control is required
UCA-15: Operators operates valves when it is not required causing process parameters out of safe envelope [H1, H2]	C-15: Operators must not operates valves when it is not required causing process parameters out of safe envelope
UCA-16: Operators operate valves too late when BPC is disabled and manual process control is required [H1, H2]	C-16: Operators must not operate valves too late when BPC is disabled and manual process control is required

Then, considering unsafe control actions, loss scenarios are identified in Table 13.

Table 13 Loss Scenarios of the UCAs for air cooler and separator

Unsafe Control Actions	Loss Scenarios
UCA-1: BPC provide Open produced water valve function when water level is low, causing hydrocarbon enter to the water stream and potentially release from the process [H1, H2]	Scenario 1 for UCA-1: Water level is low but BPC considers it as high enough to open the produced water valve [UCA-1]. This happens because of wrong set point of water level sensor, due to design or modifications during operation.

	It causes hydrocarbon enter to the water stream and potentially release from the process [H1, H2]
UCA-2: BPC maintain Open produced water valve function for too long causing hydrocarbon enter to the water stream and potentially release from the process [H1, H2]	Scenario 1 for UCA-2: Water level is low but BPC does not detect it correctly and maintain the produced water valve open for a while [UCA-2]. This happens because of wrong set point of water level sensor, due to design or modifications during operation. It causes hydrocarbon enter to the water stream and potentially release from the process [H1, H2]
UCA-3: BPC does not provide Close produced water valve function when water level is low, causing hydrocarbon enter to the water stream and potentially release from the process [H1, H2]	Scenario 1 for UCA-3: Water level is low but BPC does not detect it because of wrong set point of water level sensor, due to design or modifications during operation, and consequently does not close the produced water valve [UCA-3]. It causes hydrocarbon enter to the water stream and potentially release from the process [H1, H2] Scenario 2 for UCA-3: Water level is low but BPC does not detect it because of failed or not correctly calibrated water level sensor, due to lack of proper maintenance and calibration. Consequently, BPC does not close the produced water valve [UCA-3]. It causes hydrocarbon enter to the water stream and potentially release from the process [H1, H2] Scenario 3 for UCA-3: Water level is low and BPC detects it and send the command to close the produced water valve. The valve does not function correctly due to lack of proper maintenance [UCA-3]. It causes hydrocarbon enter to the water stream and potentially release from the process [H1, H2]
UCA-4: BPC provides Close produced water valve function too late while water level is low, causing hydrocarbon enter to the water stream and potentially release from the process [H1, H2]	Scenario 1 for UCA-4: Water level is low but BPC detects it too late because of wrong set point of water level sensor, due to design or modifications during operation, and consequently close the produced water valve too late [UCA-4]. It causes hydrocarbon enter to the water stream and potentially release from the process [H1, H2] Scenario 2 for UCA-4: Water level is low but BPC detect it too late because of not correctly calibrated water level sensor, due to lack of proper calibration. Consequently, BPC close the produced water valve too late [UCA-4]. It causes hydrocarbon enter to the water stream and potentially release from the process [H1, H2]

	Scenario 3 for UCA-4: Produced water valve functions too late when water level is low [UCA-4] because the valve closing time is too high. It causes hydrocarbon enter to the water stream and potentially release from the process [H1, H2]
UCA-5: BPC does not provide Open valve function when condensate level is high in the separator, causing high pressure in the separator and condensate enter to gas stream. [H1, H2]	Scenario 1 for UCA-5: Condensate level is high but BPC does not detect it because of wrong set point of condensate level sensor, due to design or modifications during operation, and consequently does not open the condensate valve [UCA-5]. It causes high pressure in the separator and condensate entering to gas stream and potentially release from the process [H1, H2] Scenario 2 for UCA-5: Condensate level is high but BPC does not detect it because of failed or not correctly calibrated condensate level sensor, due to lack of proper maintenance and calibration. Consequently, BPC does not open the condensate valve [UCA-5]. It causes high pressure in the separator and condensate entering to gas stream and potentially release from the process [H1, H2] Scenario 3 for UCA-5: Condensate level is high and BPC detects it and send the command to open the condensate valve. The valve does not function correctly due to lack of proper maintenance [UCA-5]. It causes high pressure in the separator and condensate entering to gas stream and potentially release from the process [H1, H2]
UCA-6: BPC provide Open valve function when condensate level is low in the separator, causing gas enter to condensate stream. [H1, H2]	Scenario 1 for UCA-6: BPC function to operate condensate valve is not correct and opens the condensate valve when condensate level is low in the separator due to wrong definition in design or modification during operation [UCA-6]. It causes gas enter to the condensate stream and potentially release from the process [H1, H2] Scenario 2 for UCA-6: Condensate level is low but BPC considers it as high because of wrong set point, failure or lack of calibration of condensate level sensor. This could happen due to wrong design or erroneous modifications during operation, or lack of proper maintenance and calibration of condensate sensor and consequently open the condensate valve [UCA-6]. It causes gas enter to the condensate stream and potentially release from the process [H1, H2]

UCA-7: BPC provide Open valve function too late when condensate level is high in the separator, causing high pressure in the separator and condensate enter to gas stream. [H1, H2]	Scenario 1 for UCA-7: Condensate level is high but BPC detects it too late because of wrong set point of condensate level sensor, due to design or modifications during operation, and consequently open the condensate valve too late [UCA-7]. It causes high pressure in the separator and condensate enter to gas stream. [H1, H2] Scenario 2 for UCA-7: Condensate level is high but BPC detect it too late because of not correctly calibrated condensate level sensor, due to lack of proper calibration. Consequently, BPC open the condensate valve too late [UCA-7]. It causes high pressure in the separator and condensate enter to gas stream. [H1, H2] Scenario 3 for UCA-7: Condensate valve functions too late when condensate level is high [UCA-7] because the valve opening time is too high. It causes high pressure in the separator and condensate enter to gas stream. [H1, H2]
UCA-8: BPC does not provide Close valve function when condensate level is low, causing gas enter to condensate stream (blow by) and potentially release from the process [H1, H2]	Scenario 1 for UCA-8: Condensate level is low but BPC does not detect it because of wrong set point of condensate level sensor, due to design or modifications during operation, and consequently does not open the condensate valve [UCA-8]. It causes gas enter to condensate stream (blow by) and potentially release from the process [H1, H2] Scenario 2 for UCA-8: Condensate level is low but BPC does not detect it because of failed or not correctly calibrated condensate level sensor, due to lack of proper maintenance and calibration. Consequently, BPC does not close the condensate valve [UCA-8]. It causes gas enter to condensate stream (blow by) and potentially release from the process [H1, H2] Scenario 3 for UCA-8: Condensate level is low and BPC detects it and send the command to close the condensate valve. The valve does not function correctly due to lack of proper maintenance [UCA-8]. It causes gas enter to condensate stream (blow by) and potentially release from the process [H1, H2]
UCA-9: BPC provide Close valve function when condensate level is high in the separator, causing high pressure in the separator and condensate enter to gas stream. [H1, H2]	Scenario 1 for UCA-9: BPC function to operate condensate valve is not correct and closes the condensate valve when condensate level is high in the separator due to wrong definition in design or modification during operation [UCA-9]. It causes high pressure in the separator and condensate enter to gas stream. [H1, H2]

	Scenario 2 for UCA-9: Condensate level is high but BPC considers it as low because of wrong set point, failure or lack of calibration of condensate level sensor. This could happen due to wrong design or erroneous modifications during operation, or lack of proper maintenance and calibration of condensate sensor and consequently closes the condensate valve [UCA-9]. It causes high pressure in the separator and condensate enter to gas stream. [H1, H2]
UCA-10: BPC provides Close valve function too late while condensate level is low, causing gas enter to the condensate stream (blow by) and potentially release from the process [H1, H2]	Scenario 1 for UCA-10: Condensate level is low but BPC detects it too late because of wrong set point of condensate level sensor, due to design or modifications during operation, and consequently closes the condensate valve too late [UCA-10]. It causes gas enter to condensate stream (blow by) and potentially release from the process [H1, H2] Scenario 2 for UCA-10: Condensate level is low but BPC detect it too late because of not correctly calibrated condensate level sensor, due to lack of proper calibration. Consequently, BPC closes the condensate valve too late [UCA-10]. It causes gas enter to condensate stream (blow by) and potentially release from the process [H1, H2] Scenario 3 for UCA-10: Condensate valve functions too late when condensate level is low [UCA-10] because the valve closing time is too high. It causes gas enter to condensate stream (blow by) and potentially release from the process [H1, H2]
UCA-11: Operators disable BPC when BPC is required to maintain the process within the normal conditions [H1, H2]	Scenario 1 for UCA-11: BPC is required to maintain the process within the normal conditions, but operators disable the BPC due to faulty alarms because of lack of maintenance/calibration of alarms [UCA-11]. It causes process parameters out of the normal conditions and potentially hydrocarbon release from the process [H1, H2] Scenario 2 for UCA-11: BPC is required to maintain the process within the normal conditions, but operators disable the BPC due to its malfunctioning because of lack of maintenance/calibration of initiator, logic solver or final elements [UCA-11]. It causes process parameters out of the normal conditions and potentially hydrocarbon release from the process [H1, H2]

	Scenario 3 for UCA-11: BPC is required to maintain the process within the normal conditions, but operators disable the BPC by error or due to lack of competency [UCA-11]. It causes process parameters out of the normal conditions and potentially hydrocarbon release from the process [H1, H2]
UCA-12: Operators do not provide response to alarms when process is out of normal conditions [H1, H2]	Scenario 1 for UCA-12: Operators do not provide response to alarms when process is out of normal conditions because they are overwhelmed with the process requirements due to not having adequate alarm management [UCA-12]. As result, it creates a hazardous situation and potentially hydrocarbon release from the process [H1, H2] Scenario 2 for UCA-12: Operators do not provide response to alarms when process is out of normal conditions because of repetitive faulty alarms due to lack of maintenance/calibration of alarms [UCA-12]. As result, it can create a hazardous situation and potentially hydrocarbon release from the process [H1, H2] Scenario 3 for UCA-12: Operators do not provide response to alarms when process is out of normal conditions due to lack of competency [UCA-12]. As result, it can create a hazardous situation and potentially hydrocarbon release from the process [H1, H2]
UCA-13: Operators provide response to alarms too late when process is out of normal conditions [H1, H2]	Scenario 1 for UCA-13: Operators provide response to alarms too late when process is out of normal conditions because they are overwhelmed with the process requirements due to not having adequate alarm management [UCA-13]. As result, it may create a hazardous situation and potentially hydrocarbon release from the process [H1, H2]
UCA-14: Operators do not operate valves when BPC is disabled and manual process control is required [H1, H2]	Scenario 1 for UCA-14: BPC is disabled and manual process control is required, but operators do not operate valves because they are overwhelmed with the process requirements due to not adequate alarm management [UCA-14]. As result, it may create a hazardous situation and potentially hydrocarbon release from the process [H1, H2] Scenario 2 for UCA-14: BPC is disabled and manual process control is required, but operators do not operate valves or operate wrong valves due to lack of competency or awareness [UCA-14]. As result, it may create a hazardous situation and potentially hydrocarbon release from the process [H1, H2]

UCA-15: Operators operates valves when it is not required causing process parameters out of safe envelope [H1, H2]	Scenario 1 for UCA-15: Operators manipulate valves by error or because of lack of competency when it is not required [UCA-15]. It causes process parameters out of the normal conditions and potentially hydrocarbon release from the process [H1, H2]
UCA-16: Operators operate valves too late when BPC is disabled and manual process control is required [H1, H2]	Scenario 1 for UCA-16: BPC is disabled and manual process control is required, but operators provide intervention too late because they are overwhelmed with the process requirements due to not adequate alarm management [UCA-16]. As a result, hydrocarbon may be released from the process [H1, H2]

At the end new safety measures have to be defined to prevent loss scenarios being converted to hazards. List of safety measures corresponding to loss scenarios is provided in Table 14.

Table 14 Safety measures recommended by STPA for the detailed control structure

Loss scenarios	Safety Measures
Scenario 1 for UCA-1: Water level is low but BPC considers it as high enough to open the produced water valve [UCA-1]. This happens because of wrong set point of water level sensor, due to design or modifications during operation. It causes hydrocarbon enter to the water stream and potentially release from the process [H1, H2]	Verify that water level sensor set point is established correctly in the design. Develop a formal process including required approvals for modification of water level sensor set point during operation. Include Low Low Level Alarm for water level, and also Safety Instrumented System (SIS) to shut down the process on water Low Low Level and isolate the process. Include manual shut down system to be used by operator on water Low Low Level in case SIS does not function. In case of possible spills, include secondary containment and drain system.
Scenario 1 for UCA-2: Water level is low but BPC does not detect it correctly and maintain the produced water valve open for a while [UCA-2]. This happens because of wrong set point of water level sensor, due to design or modifications during operation. It causes hydrocarbon enter to the water stream and potentially release from the process [H1, H2]	Same as safety measures defined for Scenario 1 for UCA-1
Scenario 1 for UCA-3: Water level is low but BPC does not detect it because of wrong set point of water level sensor, due to design or modifications during operation, and consequently does not close the produced water valve [UCA-3]. It causes hydrocarbon enter to	Same as safety measures defined for Scenario 1 for UCA-1.

the water stream and potentially release from the process [H1, H2]	
Scenario 2 for UCA-3: Water level is low but BPC does not detect it because of failed or not correctly calibrated water level sensor, due to lack of proper maintenance and calibration. Consequently, BPC does not close the produced water valve [UCA-3]. It causes hydrocarbon enter to the water stream and potentially release from the process [H1, H2]	Define and implement proper maintenance (preventive and corrective) for water level sensor to prevent failure. Define and implement adequate calibration program for water level sensor to ensure correct detection. Plus mitigation measures defined in Scenario 1 for UCA-1.
Scenario 3 for UCA-3: Water level is low and BPC detects it and send the command to close the produced water valve. The valve does not function correctly due to lack of proper maintenance [UCA-3]. It causes hydrocarbon enter to the water stream and potentially release from the process [H1, H2]	Same as safety measures defined for Scenario 1 for UCA-1.
Scenario 1 for UCA-4: Water level is low but BPC detects it too late because of wrong set point of water level sensor, due to design or modifications during operation, and consequently close the produced water valve too late [UCA-4]. It causes hydrocarbon enter to the water stream and potentially release from the process [H1, H2]	Same as safety measures defined for Scenario 1 for UCA-1.
Scenario 2 for UCA-4: Water level is low but BPC detect it too late because of not correctly calibrated water level sensor, due to lack of proper calibration. Consequently, BPC close the produced water valve too late [UCA-4]. It causes hydrocarbon enter to the water stream and potentially release from the process [H1, H2]	Same as safety measures defined Scenario 2 for UCA-3.
Scenario 3 for UCA-4: Produced water valve functions too late when water level is low [UCA-4] because the valve closing time is too high. It causes hydrocarbon enter to the water stream and potentially release from the process [H1, H2]	Verify that the water valve closing time is short enough to prevent hydrocarbon enter to the water stream when water level is low and water valve needs to function (prevents scenario 3 for UCA-4 to happen). Plus mitigation measures defined in Scenario 1 for UCA-1.
Scenario 1 for UCA-5: Condensate level is high but BPC does not detect it because of wrong set point of condensate level sensor, due to design or modifications during operation, and consequently does not open the condensate valve [UCA-5]. It causes high pressure in the separator and condensate entering to gas stream and potentially release from the process [H1, H2]	Verify that condensate level sensor set point is established correctly in the design. Develop a formal process including required approvals for modification of condensate level sensor set point during operation. Include High High Level Alarm for condensate level, and also Safety Instrumented System (SIS) to shut down the process separator on condensate High High level and isolate the process. Include manual shut down system to be used by operator on condensate High High level in case SIS does not function.

	Include PSV with set point below pressure design to protect the separator from being over pressurized and send the gas to flare system. In case of possible spills, include secondary containment and drain system.
Scenario 2 for UCA-5: Condensate level is high but BPC does not detect it because of failed or not correctly calibrated condensate level sensor, due to lack of proper maintenance and calibration. Consequently, BPC does not open the condensate valve [UCA-5]. It causes high pressure in the separator and condensate entering to gas stream and potentially release from the process [H1, H2]	Define and implement proper maintenance (preventive and corrective) for condensate level sensor to prevent failure. Define and implement adequate calibration program for condensate level sensor to ensure correct detection. Plus mitigation measures defined in Scenario 1 for UCA-5.
Scenario 3 for UCA-5: Condensate level is high and BPC detects it and send the command to open the condensate valve. The valve does not function correctly due to lack of proper maintenance [UCA-5]. It causes high pressure in the separator and condensate entering to gas stream and potentially release from the process [H1, H2]	Define and implement proper maintenance (preventive and corrective) for condensate valve to ensure it function correctly. Plus mitigation measures defined in Scenario 1 for UCA-5.
Scenario 1 for UCA-6: BPC function to operate condensate valve is not correct and opens the condensate valve when condensate level is low in the separator due to wrong definition in design or modification during operation [UCA-6]. It causes gas enter to the condensate stream and potentially release from the process [H1, H2]	Verify that condensate valve function is defined correctly in the design, i.e. does not open when condensate level is low in the separator. Include Low Low Level Alarm for condensate level, and also Safety Instrumented System (SIS) to shut down the process on condensate Low Low Level. Include manual shut down system to be used by operator on condensate Low Low Level in case SIS does not function.
Scenario 2 for UCA-6: Condensate level is low but BPC considers it as high because of wrong set point, failure or lack of calibration of condensate level sensor. This could happen due to wrong design or erroneous modifications during operation, or lack of proper maintenance and calibration of condensate sensor and consequently open the condensate valve [UCA-6]. It causes gas enter to the condensate stream and potentially release from the process [H1, H2]	Verify that condensate level sensor set point is established correctly in the design. Develop a formal process including required approvals for modification of condensate level sensor set point during operation. Define and implement proper maintenance (preventive and corrective) for condensate level sensor to prevent failure. Define and implement adequate calibration program for condensate level sensor to ensure correct detection. Plus mitigation measures defined in Scenario 1 for UCA-6.
Scenario 1 for UCA-7: Condensate level is high but BPC detects it too late because of wrong set point of condensate level sensor, due to design or modifications during operation, and consequently open the condensate valve too late	Same as safety measures defined for scenario 1 for UCA-5.

