U.S. CHEMICAL SAFETY AND HAZARD INVESTIGATION BOARD

INVESTIGATION REPORT

CATASTROPHIC RUPTURE OF HEAT EXCHANGER (SEVEN FATALITIES)

TESORO ANACORTES REFINERY

ANACORTES, WASHINGTON
APRIL 2, 2010

KEY ISSUES

- INHERENTLY SAFER DESIGN
- TESORO PROCESS SAFETY CULTURE
- CONTROL OF NONROUTINE WORK
- MECHANICAL INTEGRITY INDUSTRY STANDARD DEFICIENCIES
- REGULATORY OVERSIGHT OF PETROLEUM REFINERIES

REPORT 2010-08-I-WA
JANUARY 2014

Draft for Public Comment

[This page left intentionally blank.]

Table of Contents

List of Figures

Acronyms and Abbreviations

^{o}F	degrees Fahrenheit
AcciMap	Accident Map
ALARP	As Low As Reasonably Practicable
AIHA	American Industrial Hygiene Association
ANSI	American National Standards Institute
API	American Petroleum Institute
API RP 571	API RP 571—Damage Mechanisms Affecting Fixed Equipment in the Refining Industry
API RP 580	API RP 580—Risk-Based Inspection
API RP 581	API RP 581—Risk-Based Inspection Technology
API RP 941	API RP 941—Steels for Hydrogen Service at Elevated Temperatures and Pressures in Petroleum Refineries and Petrochemical Plants
API RP[1]	API Recommended Practices. API standards that communicate recognized industry practices. Recommended practices (RPs) may include both mandatory and non-mandatory requirements. *Shall:* As used in a standard, “shall” denotes a minimum requirement in order to conform to the standard. *Should:* As used in a standard, “should” denotes a recommendation or that which is advised but not required in order to conform to the standard.
API Standard[2]	API Standards include Specifications, Recommended Practices, Standards, and Codes. Standards combine elements of both specifications and recommended practices. “Standard” is also a broad term covering all API documents that have been developed in accordance with API procedures for standards development.
API TR 941	API Technical Report 941—The Technical Basis Document for API RP 941
APOSC	Assessment Principles for Offshore Safety Cases
ASNT	American Society for Nondestructive Testing
AUBT	Advanced Ultrasonic Backscatter Technique
bpd	Barrels Per Day
CAA	Clean Air Act

1 http://www.api.org/publications-standards-and-statistics/~/media/Files/Publications/FAQ/2011-Procedures-Final.ashx *API Procedures for Standards Development.* 2011; p 3.

2 *Ibid* at pp 2-3.

Cal/OSHA	California Occupational Safety and Health Administration
CCPS	Center for Chemical Process Safety (American Institute of Chemical Engineers)
CFR	Code of Federal Regulations
CSB	U.S. Chemical Safety and Hazard Investigation Board
CSHO	Compliance Safety and Health Officer
DCS	Distributed Control System
DOSH	Division of Occupational Safety and Health (within Washington L&I)
DMHR	Damage Mechanism Hazard Review (also known as a corrosion review)
EPA	U.S. Environmental Protection Agency
HAZ	Heat Affected Zone
HSE	Health and Safety Executive
HTHA	High Temperature Hydrogen Attack
IOW	Integrity Operating Window
IST	Inherently Safer Technology
L&I	Washington State Department of Labor & Industries
MOC	Management of Change
MOOC	Management of Organizational Change
MSDS	Material Safety Data Sheet
NDE	Nondestructive Examination
NDT	Nondestructive Testing
NEJAC	National Environmental Justice Advisory Council
NEP	OSHA Petroleum Refinery Process Safety Management National Emphasis Program
NHT	Catalytic Reformer / Naphtha Hydrotreater Unit
NIST	National Institute of Standards and Technology
OSHA	U.S. Occupational Safety and Health Administration
OSHAct	Occupational Safety and Health Act of 1970, 29 U.S.C. 667
PHA	Process Hazard Analysis
PQV	PSM Program Quality Verification Inspection—referenced in OSHA's 1994 PSM Compliance Directive[3]
PSIA	Pounds Per Square Inch Absolute

[3] OSHA Instruction CPL 2-2.45A CH-1 September 13, 1994 Directorate of Compliance Programs, 29 CFR 1910.119, Process Safety Management of Highly Hazardous Chemicals -- Compliance Guidelines and Enforcement Procedures. https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=DIRECTIVES&p_id=1559 (accessed December 28, 2013).

PSIG	Pounds Per Square Inch Gauge
PSM	Process Safety Management
PSM Standard	OSHA Process Safety Management of Highly Hazardous Chemicals Standard, 29 CFR §1910.119
PWHT	Post-Weld Heat Treatment
RAGAGEP	Recognized and Generally Accepted Good Engineering Practice
RBI	Risk-Based Inspection
RMP	Risk Management Plan (EPA), as defined in U.S.C. Section 42, Chapter 85, Subchapter I, Part A, Section 7412(r)
RP	Recommended Practice (API)
S-Scan	Sectorial Scan
SS	Stainless Steel
TOP	Triangle of Prevention
UK	United Kingdom
USW	United Steelworkers Union
UT	Ultrasonic Technique
WAC	Washington Administrative Code
WFMT	Wet Fluorescent Magnetic Particle Testing

1.0 Executive Summary

1.1 Incident Summary

On April 2, 2010, the Tesoro Refining and Marketing Company LLC ("Tesoro") petroleum refinery[4] in Anacortes, Washington ("the Tesoro Anacortes Refinery"), experienced a catastrophic rupture of a heat exchanger in the Catalytic Reformer / Naphtha Hydrotreater unit ("the NHT unit"). The heat exchanger, known as E-6600E ("the E heat exchanger"), catastrophically ruptured because of High Temperature Hydrogen Attack (HTHA).[5] Highly flammable hydrogen and naphtha at more than 500 degrees Fahrenheit (ºF), were released from the ruptured heat exchanger and ignited,[6] causing an explosion and an intense fire that burned for more than three hours. The rupture fatally injured seven Tesoro employees (one shift supervisor and six operators) who were working in the immediate vicinity of the heat exchanger at the time of the incident. To date, this is the largest fatal incident at a US petroleum refinery since the BP Texas City accident in March 2005.[7]

The NHT unit at the Tesoro Anacortes Refinery contained two parallel groups, or banks, of three heat exchangers (A/B/C and D/E/F) used to preheat process fluid before it entered a reactor, where impurities were treated for subsequent removal. The E heat exchanger was constructed of carbon steel.[8] A schematic of the six heat exchangers is illustrated in Figure 1.

At the time of the release, the Tesoro workers were in the final stages of a startup activity to put the A/B/C bank of heat exchangers back in service following cleaning. The D/E/F heat exchangers remained in service during this operation. Because of the refinery's long history of frequent leaks and occasional fires during this startup activity, the CSB considers this work is to be hazardous and nonroutine.[9] While the operations staff was performing the startup operations, the E heat exchanger in the middle of the operating D/E/F bank catastrophically ruptured.

---

4 Tesoro purchased all of the Shell Oil Company's stock in the Shell Anacortes Refining Company in 1998. Approximately 350 employees work at the Anacortes refinery and 185 of them are operations and maintenance workers who are represented by the United Steelworkers union (USW).

5 HTHA is a damage mechanism that results in fissures and cracking and occurs when carbon steel equipment is exposed to hydrogen at high temperatures and pressures.

6 The autoignition temperature of a material is defined as the temperature at which it will ignite spontaneously on contact with oxygen, without spark or flame. The Tesoro Material Safety Data Sheet (MSDS) for naphtha listed autoignition temperature as 437 ºF. As the process temperature was more than 500 ºF, autoignition was likely.

7 The 2005 BP Texas City incident resulted in 15 fatalities and 180 injuries.

8 The portion of the E heat exchanger that failed was constructed of carbon steel. The details of the exchanger materials are addressed in Section 4.2.1, NHT Heat Exchanger Construction.

9 Nonroutine does not refer to the frequency at which the activity occurs. Nonroutine refers to whether the activity is part of the normal sequence of converting raw materials to finished products. Startup is considered a nonroutine activity. Center for Chemical Process Safety (CCPS), *Guidelines for Risk Based Process Safety*. 2007; p 286.