[UCA-7]. It causes high pressure in the separator and condensate enter to gas stream. [H1, H2]	
Scenario 2 for UCA-7: Condensate level is high but BPC detect it too late because of not correctly calibrated condensate level sensor, due to lack of proper calibration. Consequently, BPC open the condensate valve too late [UCA-7]. It causes high pressure in the separator and condensate enter to gas stream. [H1, H2]	Define and implement adequate calibration program for condensate level sensor to ensure correct detection. Plus mitigation measures defined in Scenario 1 for UCA-5.
Scenario 3 for UCA-7: Condensate valve functions too late when condensate level is high [UCA-7] because the valve opening time is too high. It causes high pressure in the separator and condensate enter to gas stream. [H1, H2]	Verify that the condensate valve opening time is short enough to prevent condensate enter to the gas stream and high pressure in separator (prevents scenario 3 for UCA-7 to happen). Plus mitigation measures defined in Scenario 1 for UCA-5.
Scenario 1 for UCA-8: Condensate level is low but BPC does not detect it because of wrong set point of condensate level sensor, due to design or modifications during operation, and consequently does not open the condensate valve [UCA-8]. It causes gas enter to condensate stream (blow by) and potentially release from the process [H1, H2]	Verify that condensate level sensor set point is established correctly in the design. Develop a formal process including required approvals for modification of condensate level sensor set point during operation. Include Low Low Level Alarm for condensate level, and also Safety Instrumented System (SIS) to shut down the process separator on condensate Low Low level and isolate the process. Include manual shut down system to be used by operator on condensate Low Low level in case SIS does not function. In case of possible spills, include secondary containment and drain system.
Scenario 2 for UCA-8: Condensate level is low but BPC does not detect it because of failed or not correctly calibrated condensate level sensor, due to lack of proper maintenance and calibration. Consequently, BPC does not close the condensate valve [UCA-8]. It causes gas enter to condensate stream (blow by) and potentially release from the process [H1, H2]	Define and implement proper maintenance (preventive and corrective) for condensate level sensor to prevent failure. Define and implement adequate calibration program for condensate level sensor to ensure correct detection. Plus mitigation measures defined in Scenario 1 for UCA-8
Scenario 3 for UCA-8: Condensate level is low and BPC detects it and send the command to close the condensate valve. The valve does not function correctly due to lack of proper maintenance [UCA-8]. It causes gas enter to condensate stream (blow by) and potentially release from the process [H1, H2]	Define and implement proper maintenance (preventive and corrective) for condensate valve to ensure it function correctly. Plus mitigation measures defined in Scenario 1 for UCA-8.
Scenario 1 for UCA-9: BPC function to operate condensate valve is not correct and closes the condensate valve when condensate level is high in the separator due to wrong definition in design or modification during operation [UCA-9]. It causes high pressure in the separator and condensate enter to gas stream. [H1, H2]	Verify that condensate valve function is defined correctly in the design, i.e. does not close when condensate level is high in the separator. Include High High Level Alarm for condensate level, and also Safety Instrumented System (SIS) to shut down the process on condensate High High Level.

	Include PSV with set point below separator's pressure design to protect the separator from being over pressurized and send gas to flare system. Include manual shut down system to be used by operator on condensate High High Level in case SIS does not function.
Scenario 2 for UCA-9: Condensate level is high but BPC considers it as low because of wrong set point, failure or lack of calibration of condensate level sensor. This could happen due to wrong design or erroneous modifications during operation, or lack of proper maintenance and calibration of condensate sensor and consequently closes the condensate valve [UCA-9]. It causes high pressure in the separator and condensate enter to gas stream. [H1, H2]	Verify that condensate level sensor set point is established correctly in the design. Develop a formal process including required approvals for modification of condensate level sensor set point during operation. Define and implement proper maintenance (preventive and corrective) for condensate level sensor to prevent failure. Define and implement adequate calibration program for condensate level sensor to ensure correct detection. Plus mitigation measures defined in Scenario 1 for UCA-9.
Scenario 1 for UCA-10: Condensate level is low but BPC detects it too late because of wrong set point of condensate level sensor, due to design or modifications during operation, and consequently closes the condensate valve too late [UCA-10]. It causes gas enter to condensate stream (blow by) and potentially release from the process [H1, H2]	Verify that condensate level sensor set point is established correctly in the design. Develop a formal process including required approvals for modification of condensate level sensor set point during operation. Include Low Low Level Alarm for condensate level, and also Safety Instrumented System (SIS) to shut down the process separator on condensate Low Low level and isolate the process. Include manual shut down system to be used by operator on condensate Low Low level in case SIS does not function. Verify that process equipment downstream of the condensate valve have adequate pressure rating for possible blow by case. In case of possible spills, include secondary containment and drain system.
Scenario 2 for UCA-10: Condensate level is low but BPC detect it too late because of not correctly calibrated condensate level sensor, due to lack of proper calibration. Consequently, BPC closes the condensate valve too late [UCA-10]. It causes gas enter to condensate stream (blow by) and potentially release from the process [H1, H2]	Define and implement adequate calibration program for condensate level sensor to ensure correct detection. Plus mitigation measures defined in Scenario 1 for UCA-10.
Scenario 3 for UCA-10: Condensate valve functions too late when condensate level is low [UCA-10] because the valve closing time is too high. It causes gas enter to condensate stream (blow by) and potentially release from the process [H1, H2]	Verify that the condensate valve closing time is short enough to prevent gas enter to the condensate stream (blow by), i.e. prevents scenario 3 for UCA-10 to happen.

Scenario 1 for UCA-11: BPC is required to maintain the process within the normal conditions, but operators disable the BPC due to faulty alarms because of lack of maintenance/calibration of alarms [UCA-11]. It causes process parameters out of the normal conditions and potentially hydrocarbon release from the process [H1, H2]	Define and implement proper maintenance (preventive and corrective) for process alarms to prevent faulty alarms. Define and implement adequate calibration program for process sensors to ensure correct detection and prevent faulty alarms.
Scenario 2 for UCA-11: BPC is required to maintain the process within the normal conditions, but operators disable the BPC due to its malfunctioning because of lack of maintenance/calibration of initiator, logic solver or final elements [UCA-11]. It causes process parameters out of the normal conditions and potentially hydrocarbon release from the process [H1, H2]	Define and implement proper maintenance (preventive and corrective) for process alarms, logic solver and final elements to prevent malfunctioning of BPC. Define and implement adequate calibration program for process sensors to ensure correct detection and prevent malfunctioning of BPC.
Scenario 3 for UCA-11: BPC is required to maintain the process within the normal conditions, but operators disable the BPC by error or due to lack of competency [UCA-11]. It causes process parameters out of the normal conditions and potentially hydrocarbon release from the process [H1, H2]	Ensure operators are competent in operating the plant (develop and implement a competency assurance system for operators). Develop and implement procedural control for disabling BPC including required authorization. Develop and implement physical and mental fitness to work program for operators.
Scenario 1 for UCA-12: Operators do not provide response to alarms when process is out of normal conditions because they are overwhelmed with the process requirements due to not having adequate alarm management [UCA-12]. As result, it creates a hazardous situation and potentially hydrocarbon release from the process [H1, H2]	Carry out an alarm management to ensure that operators are not overwhelmed with the process requirements.
Scenario 2 for UCA-12: Operators do not provide response to alarms when process is out of normal conditions because of repetitive faulty alarms due to lack of maintenance/calibration of alarms [UCA-12]. As result, it can create a hazardous situation and potentially hydrocarbon release from the process [H1, H2]	Define and implement proper maintenance (preventive and corrective) for process alarms to prevent faulty alarms. Define and implement adequate calibration program for process sensors to ensure correct detection and prevent faulty alarms.
Scenario 3 for UCA-12: Operators do not provide response to alarms when process is out of normal conditions due to lack of competency [UCA-12]. As result, it can create a hazardous situation and potentially hydrocarbon release from the process [H1, H2]	Ensure operators are competent in operating the plant (develop and implement a competency assurance system for operators).
Scenario 1 for UCA-13: Operators provide response to alarms too late when process is out of normal conditions because they are overwhelmed with the process requirements due to not having adequate alarm management	Carry out an alarm management to ensure that operators are not overwhelmed with the process requirements.

[UCA-13]. As result, it may create a hazardous situation and potentially hydrocarbon release from the process [H1, H2]	
Scenario 1 for UCA-14: BPC is disabled and manual process control is required, but operators do not operate valves because they are overwhelmed with the process requirements due to not adequate alarm management [UCA-14]. As result, it may create a hazardous situation and potentially hydrocarbon release from the process [H1, H2]	Carry out an alarm management to ensure that operators are not overwhelmed with the process requirements.
Scenario 2 for UCA-14: BPC is disabled and manual process control is required, but operators do not operate valves or operate wrong valves due to lack of competency or awareness [UCA-14]. As result, it may create a hazardous situation and potentially hydrocarbon release from the process [H1, H2]	Ensure operators are competent in operating the plant (develop and implement a competency assurance system for operators).
Scenario 1 for UCA-15: Operators manipulate valves by error or because of lack of competency when it is not required [UCA-15]. It causes process parameters out of the normal conditions and potentially hydrocarbon release from the process [H1, H2]	Ensure operators are competent in operating the plant (develop and implement a competency assurance system for operators).
Scenario 1 for UCA-16: BPC is disabled and manual process control is required, but operators provide intervention too late because they are overwhelmed with the process requirements due to not adequate alarm management [UCA-16]. As a result, hydrocarbon may be released from the process [H1, H2]	Carry out an alarm management to ensure that operators are not overwhelmed with the process requirements.

Considering the detailed control structure for air cooler and separator (Figure 55), detailed safety measures are recommended in Table 14. A summary of these safety measures is provided in Table 15.

Table 15 STPA recommendations using refined control structure of air cooler and separator

	Recommendations
1	Verify that set point of water level and condensate level sensors are established correctly in the design.
2	Verify that condensate valve function is defined correctly in the design, i.e. does not close when condensate level is high in the separator or does not open when condensate level is low in the separator.
3	Verify that the condensate valve operating (closing and opening) time is short enough to prevent gas enter to the condensate stream (blow by) and to prevent condensate enter to the gas stream and high pressure in separator
4	Verify that the water valve closing time is short enough to prevent hydrocarbon enter to the water stream when water level is low and water valve needs to function

5	Verify that process equipment downstream of the condensate valve have adequate pressure rating for possible blow by case.
6	Include High High and Low Low alarms for condensate level, and also Safety Instrumented System (SIS) to shut down the process on condensate High High and Low Low levels.
7	Include Low Low alarm for water level, and also Safety Instrumented System (SIS) to shut down the process on water Low Low level and isolate the process.
8	Include manual shut down system to be used by operator on condensate High High, Low Low level and water Low Low level in case SIS does not function.
9	Include PSV with set point below separator's pressure design to protect the separator from being over pressurized and send gas to flare system.
10	Include secondary containment and drain system for possible spills,
11	Carry out an alarm management to ensure that operators are not overwhelmed with the process requirements.
12	Define and implement adequate maintenance (preventive and corrective) and calibration program for process parameter sensors (condensate and water level sensors), logic solver and final elements to ensure correct detection, prevent faulty alarms and prevent malfunctioning of BPC.
13	Define and implement proper maintenance (preventive and corrective) for condensate valve to ensure it functions correctly.
14	Develop a formal process including required approvals for modification of condensate and water level sensors set point during operation.
15	Develop and implement procedural control for disabling BPC including required authorization.
16	Develop and implement physical and mental 'fitness to work' program for operators.
17	Ensure operators are competent in operating the plant (develop and implement a competency assurance system for operators).

After refining the control structure for air cooler and separator, new recommendations are obtained. In some cases, they are more precise and contain more details comparing with the recommendations generated based on generic control structure. For example, before refining the control structure, there is a general recommendation on shut down system. As result of refining the control structure, this recommendation is obtained through three specific and more precise recommendations which clarify the need of shut down for three different scenarios: very low level of water, very low level of condensate and very high pressure.

6.2.5 Discussion and Conclusion

The recommended safety measures generated by application of STPA on general control structure and detailed control structure for air cooler and separator are summarized in Table 16.

Table 16 Recommendations generated by STPA using general control structure and refined control structure of air cooler and separator

	Recommendations
1	Ensure that for each abnormal condition an appropriate function is defined in the process control system. And ensure that final elements are designed correctly as required by defined functions.

2	Ensure that right sensor is selected for each process parameter and it will be capable to detect the abnormal conditions. Verify that the set point of process parameter sensors are established correctly.
3	Test, maintain and calibrate process control elements (sensor/initiator, logic solver and actuator/final element) adequately. Prepare a manual for testing, maintenance and calibration of process control elements and ensure that it is included in the competency program of maintenance team.
4	Carry out an alarm management to ensure that operators are not overwhelmed with the process requirements.
5	Design and implement a maintenance management system to ensure adequate maintenance including not facing with lack of required spares and tools for maintenance.
6	Review the maintenance workload and maintenance team dimension and ensure that there are enough workers in the maintenance team for the assigned tasks.
7	Ensure maintenance team is competent in maintaining the equipment and instrument.
8	Design and implement a competency assurance system for maintenance team.
9	Verify that set point of water level and condensate level sensors are established correctly in the design.
10	Verify that condensate valve function is defined correctly in the design, i.e. does not close when condensate level is high in the separator or does not open when condensate level is low in the separator
11	Verify that the condensate valve operating (closing and opening) time is short enough to prevent gas enter to the condensate stream (blow by) and to prevent condensate enter to the gas stream and high pressure in separator
12	Verify that the water valve closing time is short enough to prevent hydrocarbon enter to the water stream when water level is low and water valve needs to function
13	Verify that process equipment downstream of the condensate valve have adequate pressure rating for possible blow by case
14	Include High High and Low Low alarms for condensate level, and also Safety Instrumented System (SIS) to shut down the process on condensate High High and Low Low levels
15	Include Low Low alarm for water level, and also Safety Instrumented System (SIS) to shut down the process on water Low Low level and isolate the process
16	Include manual shut down system to be used by operator on condensate High High, Low Low level and water Low Low level in case SIS does not function
17	Include PSV with set point below separator's pressure design to protect the separator from being over pressurized and send gas to flare system
18	Include secondary containment and drain system for possible spills
19	Define and implement adequate maintenance (preventive and corrective) and calibration program for process parameter sensors (condensate and water level sensors), logic solver and final elements to ensure correct detection, prevent faulty alarms and prevent malfunctioning of BPC
20	Define and implement proper maintenance (preventive and corrective) for condensate valve to ensure it functions correctly
21	Develop a formal process including required approvals for modification of condensate and water level sensors set point during operation
22	Develop and implement procedural control for disabling BPC including required authorization
23	Develop and implement physical and mental 'fitness to work' program for operators
24	Ensure operators are competent in operating the plant (develop and implement a competency assurance system for operators)

In order to understand differences and similarities between STPA (as a systemic hazard analysis method) and HAZOP (as a traditional method), recommendations obtained in this study as result of the STPA application are compared with the recommendations of the HAZOP study of the plant carried out during the engineering phase. The section of the HAZOP study related to the air cooler and separator is provided in Appendix I. The HAZOP recommendations related to the air cooler and separator are provided in Table 17.

Table 17 Recommendations generated by HAZOP for air cooler and separator

Recommendations
Remove CSC on bypass valve around PSV to consistent with current mode of operations.
Review the requirement for thermal/ fire relief of individual Compressor Cooler Train 1 (20HAL-103A/B/C/D/E/F) or need to CSO the manual isolation valve.
Confirm that the existing PSV on the existing Condensate Stabilizer is sized for failure of 20LV-1705A/B. If not, consider to install RO to ensure gas blowby rate does not exceed PSV capacity.
Provide PG and TG in the Compressor Separator Train 1 (20MBD-103).
Provide personnel protection from hot process fluid upstream of Compressor Cooler Train 1 (20HAL-103A/B/C/D/E/F).
Provide only local start for Compressor Cooler Train 1 (20HAL-103A/B/C/D/E/F) fan to avoid remote start during maintenance.
Consider to install manual valve downstream of 20LV-1705A/B to provide DBB for online removal of valve.
Consider to install manual isolation valve upstream of 23PV-0013 to provide DBB for online removal.
Consider to install manual isolation valve upstream of 23BDV- 0013 to provide DBB for online removal.
Confirm if hydrate formation may occur due to low temperature during recycle during later field life with low suction pressure
Review the requirement for thermal/ fire relief of individual Compressor Coolers or need to CSO the manual isolation valve.

STPA analyzes control actions at all levels of the control structure including physical equipment, while HAZOP is limited to physical equipment and focuses on component failure and deviations from normal operating conditions. Consequently, recommendations generated by STPA and HAZOP have differences and similarities. STPA recommendations are not limited to physical equipment. Recommendations generated by STPA and HAZOP for physical equipment have commonalities but also differences.

Analysis methods based on component failure cannot fully analyze complex systems. The reason is because these methods do not consider the entire system and interactions between components. In that sense, systemic methods are promising and in this study STPA is applied to a process plant.

In the analysis of process plant, system hazards were first identified. Then controllers were evaluated to identify UCAs. The causes of UCAs and improper execution of control actions were determined to define loss scenarios. And finally, recommendations were generated to prevent, control or mitigate loss scenarios.

STPA recommendations were contrasted with recommendations generated by the HAZOP study of the plant. It is observed that they are different. By application of STPA in addition to HAZOP recommendations, additional recommendations can be generated at the entire levels of the complex

socio-technical system. These recommendation cannot replace HAZOP recommendations entirely since HAZOP recommendations are valuable. However, since STPA recommendations are valid and valuable, they will be complementary to HAZOP recommendations and definitely will help to have safer process plants.

A summary of this chapter is published in Journal of Loss Prevention in the Process Industries:
<https://doi.org/10.1016/j.jlp.2019.06.014>

Chapter 7: A methodology to measure safety level in process plants

7.1. Introduction and background

In order to measure the safety level, first it is necessary to have a common understanding of safety. In other words, to have an agreed response for question: What is safety? There are various definition of safety. Below some examples are provided to use as a base for the theory of the methodology.

IEC/ISO defines safety as ‘freedom from unacceptable risk’ (IEC/ISO, 1999). Rasmussen and Svedung in their book on risk management mentioned that ‘it is very often argued that it is difficult to define safety in other terms than by the absence of accidents and that the level of safety attained can only be measured by the number of accidents and incidents’ (Rasmussen & Svedung, 2000). According to Hollnagel, such definitions of safety are indirect rather than direct since safety is defined by what happens when it is absent or missing. Properly speaking, they are therefore definitions of lack of safety (or unsafety) rather than of safety. One consequence of this is that safety management relies on measurements that refer to the absence of safety rather than to the presence of safety. Because the focus is on things that go wrong, there will be something to measure when safety is absent, but paradoxically nothing to measure when safety is present (Hollnagel E. , 2012). This has practical consequences on how safety is measured. It is the reason behind having many safety indicators based on accidents, mishaps or near misses.

In a Handbook published by U.S. DOE on Accident and Operational Safety Analysis it is explained how safety is defined: Karl Weick has noted that safety is a “dynamic nonevent”. James Reason mentions that “safety is noted more in its absence than its presence” (U.S. Department of Energy, 2012).

Hollnagel et al. define safety as Safety-I and Safety-II in FRAM Handbook. Safety I: To most people safety means the absence of unwanted outcomes such as incidents or accidents. Safety is generically defined as the system quality that is necessary and sufficient to ensure that the number of events that can be harmful to workers, the public, or the environment is acceptably low or even zero (Hollnagel, Hounsgaard, & Colligan, 2014). This definition of safety is aligned with the general understanding on safety as absence of accident and freedom from unacceptable risk. Safety-II, as defined by Hollnagel et al., accepts that we cannot understand all of our system, nor understand them entirely. Instead of looking only at adverse events, Safety-II focuses on everyday work and situations where things go right. This shift in focus towards things going right is analogous to the World Health Organisation’s (WHO’s) argument that “health is a state of complete physical, mental, and social well-being and not merely the absence of disease or infirmity”. Safety-II does not define safety as the absence of adverse events, but as the presence of successful everyday functioning (Hollnagel, Hounsgaard, & Colligan, 2014). An important underlying assumption of Safety-I is that we can understand our systems by looking at their components and how these function or malfunction (as failures, errors) (Hollnagel, Hounsgaard, & Colligan, 2014).

According to Leveson, safety is an emergent property of systems that arises from the interaction of system components. Determining whether a plant is acceptably safe, for example, is not possible by examining a single valve in the plant. In fact, statements about

the 'safety of the valve' without information about the context in which that valve is used, are meaningless. Conclusions can be reached, however, about the reliability of the valve, where reliability is defined as the probability that the behavior of the valve will satisfy its specification over time and under given conditions. This is one of the basic distinctions between safety and reliability: Safety can only be determined by the relationship between the valve and the other plant components, that is, in the context of the whole. Therefore, it is not possible to take a single system component in isolation and assess its safety. A component that is perfectly safe in one system may not be when used in another (Leveson N. G., 2012).

Treating safety as an emergent property that arises when the system components interact within a given environment leads to accident models that view accidents as a control problem: accidents occur when component failures, external disturbances, and/or dysfunctional interactions among system components are not adequately handled by the control system. Emergent properties are controlled or enforced by a set of constraints (control laws) related to the behavior of the system components. Accidents result from interactions among components that violate the safety constraints, in other words, from a lack of appropriate control actions to enforce the constraints on the interactions (Leveson N. G., 2004).

As mentioned already, the importance of having a good understanding of safety is to define a correct and practical way of measuring safety. If safety is considered as lack of accident, and measurement of safety is that nothing happens, then, how we can understand if systems operate effectively when they produce nothing. In other words, it is a challenge to determine by evidence if the absence of accidents is because of having a safe system or because of having a lucky chance (U.S. Department of Energy, 2012).

Andrew Hopkins mentioned in his book that safety is commonly measured using workforce injury statistics e.g. lost time injuries, recordable injuries, first aids (Hopkins, 2012). Not only measuring safety based on workforce injury statistics has deficiencies in showing the safety status, but also he distinguishes between occupational accidents and process safety or system safety. He argues that a low injury rate is clearly an evidence that occupational hazards are being well managed, but such statistics imply nothing about how well process safety or system hazards are being managed (Hopkins, 2012). Even by recording and keeping the number of process safety incidents in a plant, we cannot have a good measurement of safety status of the plant. Because simply we count the accidents that happened in the past and it has nothing to do with the potentiality that the plant has in term of producing accidents.

Based on Rasmussen and Svedung, the first step toward proactive safety management is to ensure that organizations operate hazardous installations within the approved design envelope and continue to do so under any condition. This ensures that operation is satisfying the precondition for safe operation as defined in the design. This implies that, in the first approximation, safety measurement should involve measuring the margin between the safety design envelope and the actual state of system operation, a solution that is realistic as long as the particular system design has been based on an adequate definition of the boundaries of safe operation (Rasmussen & Svedung, 2000). Although this is not clearly telling us how to measure safety, it is one step toward measuring safety in a way different from counting accident.

According to (Knegtering & Pasman, 2013) safety can only be measured by identifying and quantifying the risks. Risk is usually expressed as the product of consequence of an event and its probability. Consequence in turn depends on effects generated in the event and the possible presence and vulnerability of exposed 'targets'. There are many other parameters, such as changes in activities from normal operation to shutdown, turnaround and startup, repairs, weather conditions, procedural changes, equipment degradation, which have influence on actual risk level. An acceptable safety level is thus not 'guaranteed', because the safety level fluctuates with changing plant activities, conditions, and circumstances (Knegtering & Pasman, 2013). Thus, measuring safety level should consider possible fluctuation caused by different reasons into account to be an acceptable and reliable measurement.

The design of a plant is such that in case of foreseen possible deviations and disturbances from normal safe operation, instrument sensors or human observation should detect something is going 'wrong'. In most cases, alarms become triggered upon which attempts are made to correct the process or there may result in a trip or a shutdown to send the plant to a safe state. However, there are unforeseen deviations, possibly not instrumented ones, unnoticed ones because of operator/supervisor distraction, signs not perceived as an alarm because they are indirectly related to safety, changes observed but not acted upon because of other priorities, and errors or violations, such that the level of safety can deteriorate unnoticed (Knegtering & Pasman, 2013). Consequently, unforeseen deviations have to be included in safety measurement, nevertheless, it introduces a further challenge in measuring safety level.

Different works in academic and industrial environments are done to measure safety. Some notable ones are provided in this section.

Knegtering & Pasman developed a conceptual approach using process parameter signals and signals from various safety indicators to measure safety level of a process plant. Their approach is explained here (Knegtering & Pasman, 2013): The ultimate objective is to measure how safe the process system is at a certain moment in time at a particular place. As such, it is important to know whether a major event is close or remote. Therefore, it would be helpful if likelihood information would be available for the hazardous event to occur within hours, days, weeks, or months. It is about to know how safe it is 'today' so that preventive actions can be taken timely. Fulfillment of this requires continuously receiving, collecting, and interpreting signals and indicator values about the quality of functioning of the components, the risk controls, and fluctuation in density of exposed potential 'targets'. Knegtering & Pasman used bowtie model for this purpose. Risk factors can cause potential threats to components and subsystems on both sides of a bowtie. What is observed and concluded is that signs of certain emerging risk factors e.g., uncommon noise occurring, form evidence of increased risk on the short term and that these factors because of the cause-effect direction in the bowtie are located in the left side close to the Top Event. Enhanced frequency of pressure or temperature levels out of range and/or alarms triggered, form also short-term signs but may be tied to components on larger distance from Top Event. In particular the safety management system KPI's, e.g., maintenance behind schedule, are indicators for risk factors having more remote influence while affecting both sides. In this case, there will be a correlation with the actual safety level. Another example of such a typical safety KPI

concerns the ‘safety culture’ (Knegtering & Pasman, 2013). Figure 56 shows the bowtie model with three areas covering the left side.

Figure 56 Effects of failure in terms of time to a Top Event (Knegtering & Pasman, 2013)

Components could be placed in the bowtie such that the time effect of their failure on the Top Event to occur corresponds with their distance to the Top Event point. The first most left area shows dominance of long term safety indicators, which vary over the years. Long term examples could be, for example, experience change of employees or a changing safety culture. The middle area concerns the midterm dynamic, for instance the effect of seasons, corrosion, and increasing leakages, which could vary from week to week or over months. A failing Distributed Control System (DCS) will have an effect in a matter of hours, while a Safety Instrumented System (SIS) might have to function within seconds. In this way a safety barometer could provide not only information to management about increased risks but also information about the time span after which trouble can be expected. Both types of information together will indicate the actual safety level. The output of such a barometer could be shown on a safety dashboard to reflect the overall situation from moment to moment. The effort to construct a processor to deal with all the signals and to produce a reliable alarm will be not insignificant but worthwhile. The proof of the above theory is not simple, because it needs a well-defined case of a plant installation and real input data of its indicators and probably quite a few iterations over a prolonged time period with an encouraging result, before one can have any trust in a model (Knegtering & Pasman, 2013). The approach developed by Knegtering and Pasman is based on bowtie which in turn is based on Swiss Cheese Model.

Maroño et al. developed a methodology for the evaluation of operational safety in the chemical industry. Their methodology is explained here (Maroño, Pena, & Santamaria, 2006): In the light of the systems theory, a new perspective arises: the improvement of operational safety at the plants can be represented as a cyclic process (Figure 57), where feedback loops provide the means to check the effectiveness of the whole cycle and consequently the validity of the measurement system used. It consists of three main systems: management of information, measurement of safety and implementation of improvements, as depicted in Figure 57.

Figure 57 Operational safety improvement cycle (Maroño, Pena, & Santamaria, 2006)

The system of information management should guarantee the availability and easy retrieval of all the pertinent information, including engineering design data, plant programs, P&IDs, operating procedures, records of incidents/accidents, etc. The safety measurement system should be able to assess the influence of all the safety relevant factors and enable the identification of safety degradation situations at the plants. Finally, the system for implementation of improvements should monitor the corrective actions and new proposals and provide the inputs to the feedback loop that closes the cycle.

The operational safety index ‘PROCESO’ developed by Maroño et al. attempts to provide a new evaluation methodology suitable for self-assessment in chemical and petrochemical plants. The index has been built up using a deductive method and has a tree-like structure. PROCESO takes into account 25 areas in the review of the plant safety, each of them separately quantified by a set of indicators that are used to measure specific aspects of safety. The final value of the index PROCESO is obtained as the sum of the contributions of each individual indicator. The highest attainable value of the index has been set at 100 points, corresponding to the most degraded safety condition. As the value of the index decreases, the level of operational safety increases. The index value is calculated according to the formula provided in Figure 58.

$$IP = \sum_{i=1}^n w_i \sum_{j=1}^{m_i} I_{ij}$$

where

IP is the final index value,

I_{ij} is the value of each individual indicator within area i ,

w_i is the weight of area i ,

n is the total number of index areas (25),

i identifies each area,

j identifies each indicator within area i ,

m_i is the number of indicators in each area (variable depending on each area).

Figure 58 The formula to obtain the 'PROCESO' index value (Maroño, Pena, & Santamaria, 2006)

In their work an attempt has been made to attain independence of indicators by using a deductive model in the first place, and then by establishing the weights of the different safety areas via an expert judgement technique. The procedure followed to develop the new Index 'PROCESO' is schematized in Figure 59.

Figure 59 Procedure followed to develop the 'PROCESO' index (Maroño, Pena, & Santamaria, 2006)

The procedure can be summarized in four main steps:

- Step I definition of structure
- Step II identification and definition of indicators
- Step III allocation of weights to the different index areas

- Step IV validation of index through its application to real plants (case studies)

Although systems theory is mentioned in the explanation of the index developed by Maroño et al., apparently the index is not clearly based on a specific accident model and mainly relies on expert judgment.

In the industrial environment, many works have been done to measure safety. Center for Chemical Process Safety (CCPS, 2007), American Petroleum Institute (API, 2016), International Association of Oil & Gas Producers IOGP (IOGP, 2018), European Chemical Industry Council (CEFIC, 2011), Organization for Economic Cooperation and Development (OECD, 2008) and UK Health and Safety Executive (HSE UK, 2006) amongst others have published procedures and guidelines on process safety indicators. CCPS, API and IOGP assumed a predictive relationship between lower and higher consequence process safety event similar to the one introduced by Heinrich for personal safety events. Heinrich suggested an accident pyramid which represents a predictive relationship between lower and higher consequence personal safety events (Heinrich, 1931). Figure 60 depicts a process safety pyramid with four classifications or tiers based on predictive relationship assumed between lower and higher consequence process safety events.

Figure 60 Process Safety Indicator Pyramid

The tiers of the pyramid represent a continuum of leading and lagging process safety indicators. Tier 1 is the most lagging and Tier 4 is the most leading.

Generally speaking, most of the safety measurements suggested in the industrial environment are mainly based on counting accidents and/or near misses. This is not limited to process safety and includes occupational safety. Regarding process safety, lagging indicators or indicators based on process accidents cannot be helpful in measuring safety because major accidents are rare and occur so infrequently specially at a site level. Therefore, lagging indicators cannot be used to measure safety and may not be useful as early warnings to prevent accidents. There have been some efforts, like the IOGP publication on leading

process safety indicator (IOGP, 2016), that focus on developing indicators that provide feedback before an accident occurs (leading indicators).

Leading indicators are generally intended to help in identifying early signals of deteriorating performance and thereby to provide means for warning of impending problems before an actual accident occurs. Early warnings from these indicators should initiate a further investigation of the causes of the symptoms to ensure that corrective actions will be timely initiated and rightly directed.

In addition to the publications on safety measurement in the industrial environment, there have been some tools developed by companies like e-Vision (e-Vision, 2019), CGE (CGE Risk Management Solutions, 2019), DNV-GL (DNV-GL, 2019) Petrotechnics (Petrotechnics, 2019), RiskPoynt (RiskPoynt, 2019) and Safetec (SAFETEC, 2019) among others to visualize and monitor the safety and status of safety barriers.

However, mentioned publications or tools are not based on any systemic approach on accidents and in some cases they are based on Swiss Cheese Model that is a model based on chain of event. Swiss Cheese Model has some component of systems but it is not considered as a thoroughly systemic model.

As summary, researchers in the academic environment have made some efforts to measure safety and in the industrial environment some works have been done and guides or practices have been published to find a solution for safety measurement. Nevertheless, none of them used systems theories that is the promising solution for sociotechnical complex systems we encounter these days in process plants.

7.2. Theory behind the methodology

In this work, authors tried to find a solution to measure safety level of a process plant using a systemic accident model called STAMP. It means to develop a methodology to enable safety level measurement. Then, by measuring safety level, actions can be taken proactively in order to prevent a gradual movement of the process plant toward an unsafe state.

STPA, that is a hazard analysis technique based on STAMP, is used to develop the methodology to measure safety level. For this, a new concept called 'safety checkpoint' is introduced and included in STPA. A safety checkpoint is a requirement defined to prevent a loss scenario to happen or to satisfy safety measures associated to the loss scenario.

Then, defined safety checkpoints are used to determine the safety level of the process plant. For this, a weighing system is defined for safety checkpoints and a formula is suggested to calculate the safety level using the status of safety checkpoints and their weights.

With this approach the system is studied as a whole and all the loss scenarios are identified. Then, loss scenarios and their associated safety recommendations are monitored via safety checkpoints that literally means measuring safety status of the system as a whole. The proposed methodology is provided below:

Step 1) Define purpose of the analysis

- Identify system boundary
- Identify possible accidents (losses) that may occur in the system

- Identify the hazards in the system
- Identify system-level safety constraints
- Step 2) Model the control structure
  - Draw the control structure for the system under study
  - Create the process model and identify the variables of this model
- Step 3) Identify unsafe control actions
  - Identify control actions
  - Postulate control action behaviors: control action is provided, not provided, provided too early or too late, or stopped too soon
  - Determine if control action behaviors are unsafe for each scenario
  - Define constraints on the behavior of controllers
- Step 4) Identify loss scenarios
  - Identify possible causes of unsafe control actions or improper execution of control actions causing hazards (loss scenarios)
  - Define safety measures to prevent, control or mitigate loss scenarios
  - *Define safety checkpoint(s) for each loss scenario/safety measure. It includes definition of data source for each safety checkpoint, the frequency of obtaining the data and the expected data for each safety checkpoint*
  - *Consolidate defined safety checkpoints (eliminate repetitions and combine related ones) and prepare final list of safety checkpoints. Determine the weighing of each safety checkpoint based on the number of loss scenarios/safety measures related to each safety checkpoint*
  - *Define the indicator, acceptability criteria and levels of safety for each safety checkpoint*
  - *Develop a mechanism to calculate cumulative safety level based on the safety level and weight of each safety checkpoint*

This methodology is a modified STPA. Some new items are introduced to STPA in order to measure safety level. The new items showed above in *Italic*.

After identification of loss scenarios and definition of their safety measures, it is necessary to define safety checkpoints. Safety checkpoints are defined in a way to prevent loss scenarios to happen or to satisfy safety measures associated to loss scenarios. When defining safety checkpoints it is necessary to determine data sources and frequency to obtain data on checkpoints.

Then, it is the time to consolidate defined safety checkpoints. It is done by elimination of repeated safety checkpoints and unification of those safety checkpoints that are combinable. While consolidating safety checkpoints, it is necessary to trace and record the number of loss scenarios controlled by each final safety checkpoint since it will be used later for weighing system of safety checkpoints.

When the list of safety checkpoints is finalized, it is necessary to determine a weight for each safety checkpoint that shows the importance of that safety checkpoint. Weight of each safety checkpoint is shown in percentage that is calculated based on the number of loss scenarios prevented or safety measures satisfied by each safety checkpoint among total number of loss scenarios or safety measures.

For each safety checkpoint, an indicator is defined to indicate the status of that safety checkpoint. When defining the indicator, acceptability criteria of the indicator outcome/value is determined in three level: ‘not acceptable’, ‘partially acceptable’ and ‘acceptable’. For this, acceptable range of each safety checkpoint is obtained from design basis, operation manual or best practices.

Three different safety levels are established for acceptability criteria and a value is assigned to each level for further calculation of cumulative safety level (Equation 1):

Table 18 Safety levels and corresponding values established for acceptability criteria

Acceptability Criteria	Safety Level (Color)	Safety Level (Value)
Not acceptable	Red	0
Partially acceptable	Amber	0,5
Acceptable	Green	1

Cumulative safety level is an approximate level that is calculated based on the value obtained for safety checkpoints and the weight assigned to safety checkpoints. The mechanism or formula developed to calculate cumulative safety level based on the safety level value and weight of each safety checkpoint is provided in Equation 1.

Equation 1 Formula to calculate cumulative safety level based on data of safety checkpoints

$$\text{Cumulative Safety Level} = \sum_{i=0}^n \text{Safety Level determined for Safety Checkpoint (i)} * \text{Weight of the Safety Checkpoint (i)}$$

This methodology is applied on a process plant and outcome is provided in the next section.

7.3. The methodology and its application in a process plant

The proposed methodology, explained in previous section, is applied on the process plant already used as case study for application of STPA. The process description is already provided in section 6.1. Steps 1 to 3 of the proposed methodology are identical to the steps 1 to 3 of STPA that are provided in sections 6.2.1 to 6.2.3. Identified loss scenarios in section 6.2.4 are used to define safety checkpoints. For each loss scenario/safety measure identified for general (high level) control structure safety checkpoints are defined (Table 19). This includes definition of data source for each safety checkpoint, the frequency of obtaining the data and expected data for each safety checkpoint (Table 19)

Table 19 Defined safety checkpoint for loss scenario/safety measure at general control structure level