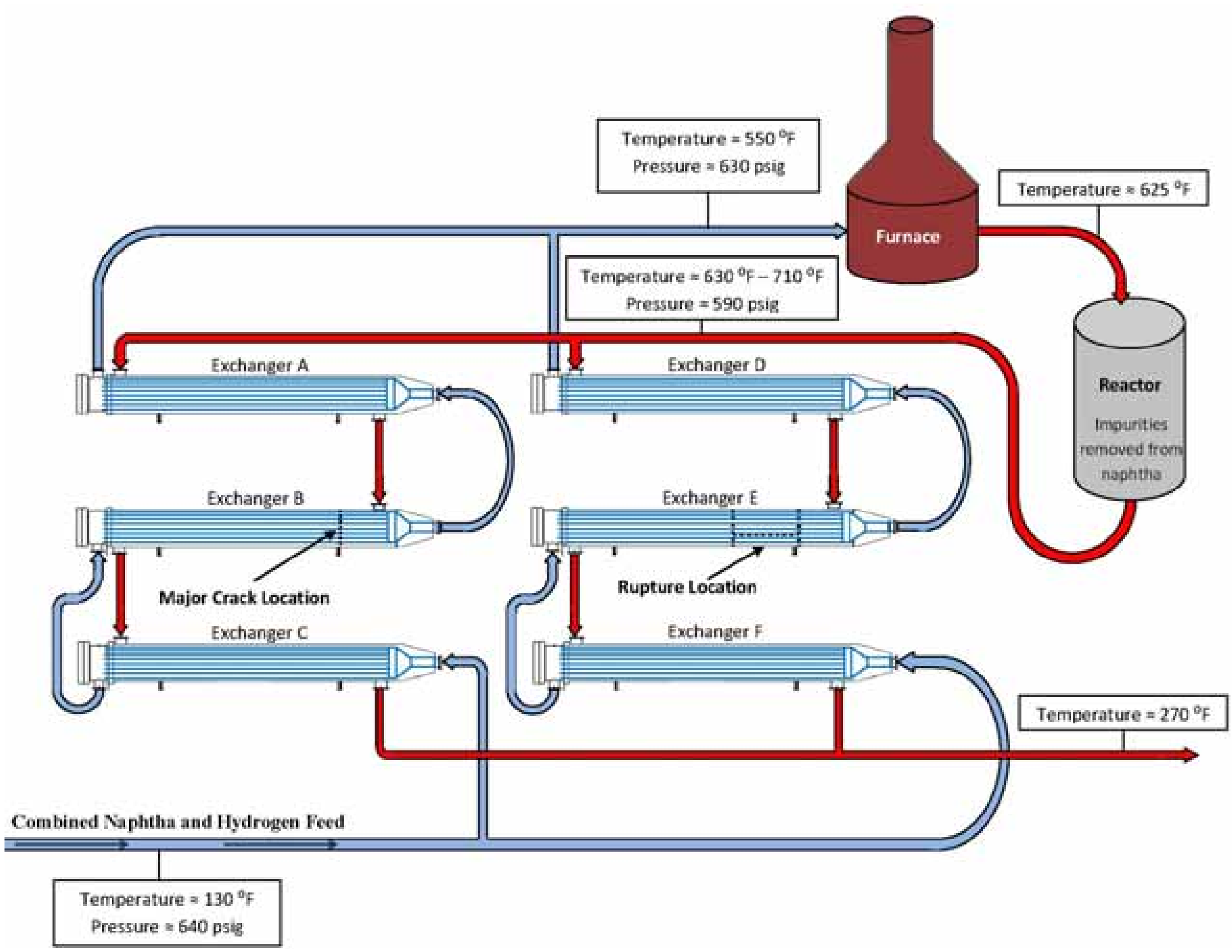


Figure 1. Schematic of the Tesoro Anacortes Refinery NHT Unit Heat Exchangers. There are two banks of three heat exchangers: A/B/C bank and D/E/F bank. The E heat exchanger catastrophically ruptured on April 2, 2010.

1.2 Key Findings

1.2.1 Technical Findings

1. The rupture of the E heat exchanger was the result of the carbon steel heat exchanger being severely weakened by a damage mechanism known as HTHA. The B heat exchanger did not fail, but was constructed with the same materials and operated under the same conditions as the E heat exchanger. The B heat exchanger was also severely weakened by HTHA damage. HTHA is a damage mechanism that results in fissures and cracking and occurs when carbon steel equipment

is exposed to hydrogen at high temperatures and pressures.[10] The resulting damage severely degrades the mechanical properties of the steel.[11] (Section 4.1)

2. HTHA can accumulate in high-stress areas in carbon steel, such as non-post-weld heat-treated welds. The welds of the B and E carbon steel heat exchangers were not post-weld heat-treated. The high stress areas near the welds of these heat exchangers were found to contain HTHA damage. The rupture location of the E heat exchanger was along these high-stress weld regions and was attributable to cracks caused by HTHA. (Sections 4.1.2 and 4.2.1)

3. In 1970, the American Petroleum Institute (API) published API Recommended Practice (RP) 941 *Steels for Hydrogen Service at Elevated Temperatures and Pressures in Petroleum Refineries and Petrochemical Plants*. This document provides Nelson curves to predict the occurrence of HTHA in various materials of construction as a function of temperature and hydrogen partial pressure.[12] The Nelson curves are predicated on past equipment failure incidents and are plotted based on self-reported process conditions that are ill-defined and lack consistency. (Section 4.4.1.1)

4. The CSB performed computer reconstruction[13] of the process conditions within the NHT heat exchangers. The results of the computer reconstruction show that the portion of the carbon steel E heat exchanger that ruptured was estimated to have operated below the applicable Nelson curve. This was considered the safe region of operation where HTHA could not occur. Therefore, the carbon steel Nelson curve methodology is inaccurate, cannot be depended on to prevent HTHA equipment failures, and cannot be reliably used to predict the occurrence of HTHA equipment damage. (Section 4.4.1.1)

5. The hottest portion of the B and E heat exchangers was clad with stainless steel, which improved resistance to HTHA. On the basis of CSB computer reconstruction of the process conditions in the heat exchangers, the CSB estimates that this stainless steel-clad portion of the heat exchangers operated at process conditions that were at times above the carbon steel Nelson curve. However, the unclad portion where the rupture of the E heat exchanger occurred, and where HTHA existed in the B and E heat exchangers, was estimated to have operated below the Nelson curve. (Sections 4.2.1 and 4.4.1.2)

---

[10] McIntyre, Vogelsange, *Progress in Corrosion- The First 50 Years of the EFC;* Maney Publishing 2009*;* Section 12.5.1.

[11] Shih, H.M. and Johnson, H.H. A *Model Calculation of the Nelson Curves for Hydrogen Attack;* Acta Metallurgica, Volume 30. 1982; pp 537-545.

[12] Hydrogen partial pressure is a calculated parameter. It is the pressure that would be exerted by a single component of a gas mixture. For example, the hydrogen partial pressure of a 500 psia gas mixture in a vessel that contains 50 mol% hydrogen and 50 mol% propane equals 250 psia.

[13] The CSB modeled the exchanger process conditions using Aspen HYSYS® and Aspen Exchanger Design and Rating. The model required the use of several assumptions, such as fouling distribution, because of a lack of both process and fouling data gathered by Tesoro. As a result, all model results are estimates. Due to limitations in historical data, modeling estimates were limited to 2007-2010. See Appendix C for a detailed description of the modeling assumptions and results.

6. It is very difficult to inspect for HTHA because the damage might not be detected; it can be microscopic and may be present only in small localized areas of equipment. In addition, equipment must already be damaged by HTHA for equipment inspection to identify HTHA. Successful identification of HTHA is highly dependent on the specific techniques employed and the skill of the inspector, and there are few inspectors who have this expertise. Inspection is therefore not sufficiently reliable to ensure mechanical integrity and prevent HTHA equipment damage. (Section 4.1.4)

7. Equipment inspections and post-weld heat treating rely on procedures and human implementation, which are low on the hierarchy of controls[14] and thus are weaker safeguards to prevent HTHA failures than the use of materials that are not susceptible to HTHA damage. (Section 4.1.2)

8. Inherently safer design is a better approach to prevent HTHA. API has identified high chromium steels that are significantly more resistant to HTHA than carbon steel. The B and E heat exchangers were not constructed from these inherently safer materials. (Sections 4.1.3 and 4.1.4)

1.2.2 Organizational Findings

9. The startup of the NHT heat exchangers was hazardous nonroutine work. Leaks routinely developed that presented hazards to workers conducting the startup activities. Process Hazard Analyses (PHAs) [15] at the refinery repeatedly failed to ensure that these hazards were controlled and that the number of workers exposed to these hazards was minimized. (Section 5.2.3)

10. The Shell Anacortes Refining Company was owned and operated by the Shell Oil Company ("Shell Oil") prior to 1998. The 1996 Shell Oil NHT unit PHA simply cited ineffective, non-specific, judgment-based, qualitative safeguards to prevent equipment failure from HTHA. However, the effectiveness of these safeguards was neither evaluated nor documented; instead the PHA merely listed general safeguards. Had the adequacy of the safeguards been verified, improved safeguards intended to protect against HTHA failure could have been recommended. The 2001 and 2006 Tesoro PHA revalidations did not address or modify the analysis performed

[14] An effectiveness ranking of techniques used to control hazards and the risk they represent can be described as a hierarchy of controls – the higher up (further left) on the hierarchy, the more effective the risk reduction achieved (Figure 17).