Loss scenarios	Safety Measures	Safety Checkpoint	Source / Frequency	Expected Data
Scenario 1 for UCA-1: Process is out of normal conditions but automated process control does not detect it	Ensure that right sensor is selected for each process parameter	1. Right sensor is selected for each process parameter.	Design / Once	Right Sensor (Acceptable)

because sensors are not capable to detect the abnormal conditions (not the right sensors selected) [UCA 1]. As a result, hydrocarbon may be released from the process [H1,H2]	that will be capable to detect the abnormal conditions.	2. In case of replacement or repair, right sensor is used for each process parameter (MOC and authorization)	MOC process audit / Annual	MOC audit report with no major finding
Scenario 2 for UCA-1: Process is out of normal conditions but automated process control does not detect it because sensors are faulty due inadequate testing and maintenance [UCA 1]. As a result, hydrocarbon may be released from the process [H1,H2]	Test and maintain process parameter sensors adequately. (Prepare a manual for testing and maintenance of process parameter sensors, and ensure that maintenance team is competent and act according to this manual. Design and implement a competency assurance system for maintenance team).	3. Process parameter sensors maintenance, calibration and test backlog.	Maintenance management system / real time (if not, monthly)	95 % of process parameter sensors without delay in maintenance, calibration and test
		4. Process parameter sensors have maintenance, calibration and test plan	Maintenance and test manual / Once	100 % of process parameter sensors with maintenance, calibration and test plan
		5. Maintenance team members are competent	Human Resources and Competency Management / Annual	100 % of maintenance team members deemed competent
Scenario 3 for UCA-1: Process is out of normal conditions but automated process control does not detect it because set point of sensors were not correctly established in the design [UCA 1]. As a result, hydrocarbon may be released from the process [H1,H2]	Verify that the set point of process parameter sensors are established correctly.	6. Correct set point established for process parameter sensors.	Design / Once	Correct set point for sensors (Acceptable)
Scenario 4 for UCA-1: Process is out of normal conditions but automated process control does not detect it because set point of sensors are modified wrongly in the operation [UCA 1]. As a result, hydrocarbon may be released from the process [H1,H2]	Prepare a manual for modifying process parameter sensors' set point during operation, and ensure that operation team is competent and act according to the manual. Design and implement a competency assurance system for operators.	7. Modification of process parameter sensors' set point is included in the operation manual with adequate authorization.	Operation manual / Once	Included (acceptable)
		8. Process parameter sensors' set point modification audit.	Process parameter sensors' set point modification audit / Annual	Process parameter sensors' set point modification audit report with no major finding
Scenario 5 for UCA-1: Process is out of normal conditions and automated process control detects it but ignores it because it is not defined as	Ensure that appropriate function is defined for each abnormal condition in the	9. All abnormal conditions are identified and correct function is defined for	Design / Once	Abnormal conditions are identified and

abnormal condition in the process model [UCA 1]. As a result, hydrocarbon may be released from the process [H1,H2]	process control system.	each abnormal condition.		correct functions are defined.
Scenario 6 for UCA-1: Process is out of normal conditions and automated process control detects it but does not provide correct BPC function because BPC function is not defined correctly in the process model [UCA 1]. As a result, hydrocarbon may be released from the process [H1,H2]	Ensure that appropriate function is defined for each abnormal condition in the process control system.	Same as 9		
Scenario 7 for UCA-1: Process is out of normal conditions and automated process control detects it but does not provide BPC function because actuators are faulty or incapable to control the process due to inadequate testing and maintenance [UCA 1]. As a result, hydrocarbon may be released from the process [H1,H2]	Test and maintain control system's actuators adequately. (Prepare a manual for testing and maintenance of control system's actuators, and ensure that maintenance team is competent and act according to this manual. Design and implement a competency assurance system for maintenance team).	10. Control system actuators (final elements) maintenance and test backlog	Maintenance management system / real time (if not, monthly)	95 % of Control system actuators (final elements) without delay in maintenance and test
		11. Control system actuators have maintenance and test plan	Maintenance and test manual / Once	100 % of process parameter sensors with maintenance and test plan
		Same as 5		
Scenario 1 for UCA-2: Process is out of normal conditions, but automated process control provided the BPC function too late because feedback about the abnormal conditions is delayed due to sensors maintenance and calibration problems [UCA-2]. As a result, hydrocarbon may be released from the process [H1,H2]	Maintain and calibrate process parameter sensors adequately. (Prepare a manual for testing and maintenance of sensors, and ensure that maintenance team is competent and act according to this manual. Design and implement a competency assurance system for maintenance team).	Same as 3, 4 and 5		
Scenario 2 for UCA-2: Process is out of normal conditions, but automated process control provided the BPC function too late because feedback about the abnormal conditions is delayed due to sensors' wrong set point from design [UCA-2]. As a	Ensure that the set point of process parameter sensors are established correctly.	Same as 6		

result, hydrocarbon may be released from the process [H1,H2]				
Scenario 3 for UCA-2: Process is out of normal conditions, but automated process control provided the BPC function too late because feedback about the abnormal conditions is delayed due to sensors' wrong set point from operation (modifications) [UCA-2]. As a result, hydrocarbon may be released from the process [H1,H2]	Prepare a manual for modifying process parameter sensors' set point during operation, and ensure that operation team is competent and act according to the manual. Design and implement a competency assurance system for operators.	Same as 7 and 8		
		12. Operations team members are competent	Human Resources and Competency Management / Annual	100 % of Operations team members deemed competent
Scenario 4 for UCA-2: Process is out of normal conditions, but automated process control provided the BPC function too late because process model is not correct and wrongly requires late response [UCA-2]. As a result, hydrocarbon may be released from the process [H1,H2]	Ensure that appropriate function is defined for each abnormal condition in the process control system.	Same as 9		
Scenario 5 for UCA-2: Process is out of normal conditions, but automated process control provided the BPC function too late because there is a delay in the final element actuation due to the design of final element [UCA-2]. As a result, hydrocarbon may be released from the process [H1,H2]	Ensure that final elements are designed correctly as required by defined functions.	Same as 10		
Scenario 6 for UCA-2: Process is out of normal conditions, but automated process control provided the BPC function too late because there is a delay in the final element actuation since it is not being maintained and tested adequately [UCA-2]. As a result, hydrocarbon may be released from the process [H1,H2]	Test and maintain control system's actuators adequately. (Prepare a manual for testing and maintenance of control system's actuators, and ensure that maintenance team is competent and act according to this manual. Design and implement a competency assurance system for maintenance team).	Same as 10, 11 and 5		

Scenario 1 for UCA-3: Process is still out of normal conditions, but BPC function stops too soon because the final element fails to continue providing the control action due to not adequate maintenance [UCA-3]. As a result, hydrocarbon may be released from the process [H1,H2]	Test and maintain control system's actuators adequately. (Prepare a manual for testing and maintenance of control system's actuators, and ensure that maintenance team is competent and act according to this manual.	Same as 10, 11 and 5		
Scenario 2 for UCA-3: Process is still out of normal conditions, but operator stops the control action too soon by error due to not having adequate skills and trainings [UCA-3]. As a result, hydrocarbon may be released from the process [H1,H2]	Ensure operators are competent in operating the plant. Design and implement a competency assurance system for operators.	Same as 12		
Scenario 1 for UCA-4: BPC is required to maintain the process within the normal conditions, but operators disable the BPC due to faulty alarms because of lack of maintenance/calibration of alarms [UCA-4]. As a result, hydrocarbon may be released from the process [H1,H2]	Maintain and calibrate process alarms adequately. (Prepare a manual for testing and maintenance of process alarms, and ensure that maintenance team is competent and act according to this manual. Design and implement a competency assurance system for maintenance team).	13. Process alarms maintenance, calibration and test backlog	Maintenance management system / real time (if not, monthly)	95 % of Process alarms without delay in maintenance, calibration and test
		14. Process alarms have maintenance and test plan	Maintenance and test manual / Once	100 % of process alarms with maintenance, calibration and test plan
		Same as 5		
Scenario 2 for UCA-4: BPC is required to maintain the process within the normal conditions, but operators disable the BPC due to its malfunctioning because of lack of maintenance/calibration of initiator, logic solver or final elements [UCA-4]. As a result, hydrocarbon may be released from the process [H1,H2]	Test, maintain and calibrate process control elements (initiator, logic solver and final element) adequately. [Prepare a manual for testing, maintenance and calibration of process control elements (initiator, logic solver and final element), and ensure that maintenance team is competent and act	15. Process control elements (initiator, logic solver and final element) maintenance, calibration and test backlog	Maintenance management system / real time (if not, monthly)	95 % of Process control elements without delay in maintenance, calibration and test
		16. Process control elements (initiator, logic solver and final element) have maintenance, calibration and test plan	Maintenance and test manual / Once	100 % of process control elements (initiator, logic solver and final element) with maintenance, calibration and test plan

	according to this manual. Design and implement a competency assurance system for maintenance team].	Same as 5		
Scenario 1 for UCA-5: Manual process control is required, but operators do not provide intervention because they are overwhelmed with the process requirements due to not adequate alarm management [UCA-5]. As a result, hydrocarbon may be released from the process [H1, H2]	Carry out an alarm management to ensure that operators are not overwhelmed with the process requirements.	17. Number of alarms per operator per hour	BPC / monthly	Acceptable <= 10 alarms / Operator / Hour
Scenario 2 for UCA-5: Manual process control is required, but operators do not provide intervention or provide a wrong function because lack of competency or awareness [UCA-5]. As a result, hydrocarbon may be released from the process [H1, H2]	Ensure operators are competent in operating the plant. Design and implement a competency assurance system for operators.	Same as 12		
Scenario 1 for UCA-6: Manual process control is required, but operators provide intervention too late because they are overwhelmed with the process requirements due to not adequate alarm management [UCA-6]. As a result, hydrocarbon may be released from the process [H1, H2]	Carry out an alarm management to ensure that operators are not overwhelmed with the process requirements.	Same as 17		
Scenario 1 for UCA-7: Maintenance of the equipment and instrument is required, but maintenance team do not provide the required repair and maintenance because of lack of spares and tools [UCA-7]. As a result, hydrocarbon may be released from the process [H1, H2]	Design and implement a maintenance management system to ensure adequate maintenance including not facing with lack of required spares and tools for maintenance.	Same as 16		
Scenario 2 for UCA-7: Maintenance of the equipment and instrument is	Design and implement a competency	Same as 5		

required, but maintenance team do not provide the required repair and maintenance because of backlog due to inadequate maintenance planning resulted from lack of competency of maintenance team or not enough workers in the maintenance team [UCA-7]. As a result, hydrocarbon may be released from the process [H1, H2]	assurance system for maintenance team. Review the maintenance workload and maintenance team dimension and ensure that there are enough workers in the maintenance team for the assigned tasks.	18. Average required time for works assigned to a maintenance team member during a month	Maintenance management system / monthly	Less than 172 hour / month
Scenario 1 for UCA-8: Maintenance of the equipment and instrument is required, but maintenance team provide the required repair and maintenance too late because of lack of spares and tools in the warehouse [UCA-8]. As a result, hydrocarbon may be released from the process [H1, H2]	Design and implement a maintenance management system to ensure adequate maintenance including not facing with lack of required spares and tools for maintenance.	Same as 16		
Scenario 2 for UCA-8: Maintenance of the equipment and instrument is required, but maintenance team provide the required repair and maintenance too late because of backlog due to inadequate maintenance planning resulted from lack of competency of maintenance team or not enough workers in the maintenance team [UCA-8]. As a result, hydrocarbon may be released from the process [H1, H2]	Design and implement a competency assurance system for maintenance team. Review the maintenance workload and maintenance team dimension and ensure that there are enough workers in the maintenance team for the assigned tasks.	Same as 5 and 18		
Scenario 1 of CA-1: Automated process control command is provided, but the process control function is not executed properly due to actuator failure. As a result, hydrocarbon may be released from the process [H1,H2]	Test and maintain control system's actuators adequately. (Prepare a manual for testing and maintenance of control system's actuators, and ensure that maintenance team is competent and act according to this manual. Design and implement a competency assurance system for maintenance team).	Same as 10, 11 and 5		
Scenario 2 of CA-1: Controlled process is not out of normal condition, but automated process	Test and maintain process parameter sensors adequately.	Same as 7, 8 and 5		

control functions improperly due to faulty detections. As a result, hydrocarbon may be released from the process [H1,H2]	(Prepare a manual for testing and maintenance of process parameter sensors, and ensure that maintenance team is competent and act according to this manual. Design and implement a competency assurance system for maintenance team).			
Scenario 1 of CA-3: Operator provides manual process control, but it is not executed because of actuator failure due to lack of adequate inspection and maintenance of actuator. As a result, hydrocarbon may be released from the process [H1,H2]	Test and maintain control system's actuators adequately. (Prepare a manual for testing and maintenance of control system's actuators, and ensure that maintenance team is competent and act according to this manual. Design and implement a competency assurance system for maintenance team).	Same as 10, 11 and 5		
Scenario 2 of CA-3: Operator provides manual control improperly when it is not required due to lack of competency. As a result, hydrocarbon may be released from the process [H1,H2]	Ensure operators are competent in operating the plant. Design and implement a competency assurance system for operators.	Same as 12		
Scenario 1 for CA-4: Repair and maintenance of the equipment and instrument is not executed properly due to: - lack of competency of maintenance team, - inadequate spares and tools, or - lack of proper supervision on maintenance works. As a result, hydrocarbon may be released from the process [H1, H2]	Ensure maintenance team is competent in maintaining the equipment and instrument. Design and implement a competency assurance system for maintenance team. Design and implement a maintenance management system to ensure adequate maintenance including not facing with lack of	Same as 5 and 16		

	required spares and tools for maintenance. Properly supervise maintenance works.			

Similarly, for each loss scenario/safety measure identified for refined control structure safety checkpoints are defined (Table 20). In the same way, it includes definition of data source for each safety checkpoint, the frequency of obtaining the data and expected data for each safety checkpoint (Table 20):

Table 20 Defined safety checkpoint for loss scenario/safety measure at refined control structure level

Loss scenarios	Safety Measures	Safety Checkpoint	Source / Frequency	Expected Data
Scenario 1 for UCA-1: Water level is low but BPC considers it as high enough to open the produced water valve [UCA-1]. This happens because of wrong set point of water level sensor, due to design or modifications during operation. It causes hydrocarbon enter to the water stream and potentially release from the process [H1, H2]	Verify that water level sensor set point is established correctly in the design. Develop a formal process including required approvals for modification of water level sensor set point during operation. Include Low Low Level Alarm for water level, and also Safety Instrumented System (SIS) to shut down the process on water Low Low Level and isolate the process. Include manual shut down system to be used by operator on water Low Low Level in case SIS does not function. In case of possible spills, include secondary containment and drain system.	1. Correct set point is established for water level sensor.	Design / Once	Correct set point (Acceptable)
		2. Set point (water level sensor) modification is done according to a procedure / instruction with required authorizations.	Set point modification audit / Annual	Set point modification audit report with no major finding

Scenario 1 for UCA-2: Water level is low but BPC does not detect it correctly and maintain the produced water valve open for a while [UCA-2]. This happens because of wrong set point of water level sensor, due to design or modifications during operation. It causes hydrocarbon enter to the water stream and potentially release from the process [H1, H2]	Same as safety measures defined for Scenario 1 for UCA-1	Same as 1 and 2		
Scenario 1 for UCA-3: Water level is low but BPC does not detect it because of wrong set point of water level sensor, due to design or modifications during operation, and consequently does not close the produced water valve [UCA-3]. It causes hydrocarbon enter to the water stream and potentially release from the process [H1, H2]	Same as safety measures defined for Scenario 1 for UCA-1.	Same as 1 and 2		
Scenario 2 for UCA-3: Water level is low but BPC does not detect it because of failed or not correctly calibrated water level sensor, due to lack of proper maintenance and calibration. Consequently, BPC does not close the produced water valve [UCA-3]. It causes hydrocarbon enter to the water stream and potentially release from the process [H1, H2]	Define and implement proper maintenance (preventive and corrective) for water level sensor to prevent failure.	3. Water level sensor maintenance, calibration and test backlog	Maintenance management system / real time (if not, monthly)	Water level sensor maintenance, calibration and test without delay
		4. Water level sensor has maintenance, calibration and test plan	Maintenance, calibration and test manual / Once	Water level sensor with maintenance and test plan
Scenario 3 for UCA-3: Water level is low and BPC detects it and send the command to close the produced water valve. The valve does not function correctly due to lack of proper maintenance [UCA-3]. It causes hydrocarbon enter to the water stream and potentially release from the process [H1, H2]	Same as safety measures defined for Scenario 1 for UCA-1.	5. Produced water valve maintenance, calibration and test backlog	Maintenance management system / real time (if not, monthly)	Produced water valve maintenance, calibration and test without delay
		6. Produced water valve has maintenance, calibration and test plan	Maintenance, calibration and test manual / Once	Produced water valve with maintenance and test plan

Scenario 1 for UCA-4: Water level is low but BPC detects it too late because of wrong set point of water level sensor, due to design or modifications during operation, and consequently close the produced water valve too late [UCA-4]. It causes hydrocarbon enter to the water stream and potentially release from the process [H1, H2]	Same as safety measures defined for Scenario 1 for UCA-1.	Same as 1 and 2		
Scenario 2 for UCA-4: Water level is low but BPC detect it too late because of not correctly calibrated water level sensor, due to lack of proper calibration. Consequently, BPC close the produced water valve too late [UCA-4]. It causes hydrocarbon enter to the water stream and potentially release from the process [H1, H2]	Same as safety measures defined Scenario 2 for UCA-3.	Same as 3 and 4		
Scenario 3 for UCA-4: Produced water valve functions too late when water level is low [UCA-4] because the valve closing time is too high. It causes hydrocarbon enter to the water stream and potentially release from the process [H1, H2]	Verify that the water valve closing time is short enough to prevent hydrocarbon enter to the water stream when water level is low and water valve needs to function (prevents scenario 3 for UCA-4 to happen). Moreover, mitigation measures defined in Scenario 1 for UCA-1.	7. Produced water valve closing time	Maintenance management system / real time (if not, according to test plan)	Closing time $\leq t_s$ (being t_s established according to engineering calculations and design documents to prevents scenario 3 for UCA-4)
Scenario 1 for UCA-5: Condensate level is high but BPC does not detect it because of wrong set point of condensate level sensor, due to design or modifications during operation, and consequently does not open the condensate valve [UCA-5]. It causes high pressure in the separator and condensate entering to gas stream and potentially release from the process [H1, H2]	Verify that condensate level sensor set point is established correctly in the design. Develop a formal process including required approvals for modification of condensate level sensor set point during operation. Include High High Level Alarm for condensate level, and also Safety Instrumented System (SIS) to shut down the process separator on condensate High High level and isolate the process.	8. Correct set point is established for condensate level sensor.	Design / Once	Correct set point (Acceptable)
		9. Set point (condensate level sensor) modification is done according to a procedure / instruction with required authorizations.	Set point modification audit / Annual	Set point modification audit report with no major finding

	Include manual shut down system to be used by operator on condensate High High level in case SIS does not function. Include PSV with set point below pressure design to protect the separator from being over pressurized and send the gas to flare system. In case of possible spills, include secondary containment and drain system.			
Scenario 2 for UCA-5: Condensate level is high but BPC does not detect it because of failed or not correctly calibrated condensate level sensor, due to lack of proper maintenance and calibration. Consequently, BPC does not open the condensate valve [UCA-5]. It causes high pressure in the separator and condensate entering to gas stream and potentially release from the process [H1, H2]	Define and implement proper maintenance (preventive and corrective) for condensate level sensor to prevent failure. Define and implement adequate calibration program for condensate level sensor to ensure correct detection. Plus mitigation measures defined in Scenario 1 for UCA-5.	10. Condensate level sensor maintenance, calibration and test backlog	Maintenance management system / real time (if not, monthly)	Condensate level sensor maintenance, calibration and test without delay
		11. Condensate level sensor has maintenance, calibration and test plan	Maintenance, calibration and test manual / Once	Condensate level sensor with maintenance and test plan
Scenario 3 for UCA-5: Condensate level is high and BPC detects it and send the command to open the condensate valve. The valve does not function correctly due to lack of proper maintenance [UCA-5]. It causes high pressure in the separator and condensate entering to gas stream and potentially release from the process [H1, H2]	Define and implement proper maintenance (preventive and corrective) for condensate valve to ensure it function correctly. Plus mitigation measures defined in Scenario 1 for UCA-5.	12. Condensate valve maintenance, calibration and test backlog	Maintenance management system / real time (if not, monthly)	Condensate valve maintenance, calibration and test without delay
		13. Condensate valve has maintenance, calibration and test plan	Maintenance, calibration and test manual / Once	Condensate valve with maintenance and test plan
Scenario 1 for UCA-6: BPC function to operate condensate valve is not correct and opens the condensate valve when condensate level is low in the separator due to wrong definition in design or modification during operation [UCA-6]. It causes gas enter to the condensate stream and potentially release from the process [H1, H2]	Verify that condensate valve function is defined correctly in the design, i.e. does not open when condensate level is low in the separator. Include Low Low Level Alarm for condensate level, and also Safety Instrumented System (SIS) to shut down the process on	14. Condensate valve function is defined correctly (i.e. does not open when condensate level is low in the separator)	Design / Once	Correct functioning of condensate valve (Acceptable)

	condensate Low Low Level. Include manual shut down system to be used by operator on condensate Low Low Level in case SIS does not function.			
Scenario 2 for UCA-6: Condensate level is low but BPC considers it as high because of wrong set point, failure or lack of calibration of condensate level sensor. This could happen due to wrong design or erroneous modifications during operation, or lack of proper maintenance and calibration of condensate sensor and consequently open the condensate valve [UCA-6]. It causes gas enter to the condensate stream and potentially release from the process [H1, H2]	Verify that condensate level sensor set point is established correctly in the design. Develop a formal process including required approvals for modification of condensate level sensor set point during operation. Define and implement proper maintenance (preventive and corrective) for condensate level sensor to prevent failure. Define and implement adequate calibration program for condensate level sensor to ensure correct detection. Plus mitigation measures defined in Scenario 1 for UCA-6.	Same as 8, 9, 10 and 11		
Scenario 1 for UCA-7: Condensate level is high but BPC detects it too late because of wrong set point of condensate level sensor, due to design or modifications during operation, and consequently open the condensate valve too late [UCA-7]. It causes high pressure in the separator and condensate enter to gas stream. [H1, H2]	Same as safety measures defined for scenario 1 for UCA-5.	Same as 8 and 9		
Scenario 2 for UCA-7: Condensate level is high but BPC detect it too late because of not correctly calibrated condensate level sensor, due to lack of proper calibration. Consequently, BPC open the condensate valve too late [UCA-7]. It causes high pressure in the separator and condensate enter to gas stream. [H1, H2]	Define and implement adequate calibration program for condensate level sensor to ensure correct detection. Plus mitigation measures defined in Scenario 1 for UCA-5.	Same as 10 and 11		

Scenario 3 for UCA-7: Condensate valve functions too late when condensate level is high [UCA-7] because the valve opening time is too high. It causes high pressure in the separator and condensate enter to gas stream. [H1, H2]	Verify that the condensate valve opening time is short enough to prevent condensate enter to the gas stream and high pressure in separator (prevents scenario 3 for UCA-7 to happen). Plus mitigation measures defined in Scenario 1 for UCA-5.	15. Condensate valve opening time	Maintenance management system / real time (if not, according to test plan)	Opening time $\leq t_s$ (being t_s established according to engineering calculations and design documents to prevents scenario 3 for UCA-7)
Scenario 1 for UCA-8: Condensate level is low but BPC does not detect it because of wrong set point of condensate level sensor, due to design or modifications during operation, and consequently does not open the condensate valve [UCA-8]. It causes gas enter to condensate stream (blow by) and potentially release from the process [H1, H2]	Verify that condensate level sensor set point is established correctly in the design. Develop a formal process including required approvals for modification of condensate level sensor set point during operation. Include Low Low Level Alarm for condensate level, and also Safety Instrumented System (SIS) to shut down the process separator on condensate Low Low level and isolate the process. Include manual shut down system to be used by operator on condensate Low Low level in case SIS does not function. In case of possible spills, include secondary containment and drain system.	Same as 8 and 9		
Scenario 2 for UCA-8: Condensate level is low but BPC does not detect it because of failed or not correctly calibrated condensate level sensor, due to lack of proper maintenance and calibration. Consequently, BPC does not close the condensate valve [UCA-8]. It causes gas enter to condensate stream (blow by) and potentially release from the process [H1, H2]	Define and implement proper maintenance (preventive and corrective) for condensate level sensor to prevent failure. Define and implement adequate calibration program for condensate level sensor to ensure correct detection. Plus mitigation measures defined in Scenario 1 for UCA-8	Same as 10 and 11		

Scenario 3 for UCA-8: Condensate level is low and BPC detects it and send the command to close the condensate valve. The valve does not function correctly due to lack of proper maintenance [UCA-8]. It causes gas enter to condensate stream (blow by) and potentially release from the process [H1, H2]	Define and implement proper maintenance (preventive and corrective) for condensate valve to ensure it function correctly. Plus mitigation measures defined in Scenario 1 for UCA-8.	Same as 12 and 13		
Scenario 1 for UCA-9: BPC function to operate condensate valve is not correct and closes the condensate valve when condensate level is high in the separator due to wrong definition in design or modification during operation [UCA-9]. It causes high pressure in the separator and condensate enter to gas stream. [H1, H2]	Verify that condensate valve function is defined correctly in the design, i.e. does not close when condensate level is high in the separator. Include High High Level Alarm for condensate level, and also Safety Instrumented System (SIS) to shut down the process on condensate High High Level. Include PSV with set point below separator's pressure design to protect the separator from being over pressurized and send gas to flare system. Include manual shut down system to be used by operator on condensate High High Level in case SIS does not function.	16. Condensate valve function is defined correctly (i.e. does not close when condensate level is high in the separator)	Design / Once	Correct functioning of condensate valve (Acceptable)

Scenario 2 for UCA-9: Condensate level is high but BPC considers it as low because of wrong set point, failure or lack of calibration of condensate level sensor. This could happen due to wrong design or erroneous modifications during operation, or lack of proper maintenance and calibration of condensate sensor and consequently closes the condensate valve [UCA-9]. It causes high pressure in the separator and condensate enter to gas stream. [H1, H2]	Verify that condensate level sensor set point is established correctly in the design. Develop a formal process including required approvals for modification of condensate level sensor set point during operation. Define and implement proper maintenance (preventive and corrective) for condensate level sensor to prevent failure. Define and implement adequate calibration program for condensate level sensor to ensure correct detection. Plus mitigation measures defined in Scenario 1 for UCA-9.	Same as 8, 9, 10 and 11		
Scenario 1 for UCA-10: Condensate level is low but BPC detects it too late because of wrong set point of condensate level sensor, due to design or modifications during operation, and consequently closes the condensate valve too late [UCA-10]. It causes gas enter to condensate stream (blow by) and potentially release from the process [H1, H2]	Verify that condensate level sensor set point is established correctly in the design. Develop a formal process including required approvals for modification of condensate level sensor set point during operation. Include Low Low Level Alarm for condensate level, and also Safety Instrumented System (SIS) to shut down the process separator on condensate Low Low level and isolate the process. Include manual shut down system to be used by operator on condensate Low Low level in case SIS does not function. Verify that process equipment downstream of the condensate valve have adequate pressure rating for possible blow by case. In case of possible spills, include secondary	Same as 8 and 9		

	containment and drain system.			
Scenario 2 for UCA-10: Condensate level is low but BPC detect it too late because of not correctly calibrated condensate level sensor, due to lack of proper calibration. Consequently, BPC closes the condensate valve too late [UCA-10]. It causes gas enter to condensate stream (blow by) and potentially release from the process [H1, H2]	Define and implement adequate calibration program for condensate level sensor to ensure correct detection. Plus mitigation measures defined in Scenario 1 for UCA-10.	Same as 10 and 11		
Scenario 3 for UCA-10: Condensate valve functions too late when condensate level is low [UCA-10] because the valve closing time is too high. It causes gas enter to condensate stream (blow by) and potentially release from the process [H1, H2]	Verify that the condensate valve closing time is short enough to prevent gas enter to the condensate stream (blow by), i.e. prevents scenario 3 for UCA-10 to happen.	17. Condensate valve closing time	Maintenance management system / real time (if not, according to test plan)	Closing time $\leq t_s$ (being t_s established according to engineering calculations and design documents to prevents scenario 3 for UCA-10)
Scenario 1 for UCA-11: BPC is required to maintain the process within the normal conditions, but operators disable the BPC due to faulty alarms because of lack of maintenance/calibration of alarms [UCA-11]. It causes process parameters out of the normal conditions and potentially hydrocarbon release from the process [H1, H2]	Define and implement proper maintenance (preventive and corrective) for process alarms to prevent faulty alarms.	18. Process alarms maintenance, calibration and test backlog	Maintenance management system / real time (if not, monthly)	Process alarms maintenance, calibration and test without delay
	Define and implement adequate calibration program for process sensors to ensure correct detection and prevent faulty alarms.	19. Process alarms have maintenance, calibration and test plan	Maintenance, calibration and test manual / Once	Process alarms with maintenance, calibration and test plan
Scenario 2 for UCA-11: BPC is required to maintain the process within the normal conditions, but operators disable the BPC due to its malfunctioning because of lack of maintenance/calibration of initiator, logic solver or final elements [UCA-11]. It causes process parameters out of the normal conditions and potentially hydrocarbon release from the process [H1, H2]	Define and implement proper maintenance (preventive and corrective) for process alarms, logic solver and final elements to prevent malfunctioning of BPC.	20. Process alarms, logic solvers and final elements maintenance, calibration and test backlog	Maintenance management system / real time (if not, monthly)	Process alarms, logic solvers and final elements maintenance, calibration and test without delay
	Define and implement adequate calibration program for process sensors to ensure correct detection and prevent malfunctioning of BPC.	21. Process alarms, logic solvers and final elements have maintenance, calibration and test plan	Maintenance, calibration and test manual / Once	Process alarms, logic solvers and final elements with maintenance, calibration and test plan

Scenario 3 for UCA-11: BPC is required to maintain the process within the normal conditions, but operators disable the BPC by error or due to lack of competency [UCA-11]. It causes process parameters out of the normal conditions and potentially hydrocarbon release from the process [H1, H2]	Ensure operators are competent in operating the plant (develop and implement a competency assurance system for operators). Develop and implement procedural control for disabling BPC including required authorization. Develop and implement physical and mental fitness to work program for operators.	22. Operations team members are competent	Human Resources and Competency Management / Annual	100 % of Operations team members deemed competent
		23. BPC is disabled according to a procedure / instruction with required authorizations.	BPC disabling audit / Annual	BPC disabling audit report with no major finding
Scenario 1 for UCA-12: Operators do not provide response to alarms when process is out of normal conditions because they are overwhelmed with the process requirements due to not having adequate alarm management [UCA-12]. As result, it creates a hazardous situation and potentially hydrocarbon release from the process [H1, H2]	Carry out an alarm management to ensure that operators are not overwhelmed with the process requirements.	24. Number of alarms per operator per hour	BPC / monthly	Acceptable <= 10 alarms / Operator / Hour
Scenario 2 for UCA-12: Operators do not provide response to alarms when process is out of normal conditions because of repetitive faulty alarms due to lack of maintenance/calibration of alarms [UCA-12]. As result, it can create a hazardous situation and potentially hydrocarbon release from the process [H1, H2]	Define and implement proper maintenance (preventive and corrective) for process alarms to prevent faulty alarms. Define and implement adequate calibration program for process sensors to ensure correct detection and prevent faulty alarms.	Same as 16 and 17		
Scenario 3 for UCA-12: Operators do not provide response to alarms when process is out of normal conditions due to lack of competency [UCA-12]. As result, it can create a hazardous situation and potentially hydrocarbon release from the process [H1, H2]	Ensure operators are competent in operating the plant (develop and implement a competency assurance system for operators).	Same as 20		
Scenario 1 for UCA-13: Operators provide response to alarms too late when process is out of normal conditions because	Carry out an alarm management to ensure that operators are not	Same as 22		

they are overwhelmed with the process requirements due to not having adequate alarm management [UCA-13]. As result, it may create a hazardous situation and potentially hydrocarbon release from the process [H1, H2]	overwhelmed with the process requirements.			
Scenario 1 for UCA-14: BPC is disabled and manual process control is required, but operators do not operate valves because they are overwhelmed with the process requirements due to not adequate alarm management [UCA-14]. As result, it may create a hazardous situation and potentially hydrocarbon release from the process [H1, H2]	Carry out an alarm management to ensure that operators are not overwhelmed with the process requirements.	Same as 22		
Scenario 2 for UCA-14: BPC is disabled and manual process control is required, but operators do not operate valves or operate wrong valves due to lack of competency or awareness [UCA-14]. As result, it may create a hazardous situation and potentially hydrocarbon release from the process [H1, H2]	Ensure operators are competent in operating the plant (develop and implement a competency assurance system for operators).	Same as 20		
Scenario 1 for UCA-15: Operators manipulate valves by error or because of lack of competency when it is not required [UCA-15]. It causes process parameters out of the normal conditions and potentially hydrocarbon release from the process [H1, H2]	Ensure operators are competent in operating the plant (develop and implement a competency assurance system for operators).	Same as 20		
Scenario 1 for UCA-16: BPC is disabled and manual process control is required, but operators provide intervention too late because they are overwhelmed with the process requirements due to not adequate alarm management [UCA-16]. As a result, hydrocarbon may be released from the process [H1, H2]	Carry out an alarm management to ensure that operators are not overwhelmed with the process requirements.	Same as 22		

18 safety checkpoints are defined for general control structure and 24 safety checkpoints are defined for the refined control structure. Defined safety checkpoints at both levels are analyzed and consolidated. It means, the repeated safety checkpoints are eliminated and the related checkpoints are combined. A summary of consolidated safety checkpoints is provided in (Table 21).

Table 21 The final list of safety checkpoints (The list of consolidated safety checkpoints)

	Safety Checkpoint	Source / Frequency	Expected Data
1	Number of alarms per operator per hour	BPC / monthly	Acceptable ≤ 10 alarms / Operator / Hour
2	BPC is disabled according to a procedure / instruction with required authorizations.	BPC disabling audit / Annual	BPC disabling audit report with no major finding
3	All abnormal conditions are identified and correct function is defined for each abnormal condition.	Design / Once	Abnormal conditions are identified and correct functions are defined.
4	Condensate valve function is defined correctly (i.e. does not open/close when condensate level is low/high in the separator)	Design / Once	Correct functioning of condensate valve (Acceptable)
5	Correct set point established for process parameter sensors.	Design / Once	Correct set point for sensors (Acceptable)
6	Right sensor is selected for each process parameter.	Design / Once	Right Sensor (Acceptable)
7	Maintenance team members are competent	Human Resources and Competency Management / Annual	100 % of maintenance team members deemed competent
8	Operations team members are competent	Human Resources and Competency Management / Annual	100 % of Operations team members deemed competent
9	Average required time for works assigned to a maintenance team member during a month	Maintenance management system / monthly	Less than 172 hour / month
10	Condensate valve closing/opening time	Maintenance management system / real time (if not, according to test plan)	Closing/Opening time $\leq t_s$ (being t_s established according to engineering calculations and design documents to prevents scenario 3 for UCA-10 and scenario 3 for UCA-7)
11	Produced water valve closing time	Maintenance management system / real time (if not, according to test plan)	Closing time $\leq t_s$ (being t_s established according to engineering calculations and design documents to prevents scenario 3 for UCA-4)

12	Maintenance, calibration and test backlog: Produced water and Condensate level sensors, Produced water and Condensate Valve, Process alarms, Process Control elements (initiators, logic solvers and final elements)	Maintenance management system / real time (if not, monthly)	Produced water and Condensate level sensors, Produced water and Condensate Valve, Process alarms, Process Control elements (initiators, logic solvers and final elements) maintenance, calibration and test without delay
13	Produced water and Condensate level sensors, Produced water and Condensate Valve, Process alarms, Process Control elements (initiators, logic solvers and final elements) have maintenance, calibration and test plan	Maintenance, calibration and test manual / Once	Produced water and Condensate level sensors, Produced water and Condensate Valve, Process alarms, Process Control elements (initiators, logic solvers and final elements) with maintenance, calibration and test
14	In case of replacement or repair, right sensor is used for each process parameter (MOC and authorization)	MOC process audit / Annual	MOC audit report with no major finding
15	Modification of process parameter sensors' set point is included in the operation manual and is done with adequate authorization.	Process parameter sensors' set point modification audit / Annual	Process parameter sensors' set point modification audit report with no major finding
16	Set point (water level and condensate level sensor) modification is done according to a procedure / instruction with required authorizations.	Set point modification audit / Annual	Set point modification audit report with no major finding

The outcome (Table 21) includes safety checkpoints on different aspects and at different levels of the sociotechnical system:

- Design/Technical/Engineering
- BPC functionality
- Operational controls (e.g. disabling BPC, set point modification)
- Operational performance (e.g. maintenance backlog)
- Competency
- Organizational controls (e.g. MOC, resource allocation, maintenance planning)

Each safety checkpoint could be related to one or more loss scenarios of the plant. The higher the number of loss scenarios related to one safety checkpoint the higher importance of that safety checkpoint in the safety of the plant. In order to define the safety level of the plant based on the responses provided to each checkpoint it is necessary to calculate the weight of these safety checkpoints. Weight of each safety checkpoint is shown in percentage that is calculated based on the number of loss scenarios prevented by each safety checkpoint among total number of loss scenarios.

The number of loss scenarios related to each safety checkpoint for general and refined control structure is provided in Table 22 and Table 23.

Table 22 Number of loss scenarios related to each safety checkpoint for general control structure

	Safety Checkpoint	Number of related loss scenarios
1	Right sensor is selected for each process parameter.	1
2	In case of replacement or repair, right sensor is used for each process parameter (MOC and authorization)	1
3	Process parameter sensors maintenance, calibration and test backlog.	2
4	Process parameter sensors have maintenance, calibration and test plan	2
5	Maintenance team members are competent	13
6	Correct set point established for process parameter sensors.	2
7	Modification of process parameter sensors' set point is included in the operation manual with adequate authorization.	3
8	Process parameter sensors' set point modification audit.	3
9	All abnormal conditions are identified and correct function is defined for each abnormal condition.	3
10	Control system actuators (final elements) maintenance and test backlog	6
11	Control system actuators have maintenance and test plan	5
12	Operations team members are competent	4
13	Process alarms maintenance, calibration and test backlog	1
14	Process alarms have maintenance and test plan	1
15	Process control elements (initiator, logic solver and final element) maintenance, calibration and test backlog	1
16	Process control elements (initiator, logic solver and final element) have maintenance, calibration and test plan	4
17	Number of alarms per operator per hour	2
18	Average required time for works assigned to a maintenance team member during a month	2
Total		56

Table 23 Number of loss scenarios related to each safety checkpoint for refined control structure

	Safety Checkpoint	Number of related loss scenarios
1	Correct set point is established for water level sensor.	4
2	Set point (water level sensor) modification is done according to a procedure / instruction with required authorizations.	4
3	Water level sensor maintenance, calibration and test backlog	2

4	Water level sensor has maintenance, calibration and test plan	2
5	Produced water valve maintenance, calibration and test backlog	1
6	Produced water valve has maintenance, calibration and test plan	1
7	Produced water valve closing time	1
8	Correct set point is established for condensate level sensor.	6
9	Set point (condensate level sensor) modification is done according to a procedure / instruction with required authorizations.	6
10	Condensate level sensor maintenance, calibration and test backlog	6
11	Condensate level sensor has maintenance, calibration and test plan	6
12	Condensate valve maintenance, calibration and test backlog	2
13	Condensate valve has maintenance, calibration and test plan	2
14	Condensate valve function is defined correctly (i.e. does not open when condensate level is low in the separator)	1
15	Condensate valve opening time	1
16	Condensate valve function is defined correctly (i.e. does not close when condensate level is high in the separator)	2
17	Condensate valve closing time	2
18	Process alarms maintenance, calibration and test backlog	1
19	Process alarms have maintenance, calibration and test plan	1
20	Process alarms, logic solvers and final elements maintenance, calibration and test backlog	4
21	Process alarms, logic solvers and final elements have maintenance, calibration and test plan	1
22	Operations team members are competent	4
23	BPC is disabled according to a procedure / instruction with required authorizations.	1
24	Number of alarms per operator per hour	1
Total		62

Taking into account the number of related loss scenarios to each safety checkpoint and the way that safety checkpoints are consolidated, the number of loss scenarios related to the safety checkpoints of the final list (consolidated) is provided in Table 24. The weighing associated to each safety checkpoints is calculated in percentage. Figure 61 also shows the number of loss scenarios related to each safety checkpoint of the final list.