[15] A PHA is a hazard evaluation to identify, evaluate, and control the hazards of a process. Facilities that process a threshold quantity of hazardous materials, such as the Tesoro Anacortes Refinery, are required to conduct a PHA per the Washington Administrative Code (WAC) Title 296 Chapter 67, Safety standards for process safety management of highly hazardous chemicals (1992). *See:* http://apps.leg.wa.gov/wac/default.aspx?cite=296-67 (accessed September 29, 2013) PHAs are also required by the federal EPA Risk Management Program.

in the 1996 Shell Oil PHA. The Tesoro 2010 NHT unit PHA failed to identify HTHA as a hazard for the shell of the B and E heat exchangers.[16] (Sections 5.3.4.1, 5.3, and Appendix D)

11. For the 15 years before the April 2010 incident, assumptions used by PHA teams at the Anacortes refinery contributed to ineffective safeguards, ineffective hazard identification, and ineffective control of hazards to prevent equipment failures from HTHA damage, such as the E heat exchanger in the NHT unit.[17] (Section 5.3.4.1 and Appendix D)

12. Shell Oil completed a PHA in 1995 related to process modifications that could increase the hydrogen partial pressure in the NHT heat exchangers. However, when managing this change no consideration, evaluation, or recommendations were made to address the potential for HTHA damage to the NHT heat exchangers. (Section 5.3.4 and Appendix D)

13. Shell Oil and Tesoro periodically performed damage mechanism hazard reviews (DMHRs), called corrosion reviews. However, these reviews did not identify HTHA as a credible failure mechanism for the B and E heat exchangers. These reviews were weakened by primarily relying on design operating data for these heat exchangers rather than data from actual process operating conditions.[18] (Section 5.3.3 and Appendix D)

14. Tesoro did not monitor actual operating conditions of the B and E heat exchangers within the NHT heat exchanger banks, even though it would have been technically feasible to do so. Rather, corrosion experts hired by Tesoro primarily relied on design operating conditions that when evaluated using the Nelson curve indicated lower susceptibility to HTHA damage than the operating conditions estimated by CSB models.[19] The use of the design temperatures contributed to the incorrect conclusion that the heat exchangers were not susceptible to damage from HTHA. As a result, Tesoro was not aware that the hottest section of the B and E heat exchangers (Can

[16] The term “shell” in this context refers to the pressure containing carbon steel wall of the heat exchanger. The 2010 Tesoro NHT unit PHA did identify HTHA as a possible hazard for the tube side of the B and E exchangers. Heat exchangers of this design have process flow through two sides, separated by mechanical design. Heat is transferred from one side to the other to exchange heat. Flow on the inside of the tubes through the heat exchanger is commonly referred to as “tube-side,” while flow on the outside of the tubes is called “shell-side.” The B and E exchangers had HTHA damage to the pressure containing portion on the shell-side. The 2010 Tesoro NHT unit PHA did not identify HTHA as a hazard where HTHA occurred on the shell-side of the exchanger.

[17] Tesoro issued a new PHA procedure in 2012 that removed the list of assumptions that had previously limited the PHA teams’ analyses. Now, the PHA procedure requires that all assumptions can and should be challenged at any point in the PHA process. Furthermore, if a credible challenge is made, the assumption is eliminated for the duration of the study. This change to Tesoro’s PHA procedure should help ensure that process safety hazards and proposed safeguards are more effectively evaluated in the future.

[18] Design operating conditions include estimated and calculated conditions used to design the exchangers and the thermal profile developed.

[19] Tesoro hired corrosion experts to evaluate damage mechanisms at the Anacortes refinery. These external experts were not Tesoro employees.

4)[20] at times likely operated above the carbon steel Nelson curve. If Tesoro had measured or otherwise technically evaluated the actual operating conditions of these heat exchangers, existing company procedures required HTHA inspection.[21] Although HTHA may have been identified, inspection for HTHA is not sufficiently reliable. (Sections 5.3.3.1, 4.1.4, and Appendix D)

15. Tesoro procedures did not prohibit or effectively limit the use of additional personnel during the nonroutine hazardous startup of the NHT heat exchangers. The heat exchanger startup procedure specifies the use of only one outside operator to perform startup operations of the NHT heat exchanger banks. However on the day of the incident, a supervisor requested five additional operators to assist with the startup of the A/B/C heat exchanger bank. (Section 5.2.3)

16. The NHT heat exchangers frequently leaked flammable hydrocarbons during startup, sometimes resulting in fires. Tesoro management had been complacent about these hazardous leaks and did not always investigate the cause of the leaks. Tesoro did take some actions to prevent the leaks, but these actions did not effectively prevent the leaks before the April 2010 incident. Additional operators, such as those present during the April 2010 heat exchanger startup, were frequently needed during startup of the NHT heat exchanger banks to respond to potential hydrocarbon leaks or fires. This past practice contributed to the presence of the six additional workers in the unit during the April 2010 incident. (Sections 5.1 and 5.2)

17. The NHT heat exchanger banks were designed with large, difficult-to-manipulate manual block valves on different levels of the NHT heat exchanger structure. These valves were used to start up the NHT heat exchanger banks and typically required numerous adjustments to maintain temperature specifications. The difficulties with valve operation during startup typically resulted in the need for additional operator assistance. This past practice contributed to the presence of some of the six additional workers in the NHT unit during the April 2010 incident.[22] (Section 5.2.3)

18. The CSB found several indications of process safety culture deficiencies at the Tesoro Anacortes Refinery. Refinery management had normalized the occurrences of hazardous conditions, including frequent leaks from the NHT heat exchangers, by using steam to mitigate leaks, ineffectively correcting heat exchanger design issues, commonly requiring additional operators

[20] The general construction of each heat exchanger shell consisted of a series of four steel sections, called “Cans” welded to form a cylinder (exchanger shell). This construction required a longitudinal weld to form each “Can” or section, and three circumferential welds to join the four sections end to end. The temperature profile is such that Can 1 is the coolest and temperature increase towards the hottest section at Can 4.

[21] Tesoro’s inspection procedure would have required HTHA inspection if operating conditions were found to be within 25 pounds per square inch absolute (psia) or 25 ºF of the Nelson curve.

[22] The new design of the NHT heat exchangers has eliminated the need to clean the exchangers while the unit is operating. Post-incident, Tesoro performed a study to evaluate hazardous equipment that is cycled more frequently than the unit. This study took two months to complete and resulted in 53 recommendations. One of the recommendations is intended to ensure that a hazard review is conducted before cycling equipment that was not included in this study.

during NHT heat exchanger startups, and exceeding the staffing levels that procedures specified. (Section 5.0)

19. The refinery process safety culture required proof of danger rather than proof of effective safety implementation. For years, technical experts used design data to evaluate the B and E heat exchangers for HTHA susceptibility. Data for actual operating conditions were not readily available, and these technical experts were not required to prove safety effectiveness in reaching their conclusion that the B and E heat exchangers were not susceptible to HTHA damage. (Section 5.0)

1.2.3 Industry Codes and Standards Findings

20. *API RP 941 - Steels for Hydrogen Service at Elevated Temperatures and Pressures in Petroleum Refineries and Petrochemical Plants* is written permissively such that there are no minimum requirements to prevent HTHA failures. Currently API RP 941 uses the term "should" 27 times and the word "shall" only once. As used in a standard, "shall" denotes a minimum requirement to conform to the standard, while "should" denotes a recommendation that is advised but not required to conform to the standard. API RP 941 does not require users to verify actual operating conditions when establishing operating limits or to confirm that the selection of construction materials will prevent HTHA. (Section 6.1.1)

21. API RP 941 provides industry guidance to predict the occurrence of HTHA in various materials of construction by using the Nelson curves. The creation of these curves was based on industry experience; the curves are purely empirical, and there is no fundamental scientific basis underlying the positions and shapes of the curves. Some members of the refining industry erroneously apply these curves as sharply defined lines of demarcation that function as boundaries where HTHA can (and cannot) occur. (Sections 4.1.1 and 6.1.3)

22. The CSB has learned of at least eight recent refinery incidents where HTHA reportedly occurred below the carbon steel Nelson curve. In 2011, API issued an industry alert on HTHA in refinery service.[23] The API alert noted multiple incidents of carbon steel equipment at operating conditions where carbon steel was previously thought to be resistant to HTHA. These refinery incidents and the subsequent API response strongly suggest an industry-wide problem with the carbon steel Nelson curve. (Section 6.1.4.2)

23. The CSB found that the carbon steel Nelson curve is inaccurate and cannot be relied on to prevent HTHA equipment failures or accurately predict HTHA equipment damage. (Section 6.1.4)

24. API RP 941 does not require industry to use inherently safer materials to prevent HTHA failures. (Section 6.1.1)

---

[23] *See*: http://www.api.org/publications-standards-and-statistics/hidden-pages/industry-alert (accessed January 19, 2014).

25. API RP 581*: Risk-Based Inspection Technology* allows users to calculate a damage factor to determine the HTHA susceptibility of various materials of construction. Tesoro hired damage mechanism experts to help ensure that damage mechanism hazards were properly identified. API RP 581 does not require users to verify actual operating conditions when determining applicable damage mechanisms. The calculation for carbon steel using the design conditions applied in damage mechanism reviews results in the conclusion that the B and E heat exchangers had a "Low Susceptibility" to HTHA. The API RP 581 calculation is therefore unreliable for preventing HTHA failure or predicting the probability of HTHA damage in carbon steel equipment. (Section 6.2)

26. API RP 581*: Risk-Based Inspection Technology* is written permissively, so that there are no minimum requirements to prevent HTHA failures. There are 19 uses of "shall" in RP 581, but none is substantive—nearly all the uses of "shall" are in formulas or requirements for damage factor or inspection effectiveness calculations that are themselves non-mandatory. There are three uses of "shall" in the HTHA section, but they are again used for calculations that are not required, preceded by language such as "the following procedure may be used" or if HTHA is detected, "fitness for service should be performed." An instructive example of the permissiveness of API RP 581 is the important guidance that the document provides for conditions that would make equipment susceptible to HTHA damage. However, if the equipment is identified as meeting the criteria that would indicate HTHA is a credible damage mechanism, according to API RP 581 guidance, the equipment "should" be evaluated for HTHA susceptibility.[24] (Section 6.2)

1.2.4 Regulatory Findings

27. Despite the fact that the nation's roughly 150 petroleum refineries represent only a small fraction of the thousands of chemical processing facilities throughout the United States, the CSB has noted a considerable frequency of significant and deadly incidents at refineries over the last decade. In 2012 alone, the CSB tracked 125 significant incidents at US petroleum refineries.[25] (Section 7.1)

28. The draft CSB Chevron Regulatory Report recommends that the state of California improve the oversight of petroleum refineries by adopting the "safety case"[26] approach. The California

[24] API RP 581, *Risk-Based Inspection Technology.* 2008; pp 252-258.

[25] These incidents were reported to the Department of Energy or the National Response Center and were examined by the CSB Incident Screening Department. The CSB has concluded that incidents that result in disruptions to the national energy supply, produce serious injuries, or receive high levels of media attention are all significant.

[26] The objective of a safety case is to demonstrate to the regulatory authority that a company is fully aware of the hazards associated with its operations and that they are conducted safely so that employees and the public are not exposed to undue risks. The regulatory authority must examine the safety case and communicate the results of its examination to the facility. The safety case requires that regulatory agencies have the expertise needed to assess the adequacy of the analysis. *See* the CSB Reactive Hazards report http://www.csb.gov/assets/1/19/ReactiveHazardInvestigationReport.pdf and the CSB Chevron Regulatory Report

Governor's Interagency Task Force on Refinery Safety has committed to study the safety case. In the draft Chevron Regulatory Report, the CSB concluded that the existing regulatory regimes for onshore petroleum refineries in the United States and California: (Appendix F)

a. Rely on a safety and environmental management system framework that is primarily activity-based rather than goal-based risk reduction to as low as reasonably practicable (ALARP) or equivalent.

b. Are static, unable to adapt to innovation and advances in the management of major hazard risks.

c. Place the burden on the regulator to verify compliance with the regulations rather than shifting the burden to industries by requiring duty holders to effectively manage the risks they create and also ensure regulator acceptance of their plans for controlling those risks.

d. Do not effectively incorporate lessons learned from major accidents; nor do they have the regulatory authority to require duty holders to address newly-identified safety issues resulting from such incidents.

e. Do not effectively collect or promote industry use of major accident performance indicators to drive industry to reduce risks to ALARP.

f. Do not require the use or implementation of inherently safer systems analysis or hierarchy of controls.

g. Do not effectively involve the workforce in hazard analysis and prevention of major accidents.

h. Do not provide the regulator with the authority to accept or reject a company's hazard analysis, risk assessment, or proposed safeguards; and

i. Do not employ the requisite number of staff members with the technical skills, knowledge, and experience necessary to provide sufficient direct safety oversight of petroleum refineries.

29. The Washington State Department of Labor and Industries (L&I), which oversees workplace safety in the state, does not have sufficient personnel resources to verify that process safety management (PSM) requirements are being implemented adequately. L&I enforces state PSM requirements that are based on the federal OSHA PSM standard for hazardous chemical facilities. However, the state of Washington has only four PSM specialists in its compliance section to regulate and inspect nearly 270 PSM-covered facilities, including five petroleum refineries. Of these four specialists only one is a chemical engineer. (Section 7.2)

30. Washington L&I completed an audit of the Tesoro NHT unit under the refinery National Emphasis Program (NEP) in March 2009, one year before the incident. The Tesoro Anacortes NEP audit is noteworthy, as it was the only audit conducted pursuant to the federal OSHA NEP

http://www.csb.gov/assets/1/19/Chevron_Regulatory_Report_Draft_for_Public_Comment_12162013.pdf (accessed December 27, 2013).

that focused on a unit that subsequently experienced a catastrophic accident that the CSB has investigated. The heat exchanger that failed, the E heat exchanger, was a fundamental component of the Tesoro NEP audit. However, no citable mechanical integrity or other process safety management deficiencies related to the heat exchanger were found. (Section 7.3.3.1)

31. Shell Oil and Tesoro PHAs conducted on the NHT unit cited non-specific, judgment-based qualitative safeguards that in light of the April 2010 incident were not effective. Following the April 2010 incident the L&I Division of Occupational Safety and Health (DOSH) issued citations to Tesoro relating to its PHA program, but they were not associated with evaluating the effectiveness of safeguards such as the robustness of the HTHA prevention program. If the Washington PSM standard had required an evaluation and documentation of safeguard effectiveness, Shell Oil and Tesoro would have been obligated to conduct such an analysis. (Section 7.4)

32. In the 2006 Tesoro NHT unit PHA, Tesoro discontinued a review of its corrosion control program and a specific mechanical integrity checklist associated with the corrosion program after concluding that they were "not a legal requirement." The state of Washington PSM regulation did not require this review. Tesoro conducted the optional review ineffectively and then terminated it when the company determined that it was not strictly required. By shifting the responsibility for risk management to the duty holder, the safety case would require continual risk reduction and performance of an effective DMHR. This review is not just an activity but must meet the goal of preventing equipment failures. (Sections 5.3.4 and 7.2.1)

33. Under the existing US and Washington regulatory systems, including the PSM standard and the U.S. Environmental Protection Agency (EPA) Risk Management Program (RMP), there is no requirement to reduce risks to a specific risk target such as ALARP, which is a hallmark of the safety case regulatory regime widely used overseas. While the Clean Air Act (CAA) directed the EPA to promulgate the RMP regulations "to provide, to the greatest extent practicable, for the prevention and detection of accidental releases of regulated substances,"[27] there is no RMP ALARP requirement. Under both the PSM and RMP regulations, an employer must "control" hazards when conducting a PHA of a covered process. However, there is no requirement to address the effectiveness of the controls or to use the hierarchy of controls. Thus, a PHA can satisfy the regulatory requirements even though it might inadequately identify or control major hazards. In addition, there is no requirement to submit PHAs to the regulator, and the regulator is not responsible for assessing the quality of the PHA or the effectiveness of proposed safeguards, resulting in a regulatory system that is often reactive and frequently becomes involved in examining the details of process safety programs only after a major process accident. (Section 7.4)

[27] 42 U.S.C. §7412(r)(7)(B)(i) (1990).

1.2.5 Similar Findings in CSB Investigations of the Tesoro Anacortes and Chevron Richmond Refinery Incidents

34. The CSB conducted an investigation of the August 6, 2012, Chevron Richmond Refinery incident. That incident was also the result of a metallurgical failure caused by a well-known damage mechanism called sulfidation corrosion, and Chevron process safety programs failed to identify the hazard before the major incident that endangered the lives of 19 Chevron employees. The CSB identified a number of similar causal findings common to both the April 2010 Tesoro Anacortes Refinery incident and the August 2012 Chevron Richmond Refinery incident. (Section 7.7)

35. Mechanical integrity programs at both Tesoro and Chevron emphasized inspection strategies rather than the use of inherently safer design to control the damage mechanisms that ultimately caused the major process safety incidents. These inspections were unreliable and failed to prevent the incidents. Since the Richmond and Anacortes incidents, both Chevron and Tesoro have upgraded the materials of construction for the equipment that failed, using inherently safer design that significantly reduced the risk of the applicable damage mechanism hazards. (Section 7.7.1)

36. Both Tesoro and Chevron PHAs were ineffective in identifying the significant hazards of HTHA and sulfidation corrosion, respectively. Rather than performing rigorous analyses of damage mechanisms during the PHA process, both companies simply cited non-specific, judgment-based qualitative safeguards to reduce the risk of damage mechanisms. The effectiveness of these safeguards was neither evaluated nor documented; instead, the PHA merely listed general safeguards. (Section 7.7.2)

37. The Anacortes and Richmond refineries relied on API standards to assist in the selection of construction materials for the Tesoro NHT heat exchangers and the Chevron piping circuit, specifically API RP 941 and API RP 939-C *Guidelines for Avoiding Sulfidation (Sulfidic) Corrosion Failures in Oil Refineries*. The documents provide guidance on how to avoid HTHA and sulfidation corrosion failures, respectively, but neither document establishes minimum requirements to prevent equipment failure from the damage mechanism hazard. (Section 7.7.3)

38. Neither the Washington nor the California process safety regulations were successful in preventing major process safety incidents. Neither set of regulations required DMHRs, reduction of risk to ALARP, evaluation of effectiveness of controls, or use of the hierarchy of controls. In addition, there is no requirement to submit PHAs to the regulator, and the regulator is not responsible for assessing the quality of the PHA or the proposed safeguards. Furthermore, neither Washington nor California required the use of inherently safer design to the greatest extent feasible. A safety case regulatory regime in both states would help to ensure that all of the refineries in these states rigorously apply process safety concepts that focus more effectively on prevention. The new regulatory framework would also emphasize the implementation of

inherently safer designs and the hierarchy of controls to prevent major process safety incidents. (Section 7.7.4)

39. Both Washington and California have significant weaknesses in the staffing of PSM inspectors. Both Washington L&I (the Washington PSM regulator) and the California Occupational Safety and Health Administration (Cal/OSHA) (the California PSM regulator) lack sufficient technically experienced and qualified staff members to verify that PSM requirements are being implemented adequately. It is essential that regulators of high-hazard facilities are independent, well funded, well staffed, and technically qualified. These individuals must be able to communicate effectively with refinery personnel and to monitor the adequacy of refinery process safety practices. (Section 7.7.4)

40. Both the Chevron and Tesoro incidents could have been prevented if inherently safer equipment construction materials had been used. Although inherently safer technology (IST) is the most effective major accident prevention approach in the hierarchy of controls it is not enforced by the EPA through the General Duty Clause or other provisions of the Clean Air Act. The EPA has the authority to require the application of IST through the General Duty Clause. Furthermore, the Clean Air Act provides the authority for the EPA to develop and implement new regulations requiring the use of inherently safer systems analysis and the hierarchy of controls to establish more effective safeguards for identified process hazards to prevent major accidents. (Section 7.8)

1.3 Recommendations

As a result of the findings and conclusions of this report, the CSB makes recommendations, summarized below, to the following recipients:

The U.S. Environmental Protection Agency

Revise the Chemical Accident Prevention Provisions under 40 CFR Part 68 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. Until this revision is in effect, develop guidance and enforce the use of inherently safer systems analysis and the hierarchy of controls to the greatest extent feasible in establishing safeguards for identified process hazards through the Clean Air Act's General Duty Clause.