Table 24 Number of loss scenarios and weighing related to consolidated safety checkpoint of the final list

	Safety Checkpoint	Number of related loss scenarios	Weighing (%)
1	Number of alarms per operator per hour	3	2,54%
2	BPC is disabled according to a procedure / instruction with required authorizations.	1	0,85%

3	All abnormal conditions are identified and correct function is defined for each abnormal condition.	3	2,54%
4	Condensate valve function is defined correctly (i.e. does not open/close when condensate level is low/high in the separator)	3	2,54%
5	Right sensor is selected for each process parameter.	1	0,85%
6	Correct set point established for process parameter sensors.	12	10,17%
7	Maintenance team members are competent	13	11,02%
8	Operations team members are competent	8	6,78%
9	Average required time for works assigned to a maintenance team member during a month	2	1,69%
10	Condensate valve closing/opening time	3	2,54%
11	Produced water valve closing time	1	0,85%
12	Maintenance, calibration and test backlog: Produced water and Condensate level sensors, Produced water and Condensate Valve, Process alarms, Process Control elements (initiators, logic solvers and final elements)	26	22,03%
13	Produced water and Condensate level sensors, Produced water and Condensate Valve, Process alarms, Process Control elements (initiators, logic solvers and final elements) have maintenance, calibration and test plan	25	21,19%
14	In case of replacement or repair, right sensor is used for each process parameter (MOC and authorization)	1	0,85%
15	Modification of process parameter sensors' set point is included in the operation manual and is done with adequate authorization.	6	5,08%
16	Set point (water level and condensate level sensor) modification is done according to a procedure / instruction with required authorizations.	10	8,48%
Total		118	100%

Figure 61 Number of loss scenarios related to each safety checkpoint

Then, the indicator, acceptability criteria and associated value for each safety checkpoint are defined for the final list of safety checkpoints (Table 25).

Table 25 Indicator, acceptability criteria and safety levels for each safety checkpoint of the final list

	Safety Checkpoint	Weight (%)	Indicator	Acceptability Criteria / Safety Level		
				Not acceptable (0)	Partially acceptable (0,5)	Acceptable (1)
1	Number of alarms per operator per hour	2,54%	# alarms / Operator / Hour	> 20	> 10 and <= 20	<= 10
2	BPC is disabled according to a procedure / instruction with required authorizations.	0,85%	BPC disabling audit report findings	More than 2 major findings	1 or 2 major findings	No major finding
3	All abnormal conditions are identified and correct function is defined for each abnormal condition.	2,54%	Identification of abnormal conditions are definition of correct functions	There is no correct identification of abnormal conditions and corresponding functions	There are only few abnormal conditions that don't have correct function	All abnormal conditions are identified and correct functions are defined
4	Condensate valve function is defined correctly (i.e. does not open/close when condensate level is low/high in the separator)	2,54%	Functioning of condensate valve	Condensate valve opens/closes when condensate level is low/high respectively	N/A	Condensate valve does not open/close when condensate level is low/high respectively
5	Right sensor is selected for each process parameter.	0,85%	Selection of sensor for process parameters	There are wrong sensors selected for process parameters	N/A	Right sensor is selected for all process parameters
6	Correct set point established for process parameter sensors.	10,17%	Definition of set point for process parameter sensors	There are errors in set points established for process parameter sensors	N/A	Correct set points are established for all process parameter senso

7	Maintenance team members are competent	11,02%	Maintenance team members competency	One or more maintenance team members not deemed competent	Some of maintenance team members not satisfying some of competency requirements	100 % of maintenance team members deemed competent on all competency requirements
8	Operations team members are competent	6,78%	Operations team members competency	One or more operations team members not deemed competent	Some of operations team members not satisfying some of competency requirements	100 % of operations team members deemed competent on all competency requirements
9	Average required time for works assigned to a maintenance team member during a month	1,69%	Average work hour per month	> 206 hrs /mth	> 172 hrs / mth and <= 206 hrs /mth	<= 172 hrs / mth
10	Condensate valve closing/opening time (according to engineering calculations and design documents to prevents scenario 3 for UCA-10 and scenario 3 for UCA-7)	2,54%	Condensate valve Closing/Opening time	Closing/Opening time > 1,1*X	Closing/Opening time > X and <= 1,1*X	Closing/Opening time<= X
11	Produced water valve closing time (according to engineering calculations and design documents to prevents scenario 3 for UCA-4)	0,85%	Produced water valve Closing time	Closing time > 1,1*X	Closing time > X and <= 1,1*X	Closing time<= X
12	Maintenance, calibration and test backlog of Produced water and Condensate level sensors, Produced water and Condensate Valve, Process alarms, Process Control elements (initiators, logic solvers and final elements)	22,03%	Maintenance, calibration and test backlog	< 85% of the items of the items listed in this safety checkpoint without backlog	< 95% but >= 85% of the items listed in this safety checkpoint without backlog	>= 95 % of the items listed in this safety checkpoint without backlog
13	Produced water and Condensate level sensors, Produced water and Condensate Valve, Process alarms, Process Control elements (initiators, logic solvers and final elements) have maintenance, calibration and test plan	21,19%	Maintenance, calibration and test plan	There are some items listed in this safety checkpoint without maintenance, calibration and test plan	N/A	100 % of the items listed in this safety checkpoint with maintenance, calibration and test plan
14	In case of replacement or repair, right sensor is used for each process parameter (MOC and authorization)	0,85%	MOC audit report findings	More than 2 major findings	1 or 2 major findings	No major finding
15	Modification of process parameter sensors' set point is included in the operation manual and is done with adequate authorization.	5,08%	Process parameter sensors' set point modification audit report findings	More than 2 major findings	1 or 2 major findings	No major finding
16	Set point (water level and condensate level sensor) modification is done according to a procedure / instruction with required authorizations.	8,48%	Set point modification audit report findings	More than 2 major findings	1 or 2 major findings	No major finding

To calculate the cumulative safety level, the formula introduced in Equation 1 Formula to calculate cumulative safety level based on data of safety checkpoints) is used taking into account safety levels and weights of each safety checkpoint provided in Table 25.

In order to calculate the cumulative safety level of the plant based on this methodology, data is obtained from the plant under study and safety level of each safety checkpoint is determined (Table 26). Based on the provided data from the plant, for each safety checkpoint the associated color is marked and in some cases, additional information is provided in the comment column.

Table 26 Determined safety level of plant safety checkpoint

	Safety Checkpoint	Weight (%)	Indicator	Acceptability Criteria / Safety Level	Comment

				0	0,5	1	
1	Number of alarms per operator per hour	2,54%	# alarms / Operator / Hour	> 20	> 10 and <= 20	<= 10	4 alarms / Operator / Hour
2	BPC is disabled according to a procedure / instruction with required authorizations.	0,85%	BPC disabling audit report findings	More than 2 major findings	1 or 2 major findings	No major finding	1 major finding and 2 medium findings in the last audit report
3	All abnormal conditions are identified and correct function is defined for each abnormal condition.	2,54%	Identification of abnormal conditions are definition of correct functions	There is no correct identification of abnormal conditions and corresponding functions	There are less than 20 % of abnormal conditions that don't have correct function	All abnormal conditions are identified and correct functions are defined	
4	Condensate valve function is defined correctly (i.e. does not open/close when condensate level is low/high in the separator)	2,54%	Functioning of condensate valve	Condensate valve opens/closes when condensate level is low/high respectively	N/A	Condensate valve does not open/close when condensate level is low/high respectively	
5	Right sensor is selected for each process parameter.	0,85%	Selection of sensor for process parameters	There are wrong sensors selected for process parameters	N/A	Right sensor is selected for all process parameters	
6	Correct set point established for process parameter sensors.	10,17%	Definition of set point for process parameter sensors	There are errors in set points established for process parameter sensors	N/A	Correct set points are established for all process parameter sensor	
7	Maintenance team members are competent	11,02%	Maintenance team members competency	One or more maintenance team members not	Some of maintenance team members not satisfying	100 % of maintenance team members deemed competent	Competency of Maintenance team member is assessed based on followings according to the job profile:

				deemed competent	some of competency requirements	on all competency requirements	-required trainings and certifications -outcome of task observations
8	Operations team members are competent	6,78%	Operations team members competency	One or more operations team members not deemed competent	Some of operations team members not satisfying some of competency requirements	100 % of operations team members deemed competent on all competency requirements	Competency of Operations team member is assessed based on followings according to the job profile: -required trainings and certifications -outcome of task observations
9	Average required time for works assigned to a maintenance team member during a month	1,69%	Average work hour per month	> 206 hrs /mth	> 172 hrs / mth and <= 206 hrs /mth	<= 172 hrs / mth	
10	Condensate valve closing/opening time (according to engineering calculations and design documents to prevents scenario 3 for UCA-10 and scenario 3 for UCA-7)	2,54%	Condensate valve Closing/Opening time	Closing/Opening time > 1,1*X	Closing/Opening time > X and <= 1,1*X	Closing/Opening time<= X	
11	Produced water valve closing time (according to engineering calculations and design documents to prevents scenario 3 for UCA-4)	0,85%	Produced water valve Closing time	Closing time > 1,1*X	Closing time > X and <= 1,1*X	Closing time<= X	
12	Maintenance, calibration and test backlog of Produced water and Condensate level sensors, Produced water and Condensate Valve, Process alarms, Process Control elements (initiators, logic solvers and final elements)	22,03%	Maintenance, calibration and test backlog	< 85% of the items of the items listed in this safety checkpoint without backlog	< 95% but >= 85% of the items listed in this safety checkpoint without backlog	>= 95 % of the items listed in this safety checkpoint without backlog	20 % of the items listed in this safety checkpoint have backlog
13	Produced water and Condensate level sensors, Produced water and Condensate	21,19%	Maintenance, calibration and test plan	There are some items listed in	N/A	100 % of the items listed in this safety	

	Valve, Process alarms, Process Control elements (initiators, logic solvers and final elements) have maintenance, calibration and test plan			this safety checkpoint without maintenance, calibration and test plan		checkpoint with maintenance, calibration and test plan	
14	In case of replacement or repair, right sensor is used for each process parameter (MOC and authorization)	0,85%	MOC audit report findings	More than 2 major findings	1 or 2 major findings	No major finding	3 major findings, 4 medium findings and 3 recommend
15	Modification of process parameter sensors' set point is included in the operation manual and is done with adequate authorization.	5,08%	Process parameter sensors' set point modification audit report findings	More than 2 major findings	1 or 2 major findings	No major finding	no major finding, 1 medium finding
16	Set point (water level and condensate level sensor) modification is done according to a procedure / instruction with required authorizations.	8,48%	Set point modification audit report findings	More than 2 major findings	1 or 2 major findings	No major finding	no finding

Using the formula (**Error! Reference source not found.**), safety level values and weights of each safety checkpoint the cumulative safety level is calculated as 67.8%. The cumulative safety level can be shown in a gauge designed to demonstrate the safety level from 0 to 100% (Figure 62). There is no precise calculation behind colors in this gauge and it is for demonstration purpose. Nevertheless, there is a logic behind it: the plant can be considered safe when all the safety checkpoints are 'acceptable', consequently, 100% is considered as safe and green. When even one safety checkpoint is 'not acceptable' or 'partially acceptable', the plant cannot be considered as safe and green. Consequently, for values less than 100% the color changes gradually from green to amber and red.

Figure 62 A gauge designed to demonstrate the safety level of the plant

This methodology is developed to measure safety level of a process plant. However, the outcome can be presented in different ways to help decision maker in taking proactive and timely actions in order to prevent accidents. Few examples of presenting the outcome are provided below.

List of safety checkpoints and their status (safety level) can be shown in a table (Table 27). It helps to easily identify any safety checkpoint that its status is not 'acceptable'. Actions need to be taken to change the status of these safety checkpoints to 'acceptable' and improve the safety level of the plant.

Table 27 Summary of the status (safety level) of each checkpoint

	Safety Checkpoint	Indicator	Safety Level
1	Number of alarms per operator per hour	# alarms / Operator / Hour	
2	BPC is disabled according to a procedure / instruction with required authorizations.	BPC disabling audit report findings	
3	All abnormal conditions are identified and correct function is defined for each abnormal condition.	Identification of abnormal conditions are definition of correct functions	
4	Condensate valve function is defined correctly (i.e. does not open/close when condensate level is low/high in the separator)	Functioning of condensate valve	
5	Right sensor is selected for each process parameter.	Selection of sensor for process parameters	
6	Correct set point established for process parameter sensors.	Definition of set point for process parameter sensors	
7	Maintenance team members are competent	Maintenance team members competency	
8	Operations team members are competent	Operations team members competency	
9	Average required time for works assigned to a maintenance team member during a month	Average work hour per month	
10	Condensate valve closing/opening time (according to engineering calculations and design documents to prevents scenario 3 for UCA-10 and scenario 3 for UCA-7)	Condensate valve Closing/Opening time	
11	Produced water valve closing time (according to engineering calculations and design documents to prevents scenario 3 for UCA-4)	Produced water valve Closing time	
12	Maintenance, calibration and test backlog of Produced water and Condensate level sensors, Produced water and Condensate Valve, Process alarms, Process Control elements (initiators, logic solvers and final elements)	Maintenance, calibration and test backlog	
13	Produced water and Condensate level sensors, Produced water and Condensate Valve, Process alarms, Process Control elements (initiators, logic solvers and final elements) have maintenance, calibration and test plan	Maintenance, calibration and test plan	
14	In case of replacement or repair, right sensor is used for each process parameter (MOC and authorization)	MOC audit report findings	
15	Modification of process parameter sensors' set point is included in the operation manual and is done with adequate authorization.	Process parameter sensors' set point modification audit report findings	

16	Set point (water level and condensate level sensor) modification is done according to a procedure / instruction with required authorizations.	Set point modification audit report findings	

The overall safety status of the process plant can be shown in a pie chart (Figure 63). This pie chart helps to identify those safety checkpoints that their status is not ‘acceptable’ and also their importance in safety of the process plant. For example, the pie chart provided in Figure 63 shows that status of safety checkpoint # 12, which plays a key role in the safety of the process plant, is ‘not acceptable. Safety checkpoint # 12 is on about the ‘Maintenance, calibration and test backlog of Produced water and Condensate level sensors, Produced water and Condensate Valve, Process alarms, Process Control elements (initiators, logic solvers and final elements)’. Consequently, decision makers have a very important information about the safety of the plant and it helps them in a proactive approach in safety management.

Figure 63 Pie chart of the overall safety status of the process plant and each safety checkpoint

The overall safety status of the process plant can also be shown in a tape type meter (Figure 64). This meter helps to visualize the missing part to be considered as a safe plant. If the tape if 100 % green, it means that the plant can be considered safe. In this case, there are red and amber areas on the tape. Red area is composed of two safety checkpoints (#12 and #14) with a ‘not acceptable’ status. Amber area is composed of three safety checkpoints (#2, #7 and #8) with a ‘partially acceptable’ status. Consequently, decision makers have enough information on where to act in order to have a safe process plant. It helps them to prioritize tasks and resources and proactively work on areas that need more attention in order to prevent accident.

Figure 64 Overall safety status of the process plant in a tape type meter

This is only a demonstration to show the capability of the methodology. For industrial use, it is necessary to extend its scope to all the equipment in the plant and higher levels of the sociotechnical structure. Then, complete the list of safety checkpoints and based on the status of safety checkpoints calculate the safety level of the plant and present the outcome in different manners with useful information for different stakeholders.

A summary of the application of the methodology is published in Process Safety and Environmental Protection Journal: <https://doi.org/10.1016/j.psep.2020.01.035>

Chapter 8 Conclusions

Process industry has experienced many major accidents with multiple fatalities, significant environmental impacts or property and financial loss. There have been many actions and improvements in term of regulations, organizations and technical aspects to prevent these accidents or lessen their consequences. However, major accidents continue to occur in the process industry and often have serious consequences. This has raised concerns in safety management and highlighted problems in scientific thinking about safety.

Traditionally, safety is seen as the absence of accidents. Such definition of safety is indirect rather than direct since safety is defined by what happens when it is absent or missing. It has led to measurement of safety by the number of accidents. Because of this, there are many safety indicators based on accidents, mishaps or near misses. In fact these indicators are measuring the absence of safety rather than the presence of safety. As conclusion, with this understanding about safety, there is no way to measure safety but its absence.

Recently, safety is seen in another way; it accepts that we cannot understand all of our system, nor understand them entirely. Instead of looking only at accidents, this new approach focuses on everyday work and situations where things go right. It is equivalent to the new understanding of the health: 'health is a state of complete physical, mental, and social wellbeing and not merely the absence of disease or infirmity'.

In contrary to the safety definition based of the absence of accidents, the new approach does not assume that we can understand our systems by looking at their components and how these components function or fail. In the other words, determining whether a system is safe only by examining components of the system is not possible. In fact, statements about the safety of a component without information about the context in which the component is located have no meaning. However, statements about the reliability of a component, where reliability is defined as the probability that the component functions when demanded, could be valid.

Based on this new approach, safety is an emergent property of a system and can only be determined by the status and relationship between components in the context of the whole system. Therefore, it is not possible to take a single system component in isolation and assess it with the hope to determine the safety of the system based on the status of the individual components.

Treating safety as an emergent property of systems based on the components interaction within the system context leads to systemic accident models. These accident models can serve as a proper base for development of tools and methodologies for safety measurements. AcciMap, Functional Resonance Accident Model (FRAM) and Systems Theoretic Accident Model and Processes (STAMP) are notable systemic models trying to model complex sociotechnical systems. STAMP assumes that accidents occur when component failures, external disturbances, and/or dysfunctional interactions among system components are not adequately handled by the control system.

Causal Analysis based on Stamp (CAST) is the accident analysis technique and System Theoretic Process Analysis (STPA) is the hazard identification technique based on STAMP. In this work, CAST is used to analyze an accident happened in the process industry, 2012

Chevron Refinery accident, and the result is compared with the ones obtained by AcciMap and FRAM. In addition, STPA is used to study hazards of a process plant and the result is compared with the plant HAZOP as a traditional technique. STAMP seems to be one of the most appropriate accident models to handle complex systems.

In this work, authors tried to find a solution based on STAMP for proactive measurement of safety level before a process plant, as a complex system, gradually move toward an unsafe state. A novel methodology is developed based on STPA with the purpose of measuring safety level in process plants and ultimately preventing accidents. The measurement of safety level is done according to the status of safety checkpoints. Safety checkpoint is a new concept introduced in this work and added to STPA. A safety checkpoint is a requirement defined to prevent a loss scenario to happen or to satisfy safety measures associated to the loss scenario.

The methodology is applied to a section of a process plant. 16 safety checkpoints are defined on different aspects and at different levels of the sociotechnical system:

- Design/Technical/Engineering
- Basic Process Control (BPC) functionality
- Operational controls (e.g. disabling BPC, set point modification)
- Operational performance (e.g. maintenance backlog)
- Staff Competency
- Organizational controls (e.g. MOC, resource allocation, maintenance planning)

Each safety checkpoint could be related to one or more loss scenario of the plant. In this case 118 loss scenarios are defined. The higher the number of loss scenarios related to one safety checkpoint the higher its weight in calculating the safety level. In order to calculate the safety level of the plant based on this methodology, data is obtained from the plant and the status of each safety checkpoint is determined. Taking into account the weight of each safety checkpoint the plant safety level is calculated as 67.8%.

This methodology is developed to measure the safety level of a process plant. However, the outcome can be presented in different ways to help management in making informed risk based decisions and taking proactive and timely actions in order to prevent accidents:

- List of safety checkpoints and their status can be shown in a dashboard. It helps to easily identify any safety checkpoint that has an unacceptable status in order to take required actions to improve the safety level of the plant.
- Safety status of the process plant can be shown in a pie chart. This can help to identify safety checkpoints with unacceptable status and their importance (weight) in safety of the process plant. It provides a very important information to decision makers to prioritize actions in a proactive manner
- Overall safety status of the process plant can also be shown in a tape type meter helping to visualize the missing parts. Decision makers have enough information on where to act in order to have a safe process plant. It helps them to prioritize tasks and resources and proactively work on areas that need more attention in order to improve safety of the process plant.