Washington State Legislature, Governor of Washington

Develop and implement a step-by-step plan to supplement the existing process safety management regulatory framework with the more rigorous safety management principles of the "safety case" for petroleum refineries in the state of Washington.

Washington State Division of Occupational Safety and Health – Labor and Industries

Perform verifications at all Washington petroleum refineries to ensure prevention of equipment failure because of HTHA and that effective programs are in place to manage hazardous nonroutine work. In addition, provide oversight of the process safety culture program at the Tesoro Anacortes Refinery.

American Petroleum Institute

Revise API RP 941 and API RP 581 to prohibit the use of carbon steel equipment in HTHA-susceptible service and require verification of actual operating conditions. Make additional revisions to API RP 941 to establish minimum requirements to prevent HTHA failures and to require the use of inherently safer design.

Tesoro Refining & Marketing Company LLC

Participate with API in the API RP 941 revisions to establish minimum requirements to prevent HTHA failures and to require the use of inherently safer design. Following the API RP 941 revisions, develop and implement a plan to meet the new API RP 941 requirements. Improve process safety management programs for damage mechanism hazards to require the hierarchy of controls and the use of inherently safer design.

Tesoro Anacortes Refinery

Implement a process safety culture program that will assess and continually improve any identified process safety culture issues at the Tesoro Anacortes Refinery.

Section 8.0 details the recommendations.

2.0 Tesoro Refining & Marketing Company LLC

Tesoro Corporation was founded in 1968 as a petroleum exploration and production company. In 1969, Tesoro began operating its first refinery near Kenai, Alaska. A Fortune 100 company, Tesoro now operates six refineries in the western United States. These refineries have a combined capacity of approximately 850,000 barrels per day (bpd).[28]

2.1 Anacortes Refinery

Tesoro purchased the Anacortes refinery from Shell Oil Company in August 1998. Located approximately 70 miles north of Seattle (Figure 2 and Figure 3), the Tesoro Anacortes refinery has a total crude-oil capacity of 120,000 bpd. The refinery has been in operation since 1955.[29]

The Anacortes refinery primarily supplies gasoline, jet fuel, and diesel to markets in Washington and Oregon. It also manufactures heavy fuel oils, liquefied petroleum gas, and asphalt. Approximately 350 employees and 50 contractors work at the refinery.[30]

Figure 2. Tesoro Anacortes Refinery

---

[28] *See* http://tsocorp.com/about-tesoro/locations/ and http://tsocorp.com/about-tesoro/company-history/ (accessed January 4, 2014).

[29] Statement of Basis for the Final Air Operating Permit – Final, July 26, 2010, p 6.

[30] The United Steelworkers (USW) represents approximately 185 of the operations and maintenance workers at the refinery. *See* http://www.usw.org/media_center/releases_advisories?id=0521, (accessed November 9, 2013).

Figure 3. Aerial View of the Tesoro Anacortes Refinery.

2.2 Other Tesoro Refineries

Beginning in the late 1990s, Tesoro made a series of refinery acquisitions. In 1998, Tesoro acquired refineries in Kapolei, Hawaii[31] (from BHP Americas), and Anacortes, Washington (from Shell Oil Company). In 2001, the company purchased refineries in Mandan, North Dakota, and Salt Lake City, Utah (both from Amoco). In 2002, Tesoro acquired the Golden Eagle refinery in Martinez, California

[31] Tesoro no longer owns this refinery.

(from Ultramar, now Valero), and in 2007 Tesoro acquired its Los Angeles refinery (from Shell Oil) and USA Gasoline retail stations (from Chevron).[32] Tesoro purchased its Carson, California, refinery in 2013 (from BP).[33]

2.3 Tesoro Anacortes Refinery NHT Unit

The April 2, 2010, incident occurred in the Tesoro Anacortes Refinery Catalytic Reformer / Naphtha Hydrotreater unit ("the NHT unit"), which includes a naphtha hydrotreating process unit. Hydrotreating is a process that removes sulfur, nitrogen, and oxygen impurities from petroleum feedstock and intermediate products by reacting with hydrogen in the presence of a catalyst. Hydrotreating serves two purposes: [34]

1. It improves the quality and environmental impact of products, especially quality specifications mandated by law (for example, benzene reduction in motor gasoline).
2. It protects sensitive and costly downstream catalysts from contamination.

The Tesoro NHT unit was originally constructed in 1972 with a rated capacity of 24,800 bpd. Modifications and upgrades resulted in a rated capacity at the time of the incident of 40,550 bpd, a 64% capacity increase.

2.3.1 Catalytic Reformer

Catalytic reforming is a chemical process used to convert petroleum refinery naphtha,[35] typically having low-octane ratings,[36] into high-octane liquid products called reformates. The Catalytic Reformer uses a system of fixed bed catalytic reactors to increase the octane rating of gasoline blending stock. The reformate product is then sent to gasoline component storage for use in fuel blending. The reforming reaction generates hydrogen, which is used in the NHT.

2.3.2 Naphtha Hydrotreater – A/B/C & D/E/F Feed/Product Heat Exchangers

The removal of sulfur, nitrogen, and oxygen impurities in the NHT unit requires heating the naphtha to over 600 °F at greater than at 600 pounds per square inch gauge (psig) and mixing it with hydrogen. The initial portion of this heating took place in the NHT unit's E-6600 A/B/C and D/E/F feed and product

---

32 *See* http://www.tsocorp.com/TSOCorp/AboutUs/CompanyHistory/061236, (accessed April 24, 2013).

33 *See* http://tsocorp.com/about-tesoro/company-history/ (accessed January 4, 2014).

34 Hydrocarbon Publishing Company, *Worldwide Refinery Processing Review (Individual Technology)*, Hydrotreating summary. 2Q 2012, Item No. B1014

35 Naphtha is a fraction of crude oil that boils between approximately 85 °F and 400 °F. It includes hydrocarbons ranging from C_5 to C_{12}. Naphtha comprises approximately 15-30 weight % of raw crude oil. *See* Prestvik, R.; Moljord, K.; Grande, K.; Holmen, A. *Compositional Analysis of Naphtha and Reformate.* In G.J. Antos & A.M. Aitani (Eds.), *Catalytic Naphtha Reforming* (p. 2). New York, NY: Marcel Dekker, Inc.

36 Octane rating represents gasoline-burning efficiency. The higher the octane rating, the less likely it is for gasoline to *knock*, or produce harmful, small explosions that reduce efficiency, in an engine. *See* Van Dyke, K. (1997). *Fundamentals of Petroleum* (4th ed.) (p 318). Austin, Texas: The University of Texas at Austin.

(effluent) heat exchangers,[37] as depicted in Figure 4. (These heat exchangers are referenced throughout this report as the NHT heat exchangers.)

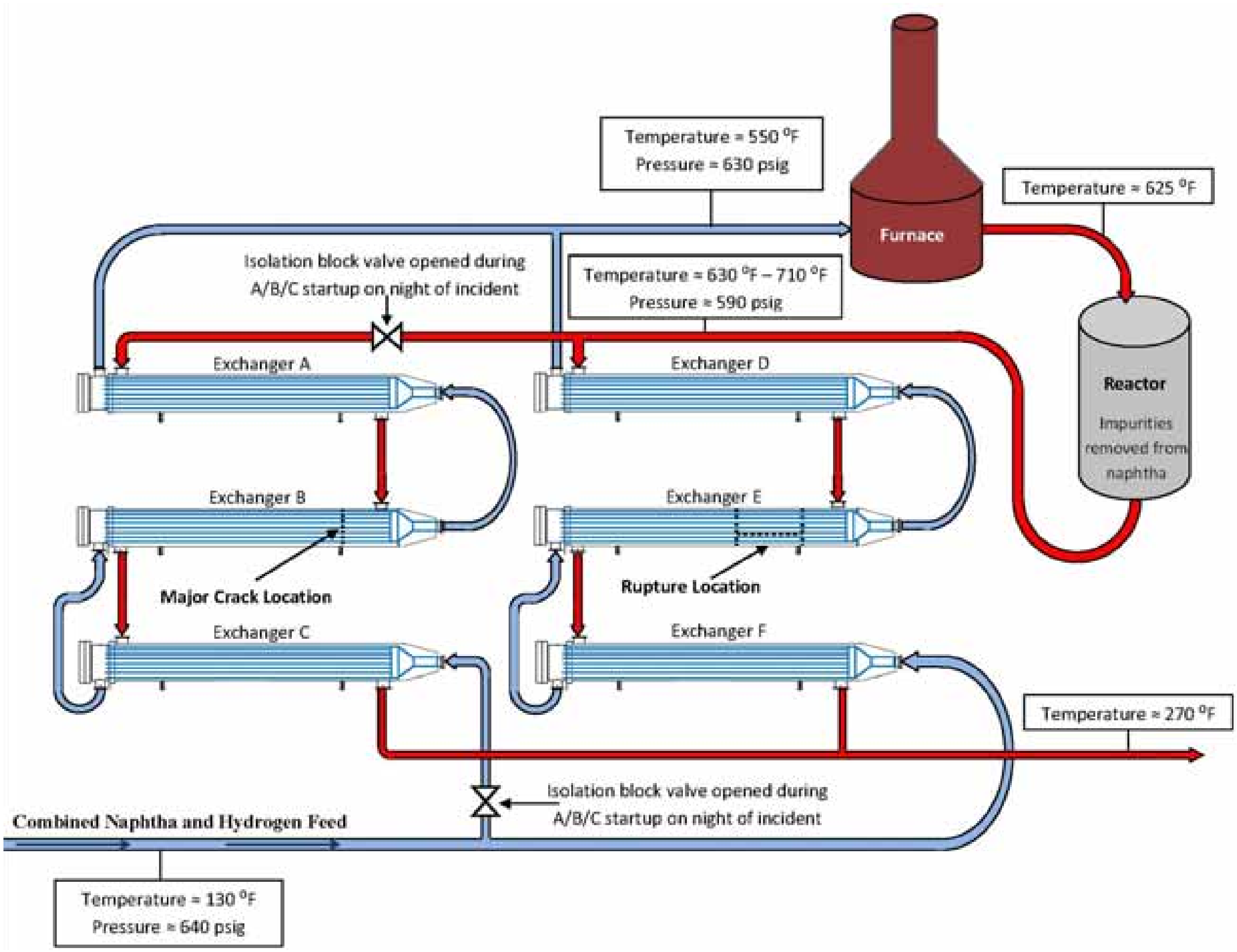


Figure 4. Process Flow of NHT Unit

The function of the NHT A/B/C and D/E/F heat exchangers is to conserve energy by using the hot NHT reactor effluent to heat the cooler reactor feed and thus reduce the energy input needed for the reactor furnace. The cool NHT liquid naphtha feed is pumped from storage and/or other active units and mixed with a stream of hydrogen-rich gas, becoming a combined liquid and gas feed stream. The resulting liquid-gas mixture is then fed to the tube-side[38] of two parallel groups, or banks of three heat exchangers (A/B/C and D/E/F) to be heated by the shell-side[39] fluid. As the liquid-gas mixture inside of the tubes is

[37] The A/B/C and D/E/F exchangers are single-pass shell and tube heat exchangers. A heat exchanger allows heat to be transferred from one process fluid to another. One fluid gets hotter while the other gets cooler. A shell and tube–type heat exchanger consists of a large pressure vessel exterior (shell) with a group (bundle) of small thin-walled pipes (tubes) that reside inside the shell. One process fluid flows through the tubes, and the other process fluid flows through the shell, over the tubes. Heat is transferred (exchanged) from one to the other through the walls of the tubes.

[38] "Tube-side" refers to process fluid that flows inside of heat exchanger tubes.

[39] "Shell-side" refers to process fluid that flows inside of the heat exchanger shell and on the outside of the tubes.

heated, the liquid portion vaporizes completely. Now liquid free, the naphtha and hydrogen vapors enter a furnace where they are further heated and then fed to the NHT reactor. The reactions to remove sulfur, nitrogen, and oxygen take place in this reactor. The hot reactor effluent[40] is then fed through the shell-side of the heat exchangers to preheat the incoming tube-side feed. The impurity-free naphtha is then fed to other processes in the refinery.

[40] Effluent is flow exiting a vessel or piece of equipment.

3.0 Incident Description

3.1 Pre-Incident Operations

During normal operation at the Tesoro Anacortes Refinery, the A/B/C and D/E/F heat exchangers were all in use. Because of the original Shell Oil Company design and the process operating conditions, the heat exchangers would foul during operation; that is, they would develop a buildup of process contaminant byproducts both inside of the heat exchanger tubes, as illustrated in Figure 5, and outside of the tubes. The fouling inhibited heat transfer between the tube-side and shell-side process fluid, thus reducing the heat transfer efficiency.

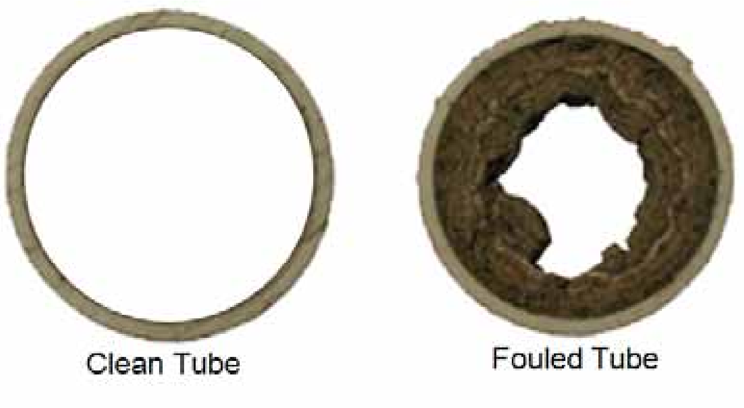


Figure 5. Example of Fouling Deposits on the Inside of Heat Exchanger Tubes. Fouling greatly reduces heat transfer between the shell-side and tube-side process fluids.[41]

Because the heat exchangers fouled, they required periodic cleaning so that process temperature requirements could be maintained. Cleaning was typically required after about six months of continuous operation. When performing this cleaning, one bank of heat exchangers was taken out of service while the other bank continued operating. The cleaned heat exchangers would then be placed back into service by slowly introducing the hot naphtha and hydrogen feed into the heat exchangers. Because of a long history of frequent leaks and occasional fires when putting these heat exchangers back into service (Section 5.1), this activity was a hazardous nonroutine operation.[42] By employing this nonroutine operation, Shell Oil and Tesoro avoided a total shutdown of the NHT unit.

On March 28, 2010, five days before the incident, the A/B/C heat exchanger bank was taken offline so that the fouled tubes in each heat exchanger could be cleaned. The D/E/F heat exchanger bank and the

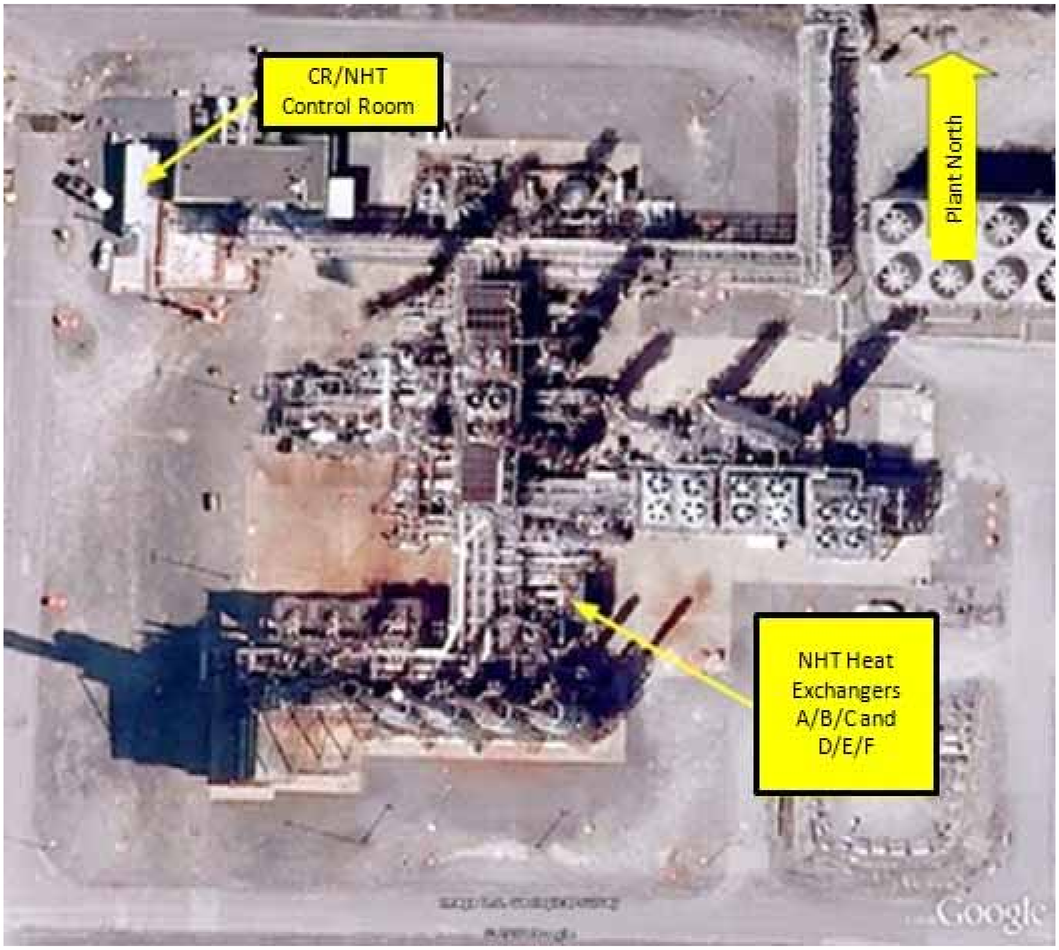
[41] Photograph of fouled tube from http://www.tekleen.com/it/water-filtration-101/ (accessed December 4, 2013).

[42] Nonroutine does not refer to the frequency at which the activity occurs. Nonroutine refers to whether the activity is part of the normal sequence of converting raw materials to finished products. Startup and shutdown of equipment are considered a nonroutine activity. Center for Chemical Process Safety (CCPS), *Guidelines for Risk Based Process Safety*. 2007; p 286.

rest of the NHT unit remained in operation. On March 31, 2010, the three-day maintenance cleaning activity was completed and the equipment was reassembled and prepared for operation.