The results obtained from this methodology are promising and provide a significant improvement comparing with the existing solutions at industrial and academic environments for safety measurement.

In the industrial environment, many works have been done to measure safety. Center for Chemical Process Safety (CCPS, 2007), American Petroleum Institute (API, 2016), International Association of Oil & Gas Producers IOGP (IOGP, 2018), European Chemical Industry Council (CEFIC, 2011), Organization for Economic Cooperation and Development (OECD, 2008) and UK Health and Safety Executive (HSE UK, 2006) amongst others have published procedures and guidelines on process safety indicators. CCPS, API and IOGP assumed a predictive relationship between lower and higher consequence process safety events similar to the accident pyramid introduced by Heinrich for personal injuries. Where the pyramid represent a continuum of leading and lagging process safety indicators from the bottom to the top. Most of the safety measurements suggested in the industrial environment are heavily based on counting accidents and/or near misses. This is not limited to process safety and includes occupational safety.

Regarding process safety, lagging indicators cannot be helpful in measuring safety because major accidents are rare and occur so infrequently specially at a site level. Therefore, lagging indicators cannot be used to measure safety and may not be useful as early warnings to prevent accidents. There have been some efforts, like the IOGP publication on leading process safety indicator (IOGP, 2016), that focus on developing indicators that provide some information before an accident occurs (leading indicators). Leading indicators are generally intended to help in identifying early signals of deteriorating performance and thereby to provide means for warning of impending problems before an actual accident occurs. Early warnings from these indicators should initiate a further investigation on the causes of the symptoms to ensure that actions will be timely taken. Depending on how leading indicators are defined, there may be a good coverage in one area and a vacuum in another area. Definition of leading indicators is mainly experience based and focuses on known areas without counting on a system based approach.

In addition to the publications on safety measurement in the industrial environment, there have been some tools developed by companies like e-Vision (e-Vision, 2019), CGE (CGE Risk Management Solutions, 2019), DNV-GL (DNV-GL, 2019) Petrotechnics (Petrotechnics, 2019), RiskPoynt (RiskPoynt, 2019) and Safetec (SAFETEC, 2019) among others to visualize and monitor the status of safety barriers.

Mentioned publications or tools are not based on any systemic approach on accidents and in some cases they are based on Swiss Cheese Model that is a model based on chain of event. Swiss Cheese Model has some component of systems but it is not considered as a thoroughly systemic model.

In the academic environment, there were some previous efforts like ‘safety barometer’ by (Knegtering & Pasman, 2013) and ‘PROCESO index’ by (Maroño, Pena, & Santamaria, 2006)) to find a solution for safety measurement. However, none of them used systems theories that is the promising solution for sociotechnical complex systems we encounter these days in process industry.

The methodology is tested on a section of a process plant using real data with promising results. The result could be shown in different formats and help decision makers to make informed risk based decisions. However, this is only a demonstration to show the capability of the methodology. For industrial use, it is necessary to extend the scope to the whole process plant and higher levels of the sociotechnical structure of the process plant. In order to validate the methodology, it is necessary to use it in a process plant for a period of time long enough for evaluation and analysis of accident data before and after implementation of the methodology and assess the validity and effectiveness of the methodology in measuring safety level and helping the management in proactive management of safety. When the methodology is implemented, another validation mechanism would be to check the level of safety obtained by the methodology at the time of accidents.

As conclusion, although some researchers in the academic environment have made efforts to measure safety and in the industrial environment some works have been done and guides or practices have been published to find a solution for safety measurement, none of them obtained results comparable to this work, nor they used systems theories that is the promising solution for sociotechnical complex systems we encounter these days in process plants. Consequently, it is recommended to continue the work by full implementation of the methodology in a process plant and validate it as mentioned before.

Appendix I HAZOP Study of the process plant under study

A copy of the HAZOP study of the node related to the cooler and separator is provided in the following 4 images:

ITEM	GUIDE PHRASE	POSSIBLE CAUSES	CONSEQUENCES	SAFEGUARDS	S	L	R	CATEGORY	ACTION No.	ACTION	ACTIONEE	REMARKS
2.1.1	No Flow	20SDV-1701 fails closed	Loss of production through Train 1 and increased production through other trains (See Node1)		-	-	-	-				
		Any manual valve inadvertently closed	Refer to Item 2.1.1	SOP								
			-	Refer to Item 2.1.1								
		20FV-1714 stuck closed	Refer to Item 2.1.1									Similar consequence based on other trains in operation
2.2.1	Less Flow	Manual valve on the individual Compressor Inlet Cooler Train 1 (20HAL-103A/B/C/D/E/F) bay	Increased flow to remaining bays resulting in higher DP and temperature to downstream equipment	SOP	3	4	11/12	Asset				
			-	20TAH-1713 to alert operator	-	-	-	-				
			-	20TAHH-1714 to trip Train 1 to close 20ESDV-1701	-	-	-	-				
		Inlet Compressor Separator Train 1 (20MBD-103) demister pad partially blocked	Reduced flow through train resulting in potential higher DP and increased production through other trains	20PT-1705 at upstream Compressor Inlet Cooler Train 1 (20HAL-103A/B/C/D/E/F) and 20PT-1716 at Inlet Compressor Separator Train 1 (20MBD-103) gas outlet to identify high DP								
			-	20PT-1701 at Inlet Compressor Separator Train 1 (20MBD-103) to identify high DP								
2.2.2		Liquid build up in Compressor Inlet Cooler Train 1 (20HAL-103A/B/C/D/E/F)	Reduced flow until liquid slug removed from Cooler	Cooler design - slope towards Inlet Compressor Separator Train 1 (20MBD-103)	-	-	-	-				Gas outlet slope to allow any liquid to drain back to Inlet Compressor Separator Train 1 (20MBD-103)
2.3.1	More Flow	20FV-1714 fails open	High flow through train resulting in high temperature and liquid entrainment to the downstream 1st Stage Inlet Compressor (23-CAE-100/200/300/400/500)	20FAH-1716 to alert operator	3	4	11/12	Asset				
			-	20TAH-1713/1716 to alert operator	-	-	-	-				
			-	20TAHH-1714 to trip the train	-	-	-	-				
			-	Downstream Inlet Compressor Suction Scrubber (20MBF-100/200/300/400/500) to handle increased liquid load	-	-	-	-				4 trains are in operation (5x25%)
		Manual valve on bypass around 20FV-1714 inadvertently opened	Refer to Item 2.3.1	SOP								
2.3.2		Other inlet train shutdown	Refer to Item 2.1.1		-	-	-	-				
2.4.1	Reverse Flow	Refer to Item 2.1.1			-	-	-	-				
2.5.1	Misdirected Flow	Manual valve on bypass line of 20PSV-1701 inadvertently opened	Loss of hydrocarbon gas to flare	SOP - valve is CSC	2	3	11/6	Business Interruption	#3	Remove CSC on bypass valve around PSV to consistent with current mode of operations	TPE	Applies across project
2.6.1	Less Pressure	Refer to Item 2.1.1			-	-	-	-				
2.7.1	More Pressure	No additional significant issues of concern identified			-	-	-	-				

Page 1 of 4: the node related to cooler and separator from process plant HAZOP

ITEM	GUIDE PHRASE	POSSIBLE CAUSES	CONSEQUENCES	SAFEGUARDS	S	L	R	CATEGORY	ACTION No.	ACTION	ACTIONEE	REMARKS
2.8.1	Less Temperature	Overcooling of gas at low flowrates or during heavy rain	Potential higher DP at Inlet Cooler Train 1 (20HAL-103A/B/C/D/E/F) and increased liquid load to Inlet Compressor Separator Train 1 (20MBO-103) (no significant adverse consequence)	-	-	-	-	-				
2.9.1	More Temperature	Compressor Inlet Cooler Train 1 (20HAL-103A/B/C/D/E/F) fan fails	Increased temperature to downstream Inlet Compressor Separator Train 1 (20MBO-103) leading to potential equipment damage	Motor status indicator to alert operator	3	4	III 12	Asset				
		-	-	20TAH-1713 to alert operator	-	-	-	-				
		-	-	20TAHH-1714 to trip train 1 to close 20ESDV-1701	-	-	-	-				
2.9.2		Operator inadvertently stop Inlet Cooler Train 1 (20HAL-103A/B/C/D/E/F) fan (remotely)	Increased temperature to downstream Inlet Compressor Separator Train 1 (20MBO-103) leading to potential equipment damage	SOP	3	3	II 9	Asset				
		-	-	20TAH-1713 to alert operator	-	-	-	-				
		-	-	20TAHH-1714 to trip train 1 to close 20ESDV-1701	-	-	-	-				
2.9.3		Fouling of Compressor Inlet Cooler Train 1 (20HAL-103A/B/C/D/E/F) tubes	Increased temperature to downstream Inlet Compressor Separator Train 1 (20MBO-103) leading to potential equipment damage	10% contingency in surface area will allow for fouling	3	3	II 9	Asset				
		-	-	20TAH-1713 to alert operator	-	-	-	-				
		-	-	20TAHH-1714 to trip train 1 to close 20ESDV-1701	-	-	-	-				
2.9.4		External fire	Potential overpressurisation of Compressor Inlet Cooler Train 1 (20HAL-103A/B/C/D/E/F) and Inlet Compressor Separator Train 1 (20MBO-103)	20PSV-1701 size for fire case	4	2	II 8	Asset	#4	Review the requirement for thermal fire relief of individual Compressor Inlet Cooler Train 1 (20HAL-103A/B/C/D/E/F) or need to CDO the manual isolation valve	TPE	
2.10.1	Less Level	20LV-1705A/B stuck open	Loss of condensate level leading to gas blowby to existing Condensate Stabiliser and potential overpressurisation	20LAL-1701 to alert operator	4	3	III 12	Asset	#5	confirm that the existing PSV on the existing Condensate Stabiliser is sized for failure of 20LV-1705A/B. If not, consider to install RO to ensure gas blowby rate does not exceed PGV capacity	TPE/CPGL	Split range CV
		-	-	20LALL-1704 to close 20SDV-1704	-	-	-	-				Tag ID on 20LALL-1701 (trip) to be revised to 20LALL-1704
2.10.1	Less Level	20LV-1702A/B stuck open	Loss of interface level leading to condensate carry over to Produced Water System and eventually gas blowby to existing Degassing Column (259V-101/201 and 44MBO-301/401) and potential overpressurisation	20LAL-1702 to alert operator	3	3	II 9	Asset				
		-	-	20LALL-1702 to close 20SDV-1703	-	-	-	-				Tag ID on 20LALL-1702 (trip) to be revised to 20LALL-1703
		-	-	Degassing Column (259V-101/201 and 44MBO-301/401) is open to Thermal Oxidiser (235H-102/202) with 248BDV-2114 to open to LP Vent on pressurise in relief header	-	-	-	-				If 248BDV-2114 does not open then relief network is fitted with rupture disc
2.11.1	More Level	20SDV-1704 fails closed	Potential level build up in the Inlet Compressor Separator Train 1 (20MBO-103) leading to liquid carry over to downstream 1st Stage Inlet Compressor (23-CAE-100/200/300/400/500) and potential equipment damage	Valve status Indicator to alert operator	5	2	II 10	Asset				
		-	-	20LAH-1701 to alert operator	-	-	-	-				
		-	-	20LAHH-1701 to close 20ESDV-1701	-	-	-	-				
		-	-	Downstream Inlet Compressor Suction Scrubber (23MBF-100/200/300/400/500) to handle liquid carry over	-	-	-	-				

ITEM	GUIDE PHRASE	POSSIBLE CAUSES	CONSEQUENCES	SAFEGUARDS	S	L	R	CATEGORY	ACTION No.	ACTION	ACTIONEE	REMARKS
2.11.2		20LV-1705A/B fails closed	Potential level build up in the Inlet Compressor Separator Train 1 (20MBO-103) leading to liquid carry over to downstream 1st Stage Inlet Compressor (23-CAE-100/200/300/400/500) and potential equipment damage	20LAH-1701 to alert operator	5	2	110	Asset				
			-	20LAHH-1701 to close 20ESDV-1701	-	-	-	-				
			-	Downstream Inlet Compressor Suction Scrubber (23MBF-100/200/300/400/500) to handle liquid carry over	-	-	-	-				
2.11.3		Manual valve on condensate line inadvertently closed	Potential level build up in the Inlet Compressor Separator Train 1 (20MBO-103) leading to liquid carry over to downstream 1st Stage Inlet Compressor (23-CAE-100/200/300/400/500) and potential equipment damage	SOP	5	2	110	Asset				
			-	Refer to item 2.11.2	-	-	-	-				
2.11.4		20FT-1707 strainer blocked	Refer to item 2.11.2		5	2	110	Asset				
2.11.5		20SDV-1703 fails closed	Increase in interface level leading to water carry over to Condensate System and potential liquid carry over to downstream 1st Stage Inlet Compressor (23-CAE-100/200/300/400/500) and potential equipment damage	Valve status indicator to alert operator	5	2	110	Asset				
			-	20LAH-1702 to alert operator	-	-	-	-				
			-	20LAH-1701 to alert operator	-	-	-	-				
			-	20LAHH-1701 to close 20ESDV-1701	-	-	-	-				
2.11.6		20LV-1702A/B fails closed	Increase in interface level leading to water carry over to Condensate System and potential liquid carry over to downstream 1st Stage Inlet Compressor (23-CAE-100/200/300/400/500) and potential equipment damage	20LAH-1702 to alert operator	5	2	110	Asset				
			-	20LAH-1701 to alert operator	-	-	-	-				
			-	20LAHH-1701 to close 20ESDV-1701	-	-	-	-				
2.11.7		Manual valve on produced water line inadvertently closed	Increase in interface level leading to water carry over to Condensate System and potential liquid carry over to downstream 1st Stage Inlet Compressor (23-CAE-100/200/300/400/500) and potential equipment damage	SOP	5	2	110	Asset				
			-	Refer to item 2.11.6	-	-	-	-				
2.11.8		20FT-1705 strainer blocked	Refer to item 2.11.6		5	2	110	Personnel Safety				
2.12.1	Loss of Containment	Leak	Release of hydrocarbon to atmosphere leading to potential fire/explosion if ignited	Asset Integrity/ Flange Management System	5	2	110	Personnel Safety				
			-	20PAL-1716 to alert operator	-	-	-	-				
			-	20PAL-1701 to trip the train	-	-	-	-				
2.12.1	Loss of Containment		Potential backflow from the 1st Stage Inlet Compressor (23-CAE-100/200/300/400/500) Suction Header	Check valve provided	-	-	-	-				
2.13.1	Impurities	Mercury	Potential operator exposure to mercury	SOP - PPE	3	3	118	Personnel Safety				
2.14.1	Change in Composition / Reaction	No additional significant issues of concern identified			-	-	-	-				
2.15.1	Corrosion / Erosion	H2O content	Increased internal corrosion	Material Selection - Duplex SS for Compressor Inlet Cooler Train 1 (20HAL-103A/B/C/D/E/F); CS with internal cladding for Inlet Compressor Separator Train 1 (20MBO-103)	3	2	116	Asset				
2.16.1	Instrumentation	Failure of transmitter	Incorrect operating conditions	-	-	-	-	-	#6	Provide PG and TG in the Inlet Compressor Separator Train 1 (20MBO-103)	TPE	
2.17.1	Occupational Safety	High fluid temperature	Potential personnel injury due to hot surface	-	2	3	116	Personnel Safety	#7	Provide personnel protection from hot process fluid upstream of Compressor Inlet Cooler Train 1 (20HAL-103A/B/C/D/E/F)	TPE	
2.19.1	Start-up/ Shutdown	Opening of 20SDV-1701 against high DP	Potential damage to downstream equipment due to sudden high pressure flow	20PDHH-1701 to alert operator	4	2	118	Asset				

Page 3 of 4: the node related to cooler and separator from process plant HAZOP

ITEM	GUIDE PHRASE	POSSIBLE CAUSES	CONSEQUENCES	SAFEGUARDS	S	L	R	CATEGORY	ACTION No.	ACTION	ACTIONEE	REMARKS
			-	20PDHH-1701 to prevent opening of 20SDV-1701	-	-	-	-				
2.18.1	Operations	Remote start of Compressor Inlet Cooler Train 1 (20HAL-103A/B/C/D/E/F) fan	Potential personnel injury during maintenance	-	4	3	112	Personnel Safety	#8	Provide only local start for Compressor Inlet Cooler Train 1 (20HAL-103A/B/C/D/E/F) fan to avoid remote start during maintenance	TPE	
2.18.2		Bypass 20HV-1714 left open following start-up	Potential bypass of inlet 20ESDV-1701 during emergency	SOP - MV to be CSC as part of Valve Checklist	4	2	118	Asset				
			-	20HV-1714 to close on ESD/ EDP	-	-	-	-				
2.18.3		Online removal of 20LV-1705A/B	Shutdown of all inlet system to avoid operator exposure to high pressure from downstream condensate system		3	3	119	Business Interruption	#9	Consider to install manual valve downstream of 20LV-1705A/B to provide DBB for online removal of valve	TPE	
2.20.1	Drawings	No additional significant issues of concern identified			-	-	-	-				
2.21.1	Others	No additional significant issues of concern identified			-	-	-	-				

Page 4 of 4: the node related to cooler and separator from process plant HAZOP

References

- Abdelhamid, T. S., & Everett, J. G. (2000). Identifying Root Causes Of Constuction Accident. *Journal of Construction Engineering and Management*, 52-60.
- Adams, E. (1976). Accident causation and the management system. *Professional safety*, 26-29.
- Aeronautica Civil of the Republic of Colombia,. (1995). *Final Report of Aircraft Accident: American Airlines Flight 965*.
- Ale, B., Gulijk, C., Hanea, A., Hanea, D., Hudson, P., Lin, P.-H., & Sillema, S. (2014). Towards BBN based risk modelling of process plants. *Safety Science*, 48–56.
- API. (2016). *RP 754, Process Safety Performance Indicators for the Refining and Petrochemical Industries*. API.
- Araujo, V. E., Norte da Silva, J. M., & Silva, L. (2017). Modeling Bayesian Networks from a conceptual framework for occupational risk analysis, *Production*, 27, e20162239. doi:10.1590/0103-6513.223916
- Armstrong, D. B., Bauer, W. W., & Dukelow, D. A. (1945). Accident prevention – an essential public health service. *American Journal of Public Health*, 216–218.
- Ashby, W. (1956). *An Introduction to Cybernetics*. London: Chapman and Hall.
- Attwood, D., Khan, F., & Veitch, B. (2006). Occupational accident models—where have we been and where are we going? *Journal of Loss Prevention in the Process Industries*, 664-682.
- Ayres, R., & Rohatgi, P. (1987). Bhopal: Lessons for technological decision-makers. *Technology in Society*, 9:19-45.
- Badreddine, A., & Ben Amor, N. (2013). A Bayesian approach to construct bow tie diagrams for risk evaluation. *Process Safety and Environmental Protection*, 159–171.
- Ball, A. J. (2015). Identification of Leading Indicators for Producibility Risk in Early-Stage Aerospace Product Development. Massachusetts Institute of Technology Libraries.
- Belmonte, F., Schoen, W., & Heurley, L. (2011). Interdisciplinary safety analysis of complex socio-technological systems based on the functional resonance accident model: An application to railway traffic supervision. *Reliability Engineering and System Safety*, 237-249.
- Benner, L. (1975). Accident investigation: Multilinear events sequencing methods. *Journal of Safety Research*, 67-73.
- Bernstein, P. L. (1998). *Against the Gods: The Remarkable Story of Risk*. Wiley.
- Bird, F. E. (1974). *Management guide to loss control*. Institute Press, Atlanta, Georgia.