3.2 Night of the Incident

On the evening of April 1, 2010, Tesoro initiated startup of the A/B/C heat exchanger bank. The NHT unit was staffed in a typical manner, with one inside board operator who monitored the console and one outside operator. An aerial view of the unit is shown in Figure 6.



Source: Google Earth

Figure 6. Aerial View of CR/NHT Unit

The inside NHT operator and the outside NHT operator began the process of placing the heat exchangers back in service. The inside operator used a step-by-step task list for the startup process, physically checking off the steps on a hardcopy of the procedure while maintaining radio communication with the outside operator. Interviews conducted by the CSB indicate that the startup of the heat exchangers was a very difficult assignment for only a single outside operator. The startup procedure required manipulation of several isolation block valves as illustrated in Figure 7, which necessitated a significant amount of manual effort to open.

Figure 7. CSB Animation of Operator Opening Long-Winded Valve on Night of Incident. Valves on heat exchanger structure had to be opened concurrently when performing the heat exchanger bank startup

These valves had to be gradually and concurrently opened, so the operator could not simply stay by each valve until it was fully opened or closed. Also, four steam lances were staged and ready for use during the startup to mitigate any leaks or fires that might occur.[43] These valves and steam lances were located at different positions in the vicinity of the A/B/C and D/E/F heat exchangers. At approximately 10:30 p.m., six additional Tesoro employees (five operators and one supervisor)[44] joined the outside operator, at the request of the supervisor, to assist in bringing the A/B/C heat exchanger bank online. The startup procedure did not specify defined roles for these six additional personnel.

3.3 The Incident

The operators continued the A/B/C heat exchanger bank startup as planned. Two leaks from the heat exchangers were reported during the startup. These leaks did not stop operations however, because leaks during startup of these heat exchangers were frequent and had become a “normal” part of the startup. Furthermore, based on past operating experience, these leaks were expected to cease when the heat exchangers reached typical operating temperature.

---

[43] Three of the four steam lances were likely in use at the time of the incident. See Section 5.0 for additional discussion on the use of steam lances.

[44] The five additional operators that assisted in the NHT heat exchanger startup were assigned to the Crude, Utilities, Vacuum Flasher, ROSE, and CFH/DHT units.

At 12:30 a.m. on April 2nd, while the seven outside personnel were still performing A/B/C heat exchanger bank startup operations, the E heat exchanger on the adjacent, in-service bank catastrophically ruptured. The pressure containing "shell" of the heat exchanger separated at weld seams,[45] as depicted in Figure 8, expelling a large volume of very hot hydrogen and naphtha.[46]

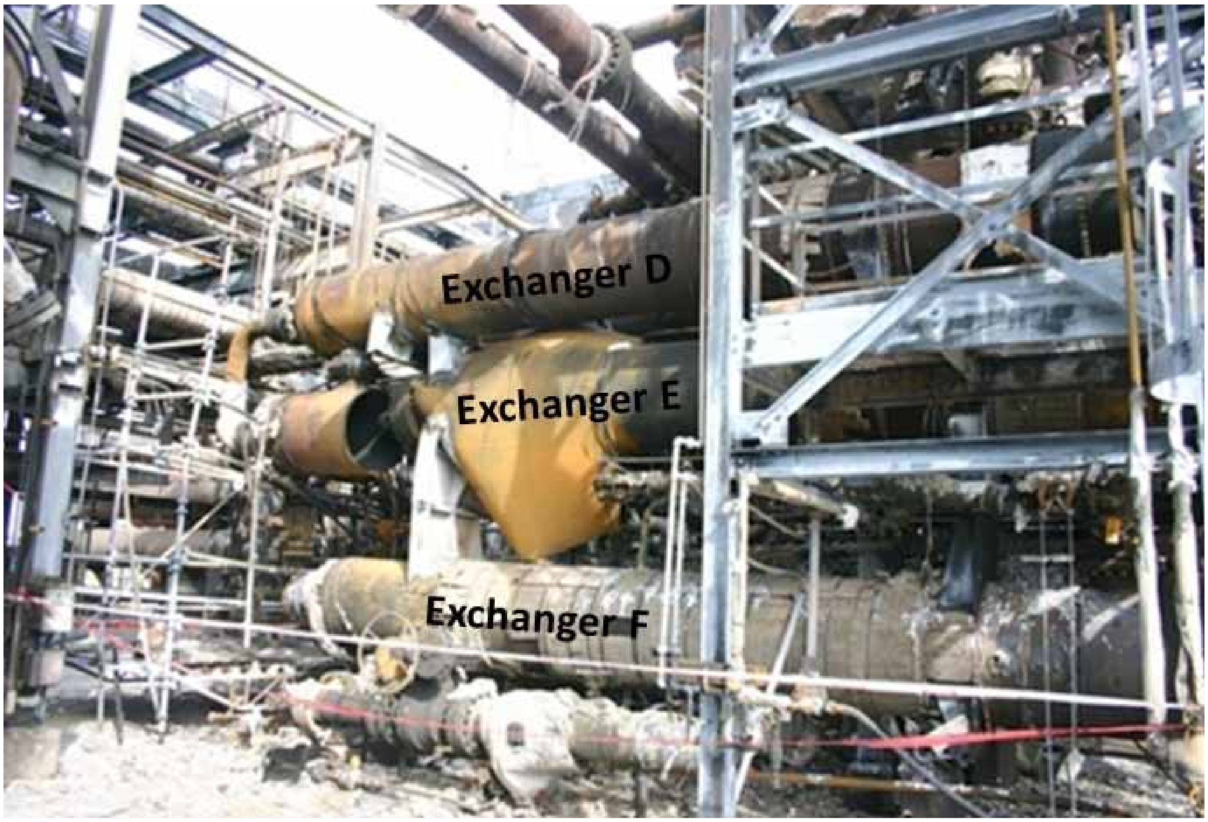


Figure 8. Post-Incident View of D/E/F NHT Heat Exchanger Bank

The naphtha and hydrogen likely autoignited upon release into the atmosphere, creating a large fireball as depicted in Figure 9.

---

[45] The failure occurred at both circumferential and longitudinal weld seams from fabrication of the exchanger.

[46] The naphtha began to condense to liquid in the B and E heat exchangers. The material in the process was above its atmospheric boiling temperature, so it vaporized when released to atmospheric conditions.

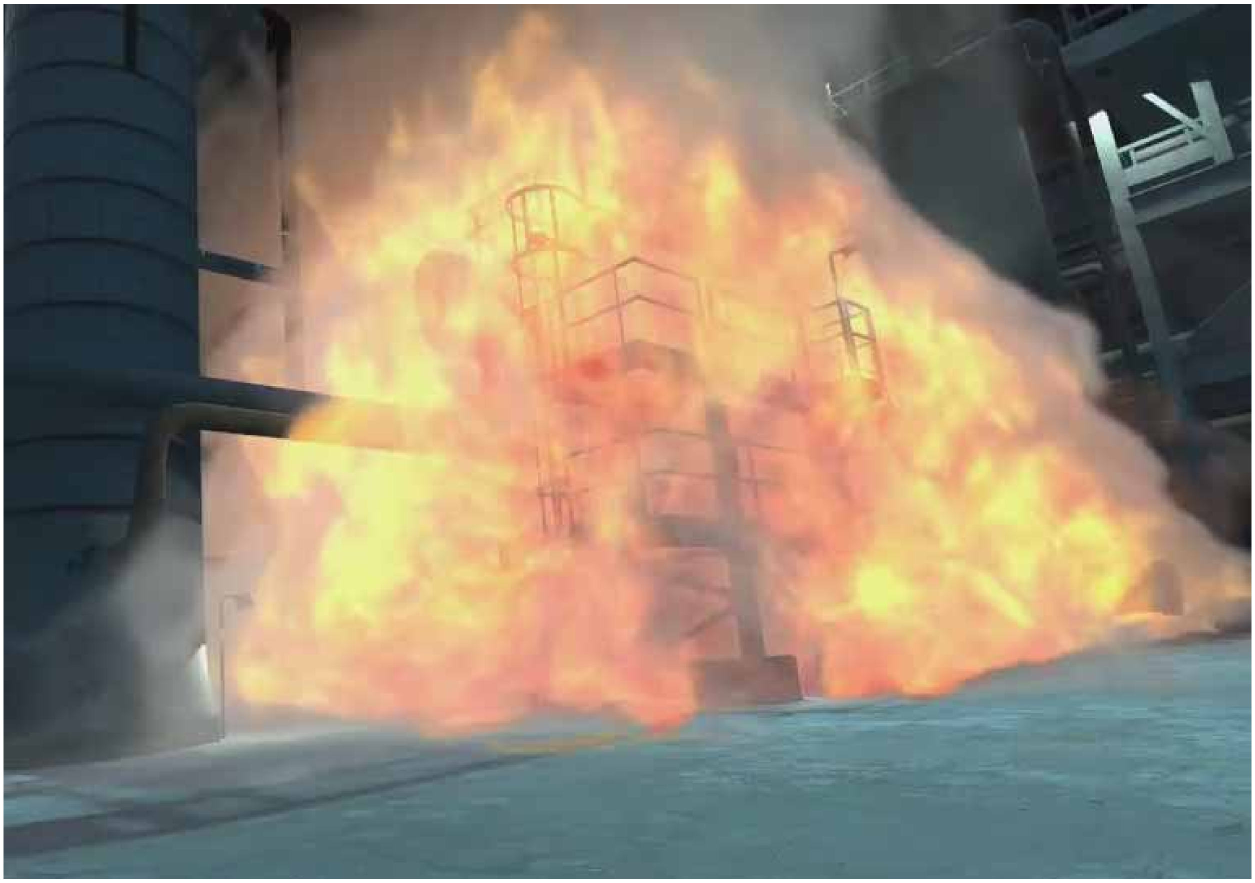


Figure 9. CSB Animation of the Fire Following the NHT Heat Exchanger Failure. The hot naphtha and hydrogen likely autoignited upon release to the atmosphere. The fire engulfed the entire heat exchanger structure.