- Bird, F. E., & Germain, G. L. (1985). *Practical Loss Control Leadership*. International Loss Control Institute.
- Bogart, W. (1989). *The Bhopal Tragedy*. Boulder, Colo.: Westview Press.
- CCPS. (2007). *Process Safety – Leading and lagging Metrics*. Center for Chemical Process Safety (CCPS).
- CEFIC. (2011). *Guidance on Process Safety Performance Indicators*. European Chemical Industry Council.
- CGE Risk Management Solution. (2019, September 3). *CGE Academy*. Retrieved from CGE Academy: https://www.cgerisk.com/knowledgebase/The_bowtie_method
- CGE Risk Management Solutions. (2019, August 20). Retrieved from CGE Risk Management Solutions: <https://www.cgerisk.com/solutions/manage-your-barriers/barrier-management/>
- Checkland, P. (1981). *Systems Thinking, Systems Practice*. New York: John Wiley & Sons,.
- Conant, R., & Ashby, W. (1970). Every good regulator of a system must be a model of that system. *International Journal of System Science*, 89-97.
- Cook, R. (1996). Verite, Abstraction, and Ordinateur Systems in the Evolution of Complex Process Control. *3rd Annual Symposium on Human Interaction with Complex Systems (HICS 96)*. Dayton, Ohio.
- Cullen, W. D. (1990). *The Public Inquiry into the Piper Alpha Disaster*. London: Department of Energy.
- DNV GL Limited Oil & Gas. (2018). *STAMP Analysis of Management of Change - Public Report*. Manchester.
- DNV-GL. (2019, August 20). Retrieved from <https://www.dnvgl.com/software/FAQ/What-is-barrier-management-and-how-it-can-help-make-operations-predictable.html>
- Dokas, I. M., Feehan, J., & Imran, S. (2013). EWaSAP: An early warning sign identification approach based on a systemic hazard analysis. *Safety Science*, 11-26.
- Dong, A. (2012). Application of CAST and STPA to Railroad Safety In China. Massachusetts Institute of Technology.
- Edkins, G. D., & Pollock, C. M. (1996). Pro-active safety management: Application and evaluation within a rail context. *Safety Science*, 83-93.
- Edwards, W. (1962). Dynamic decision theory and probabilistic information processing. *Human Factors*, 59-73.

- Environment Directorate General of the European Commission. (2019, November 4). *Environment Directorate General of the European Commission ('DG Environment')*. Retrieved from <https://ec.europa.eu/environment/seveso/>
- e-Vision. (2019, August 20). Retrieved from e-Vision: <https://www.evision-software.com/barrier-management/>
- Ferdous, R., Khan, F., Sadiq, R., Amyotte, P., & Veitch, B. (2013). Analysing system safety and risk under uncertainty using a bow-tie diagram. An innovative approach. *Process Safety and Environmental Protection*, 1–18.
- Fleming, C. H. (2015, February). Safety-driven Early Concept Analysis. Massachusetts Institute of Technology - Submitted to the Department of Aeronautics and Astronautics in partial fulfillment of the requirements for the degree of Doctor of Philosophy.
- Forrester, J. (1961). *Industrial Dynamics*. Cambridge: MIT Press.
- Fujita, Y. (1991). What Shapes Operator Performance?, JAERI Human Factors Meeting. Tokyo.
- Godfrey, E. S. (1937). Role of the health department in the prevention of accidents. *American Journal of Public Health and the Nation's Health*, 152–155.
- Gordon, J. E. (1949). The epidemiology of accidents. *American Journal of Public Health*, 504-515.
- Haddon, W. (1980). The Basic Strategies for Reducing Damage from Hazards of All Kinds. *Hazard prevention*, 8-12.
- Hale, A., Wilpert, B., & Freitag, M. (1997). *After the Event. From Accidents to Organisational Learning*. Oxford: Pergamon.
- Hannaman, G., Spurgin, A., & Lukic, Y. (1984). *Human Cognitive Reliability Model for PRA Analysis, NUS-4531. Draft EPRI Document*. Palo Alto, CA.: Electric Power Research Institute.
- Heinrich, H. W. (1931). *Industrial accident prevention*. McGraw-Hill.
- Herrera, I., & Woltjer, R. (2010). Comparing amulti-linear(STEP) and systemic(FRAM) method for accident analysis. *Reliability Engineering and System Safety*, 1269-1275.
- Hollnagel, E. (1998). *Cognitive Reliability and Error Analysis Method (CREAM)*. New York: Elsevier Science.
- Hollnagel, E. (2004). *Barriers and Accident Prevention*. Aldershot: Ashgate Publishing Limited.
- Hollnagel, E. (2012). *FRAM: the Functional Resonance Analysis Method: Modelling Complex Socio-technical Systems*. Farnham: Ashgate.

- Hollnagel, E., & Goteman, Ö. (2004). The Functional Resonance Accident Model. *University of Linköping, SE-58183 Linköping, Sweden; Scandinavian Airlines and Linköping Institute of Technology*.
- Hollnagel, E., & Speziali, J. (2008). *Study on Developments in Accident Investigation Methods - A survey of the state of the art*. Swedish Nuclear Power Inspectorate (SKI).
- Hollnagel, E., Hounsgaard, J., & Colligan, L. (2014). *FRAM – the Functional Resonance Analysis Method – a handbook for the practical use of the method*. Southern Region of Denmark: Centre for Quality.
- Hopkins, A. (2000). *Lessons from Longford: The Esso Gas Plant Explosion*. Sydney: CCH.
- Hopkins, A. (2012). *Disastrous Decisions - The Human and Organisational Causes of the Gulf of Mexico Blowout*. CCH Australia Limited.
- Hosseinian, S. S., & Jabbarani Torghabeh, Z. (2012). Major Theories of construction accident causation models- A literature review. *International Journal of Advances in Engineering & Technology*, 53-66.
- Hovden, J., Størseth, F., & Tinmannsvik, R. K. (2011). Multilevel learning from accidents – Case studies in transport. *Safety Science*, 98-105.
- HSE UK. (2006). *HSG254, Developing process safety indicators. A step-by-step guide for chemical and major hazard industries*. UK Health and Safety Executive (HSE).
- Hudson, P. (2010). *Safety Science: It's not rocket science, it's much harder*. Delft University of Technology - faculteit Techniek, Bestuur en Management.
- IEC 61882 standard. (2016). Hazard and Operability Studies (HAZOP Studies) – Application Guide. International Electrotechnical Commission (IEC).
- IEC/ISO. (1999). Guide 51: Safety aspects - Guidelines for their inclusion in standards. IEC/ISO.
- IOPG. (2016). *Report No. 556, Process Safety - Leading key performance indicators*.
- IOPG. (2018). *Report No. 456, Process Safety - Recommended Practice on Key Performance Indicators*. International Association of Oil & Gas Producers (IOGP).
- ioshmagazine. (2019 , November 4). *ioshmagazine*. Retrieved from ioshmagazine: <https://www.ioshmagazine.com/piper-alpha-regime-changer>
- Johnson, C., & de Almeida, I. (2008). An investigation into the loss of the Brazilian space programme's launch vehicle VLS-1 V03. *Safety Science*, 38-53.

- Johnson, C., & Holloway, C. (2003). The ESA/NASA SOHO mission interruption: Using the STAMP accident analysis technique for a software related 'mishap'. *Software: Practice and Experience*, 1177-1198.
- Johnson, W. G. (1973). *The Management Oversight and Risk Tree - MORT*. Grandjean: U.S Atomic Energy Commission.
- Johnson, W. G. (1975). MORT: The Management Oversight and Risk Tree. *Journal of Safety Research*, 4-15.
- Johnson, W. G. (1980). *MORT Safety Assurance Systems*. New York: Marcel Dekker, Inc.
- Khakzad, N., Khan, F., & Amyotte, P. (2013). Dynamic safety analysis of process systems by mapping bow-tie into bayesian network. *Process Safety and Environmental Protection*, 46–53.
- Khawaji, I. A. (2012, June). Developing system-based leading indicators for proactive risk mgt in the chemical processing ind. Massachusetts Institute of Technology.
- Kjellén, U. (2000). *Prevention of accidents through experience feedback*. London and New York: Taylor & Francis.
- Kletz, T. (1982). Human problems with computer control. *Plant/Operations Progress*.
- Knegtering, B., & Pasman, H. (2013). The safety barometer How safe is my plant today? Is instantaneously measuring safety level utopia or realizable? *Journal of Loss Prevention in the Process Industries*, 821-829.
- Kontogiannis, T., & Malakis, S. (2012). A systemic analysis of patterns of organizational breakdowns in accidents: A case from helicopter emergency medical service (HEMS) operations. *Reliability Engineering & System Safety*, 193-208.
- Kujath, M., Amyotte, P., & Khan, F. (2010). A conceptual offshore oil and gas process accident model. *Journal of Loss Prevention in the Process Industries*, 323-330.
- Laracy, J. (2006). A Systems Theoretic Accident Model Applied to Biodefense. *Defense & Security Analysis*, 301–310.
- Le Coze, J. (2015). Reflecting on Jens Rasmussen's legacy. A strong program for a hard problem. *Safety Science*, 123-141.
- Le Coze, J. (2017). Reflecting on Jens Rasmussen's legacy (2) behind and beyond, a 'constructivist turn'. *Applied Ergonomics*, 558-569.
- Lee, S., Moh, Y. B., Tabibzadeh, M., & Meshkati, N. (2017). Applying the AcciMap methodology to investigate the tragic Sewol Ferry accident in South Korea. *Applied Ergonomics*, 517-525.

- Leplat, J. (1987). Occupational accident research and systems approach. *New Technology and Human Error*, 181-191.
- Leveson, N. (1995). *Safeware: System Safety and Computers*. Massachusetts.
- Leveson, N. (2015). A systems approach to risk management through leading safety indicators. *Reliability Engineering & System Safety*, 17-34.
- Leveson, N. (2017). Rasmussen's legacy: A paradigm change in engineering for safety. *Applied Ergonomics*, 581-591.
- Leveson, N. G. (2001). *Evaluating accident models using recent aerospace accidents Part1: Event-based Models*. Massachusetts Institute of Technology.
- Leveson, N. G. (2004). A new accident model for engineering safer systems. *Safety Science*, 237–270.
- Leveson, N. G. (2012). *Engineering a Safer World - Systems Thinking Applied to Safety*. Cambridge, Massachusetts: The MIT Press.
- Leveson, N. G., & Thomas, J. P. (2018). *STPA Handbook*.
- Leveson, N., & Finkelstein, S. (2016). Systems Approach to Analyzing and Preventing Hospital Adverse Events. *Journal of patient safety*.
- Markowski, A., & Kotynia, A. (2011). “Bow-tie” model in layer of protection analysis. *Process Safety and Environmental Protection*, 205–213.
- Maroño, M., Pena, J., & Santamaria, J. (2006). The ‘PROCESO’ index: a new methodology for the evaluation of operational safety in the chemical industry. *Reliability Engineering and System Safety*, 349-361.
- Miles, R. J. (1973). *Systems Concepts: Lectures on Contemporary Approaches to Systems*. New York: John F. Wiley & Sons.
- NRC. (2007). *ATHEANA’s User Guide Final Report*. NUREG-1880. Washington, D.C.: US Nuclear Regulatory Commission.
- O’Neil, M. (2014). Application of CAST to Hospital Adverse Events. Massachusetts Institute of Technology.
- OECD. (2008). *Guidance on developing safety performance indicators related to chemical accident prevention, preparedness and response*. Organization for Economic Cooperation and Development (OECD).

- OECD. (2012). *Process Safety Guide Corporate governance for process safety: Guidance for senior leaders in high hazard industries. OECD Environment, Health and Safety Chemical Accidents Programme.*
- Pasman, H., & Rogers, W. (2013). Bayesian networks make LOPA more effective, QRA more transparent and flexible, and thus safety more definable! *Journal of Loss Prevention in the Process Industries*, 434-442.
- Perrow, C. (1984). *Normal Accidents: Living With High-Risk Technologies*. New York: Basic Books, Inc.
- Petersen, D. (1971). *Techniques of Safety Management*. New York: McGraw-Hill.
- Petersen, D. (1996). *Human Error Reduction and Safety Management*. Wiley.
- Petrotechnics*. (2019, August 26). Retrieved from <https://www.petrotechnics.com/what-we-do/proscent/mah-barrier-management/>
- Press, E. (1948). Epidemiological approach to accident prevention. *American Journal of Public Health*, 1442–1445.
- Qureshi, Z. H. (2008). *A Review of Accident Modelling Approaches for Complex Critical Sociotechnical Systems (DSTO-TR-2094)*. Edinburgh South Australia 5111 Australia: Command, Control, Communications and Intelligence Division, Defence Science and Technology Organisation.
- Rasmussen, J. (1990). *Human error and the problem of causality in analysis of accidents*. Oxford: Clarendon Press.
- Rasmussen, J. (1997). Risk Management in a Dynamic Society: A Modelling Problem. *Safety Science*, 183-213.
- Rasmussen, J., & Svedung, I. (2000). *Proactive Risk Management in a dynamic society*. Karlstad: Swedish Rescue Services Agency.
- Rasmussen, J., Pejtersen, A., & Goodstein, L. (1994). *Cognitive Systems Engineering*. New York: Wiley.
- Rathnayakaa, S., Khana, F., & Amyotte, P. (2011). SHIPP methodology: Predictive accident modeling approach. Part I: Methodology and model description. *Process Safety and Environmental Protection*, 151-164.
- Rathnayakaa, S., Khana, F., & Amyotte, P. (2011). SHIPP methodology: Predictive accident modeling approach. Part II. Validation with case study. *Process Safety and Environmental Protection*, 75-88.
- Reason, J. (1990). *Human Error*. Cambridge: Cambridge University Press.

- Reason, J. (1997). *Managing the risks of organizational accidents*. Aldershot: Ashgate.
- RiskPoynt. (2019, August 26). Retrieved from <https://www.riskpoynt.com/>
- Rodriguez, M., & Diaz, I. (2016). System theory based hazard analysis applied to the process industry. *International Journal of Reliability and Safety*, 72-86.
- SAFETEC. (2019, August 26). Retrieved from <https://www.safetec.no/en/services/risk-management/barrier-management/>
- Salmon, P., Cornelissen, M., & Trotter, M. (2012). Systems-based accident analysis methods- A comparison of Accimap, HFACS, and STAMP. *Safety Science*, 1158–1170.
- Salmon, P., Williamson, A., Lenne, M., Mitsopoulos, E., & Rudin-Brown, C. (2010). Systems-based accident analysis in the led outdoor activity domain: application and evaluation of a risk management framework. *Ergonomics*, 927–939.
- Samadi, J. (2012, December 14). Development of a Systemic Risk Management Approach for CO2 Capture, Transport and Storage Projects. Crisis and Risk research Center (CRC) of MINES ParisTech.
- Suokas, J. (1985). *On the reliability and validity of safety analysis, Technical Report Publications 25*. Espoo, Finland: Technical Research Center of Finland.
- Svenson, O. (1991). The accident evolution and barrier function (AEB) model applied to incident analysis in the processing industries. *Risk Analysis*, 499-507.
- Svenson, O. (2000). *Accident Analysis and Barrier Function (AEB) method - Manual for incident analysis*. Swedish Nuclear Power Inspectorate (SKI).
- Swain, A. (1987). *Accident Sequence Evaluation Program Human Reliability Analysis Procedure. NUREG/CR-4772/SAND86-1996*. Washington, DC.: Sandia National Laboratories, U.S. Nuclear Regulatory Commission.
- Swain, A., & Guttman, H. (1983). *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. NUREG/CR-1278*. Washington, D.C.: U.S. Nuclear Regulatory Commission.
- Toft, Y., & Dell, G. (2012). *Models of Causation: Safety*. Tullamarine: In HaSPA (Health and Safety Professionals Alliance), The Core Body of Knowledge for Generalist OHS Professionals Safety Institute of Australia.
- Turner, B. (1978). *Man-made disasters*. London: Wykeham.
- U.S. Chemical Safety and Hazard Investigation Board (CSB), Final Investigation Report, Report No. 2012-03-I-CA. (2015). *Chevron Richmond Refinery, Pipe Rupture and Fire, August 6, 2012*.

- U.S. Chemical Safety and Hazard Investigation Board (CSB), Interim Investigation Report. (2013). *Chevron Richmond Refinery Fire, August 6, 2012*, .
- U.S. Chemical Safety and Hazard Investigation Board (CSB), Regulatory Report, Report No. 2012-03-I-CA. (2014). *Chevron Richmond Refinery, Pipe Rupture and Fire, August 6, 2012*.
- U.S. Department of Energy. (2012). Accident and Operational Safety Analysis - Volume I: Accident Analysis Techniques. Washington, D.C. 20585.
- Underwood, & Waterson. (2013). *Accident Analysis Models and Methods - Guidance for Safety Professionals*. Loughborough: Loughborough University.
- Underwood, P., & Waterson, P. (2012). Advances in Human Aspects of Road and Rail Transportation. CRC Press, Editors: Neville Stanton.
- Vicente, K. (1995). *A Field Study of Operator Cognitive Monitoring at Pickering Nuclear Generating Station, Technical Report CEL 9504*. Cognitive Engineering Laboratory, University of Toronto.
- Vicente, K. (1999). *Cognitive Work Analysis: Toward Safe, Productive, and Healthy Computer Based Work*. Erlbaum Associates.
- Villa, V., & Cozzani, V. (2016). Application of bayesian networks to quantitative assessment of safety barriers' performance in the prevention of major accidents. *Chemical Engineering Transactions*, 151-156. doi:10.3303/CET1653026
- Viner, D. (1991). *Accident analysis and risk control*. Melbourne: Derek Viner Pty Ltd.
- Wagenaar, W., & P.T.W., H. (1987). *The analysis of accidents with a view to prevention. Report for Shell International SIPM*. The Hague: Department of Experimental Psychology, Leiden University, The Netherlands.
- Waterson, P., Le Coze, J.-C., & Andersen, H. B. (2017). Recurring themes in the legacy of Jens Rasmussen. *Applied Ergonomics*, 471-482.
- Weaver, D. A. (1971). Symptoms of operational error. *Professional Safety*.
- Weber, P., Medina-Oliva, G., Simon, C., & lung, B. (2012). Overview on Bayesian networks applications for dependability, risk analysis and maintenance areas. *Engineering Applications of Artificial Intelligence*, 671-682.
- Wiegmann, D., & Shappell, S. (2003). *A Human Error Approach to Aviation Accident Analysis: The Human Factors Analysis and Classification System*. Burlington, VT.: Ashgate Publishing Company.

- Williams, J. (1988). A data-based method for assessing and reducing human error to improve operational performance. *IEEE Conference on Human Factors in Power Plants*. Monterey California.
- Woods, D. (1984). Some results on operator performance in emergency events. *Ergonomic Problems in Process Operations, Institute of Chemical Engineering Symposium, Ser. 90*.
- Woods, D. (2000). Lessons from beyond human error: Designing for resilience in the face of change and surprise. *Design for Safety Workshop*. NASA Ames Research Center.
- Xie Xuecai, F. G., Li Zonghan, J. Q., & Ge Ying, C. P. (2020). The development history of accident causation models in the past 100years: 24Model, a more modern accident causation model. *Process Safety and Environmental Protection*, 47–82.