The operator in the NHT control room told the CSB that he felt the impacts of the rupture at his desk 350 feet away. The CSB determined that at the time of the incident two of the outside operators were likely on the top level of the heat exchanger structure (Figure 10), and the remaining five operators were most likely at ground level. All seven outside operations personnel were badly burned, and within 22 days of the incident, all succumbed to their injuries.

Figure 10. Six NHT Heat Exchangers in Two Banks of Three Heat Exchangers Each

4.0 Technical Analysis

4.1 High Temperature Hydrogen Attack

Post-incident metallurgical analysis determined that the carbon steel E heat exchanger ruptured because it was in a highly weakened state because of high temperature hydrogen attack (HTHA). The HTHA damage mechanism occurs when steel equipment is exposed to hydrogen at high temperatures and partial pressures. The resulting damage severely degrades the mechanical properties of the carbon steel.[47]

> **Carbon steel is more susceptible to HTHA than all other materials of construction considered by API RP 941.**

HTHA occurs when atomic hydrogen diffuses into the steel walls of process equipment, as illustrated in Figure 11. The hydrogen reacts[48] with carbon in the steel, producing methane gas,[49] as depicted in Figure 12. This reaction removes carbon from the steel, a process commonly referred to as "decarburization."[50]

---

[47] Shih, H.M. and Johnson, H.H. A *Model Calculation of the Nelson Curves for Hydrogen Attack;* Acta Metallurgica, Volume 30. 1982; pp 537-545.

[48] Sources differ on whether atomic hydrogen directly reacts with carbon in steel to produce methane or whether the hydrogen recombines inside the steel to form molecular (diatomic) hydrogen before reacting with carbon to form methane.

[49] API Technical Report 941. *The Technical Basis Document for API RP 941*. 2008; pp 7-8.

[50] Weiner, L.C. *Kinetics and Mechanism of Hydrogen Attack of Steel*. Corrosion, 1961, Volume 17, pp 109-115.

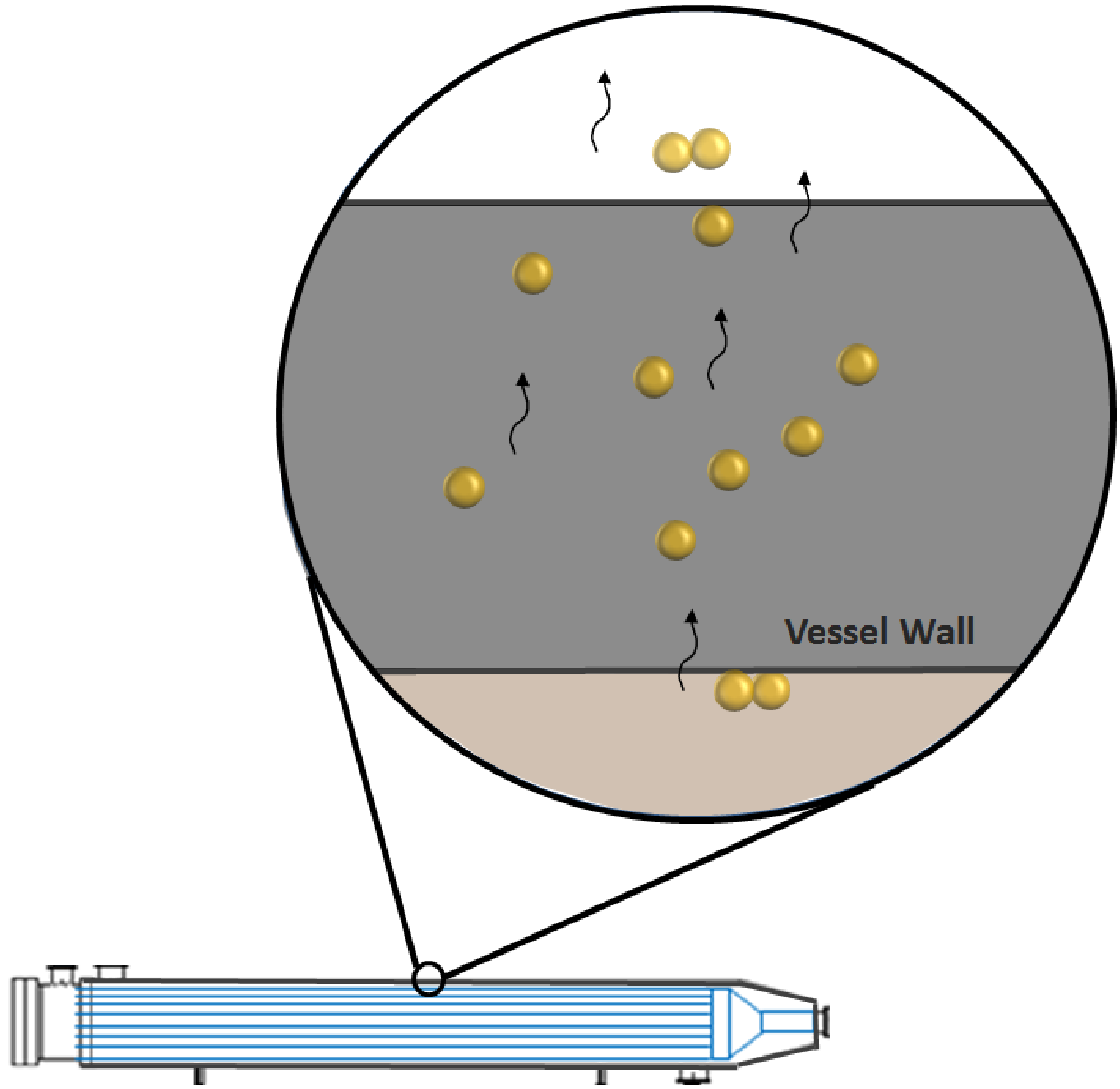


Figure 11. Atomic Hydrogen Diffuses Through Steel. In HTHA, molecular hydrogen dissociates at the vessel wall to form atomic hydrogen, which diffuses through the steel.

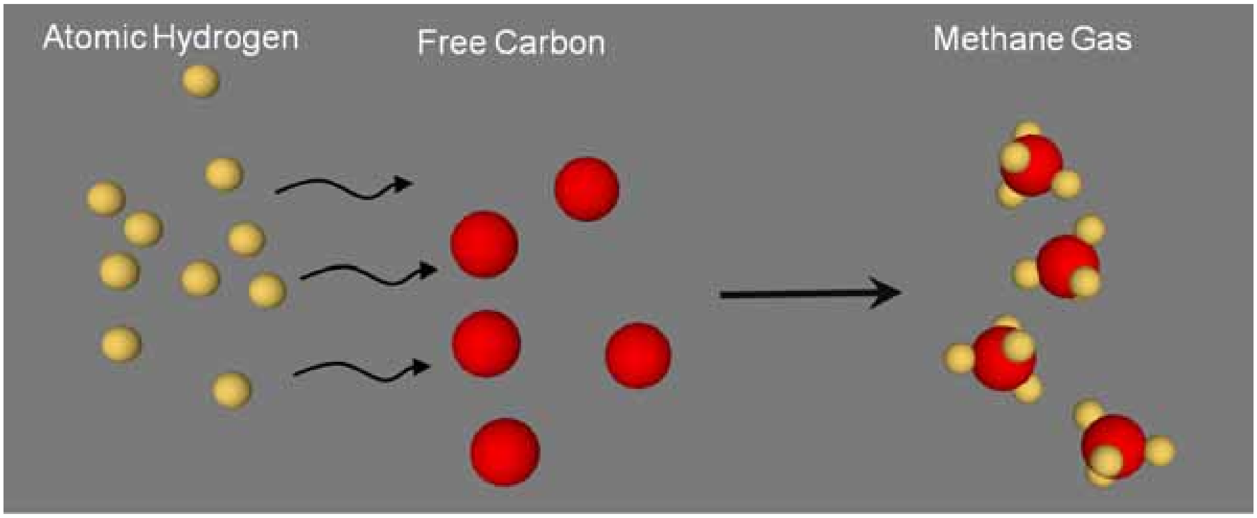


Figure 12. Decarburization Process. When the atomic hydrogen encounters free carbon inside of the steel, hydrogen and carbon react to produce methane gas.

Methane, a much larger molecule than atomic hydrogen, cannot diffuse out of the steel. Rather, it accumulates inside the vessel walls,[51] exerting force on the surrounding steel. As more methane gas is formed, the methane pressure increases. The very high pressure exerted by the methane gas inside the steel can form fissures, as illustrated in Figure 13 or blisters in the steel, as shown in Figure 14.[52]

[51] API Technical Report 941. *The Technical Basis Document for API RP 941*. 2008; pp 7-8.

[52] Allen, R.E., Jansen, R.J., Rosenthal, P.C., and Vitovec, F.H., *The Rate of Irreversible Hydrogen Attack of Steel at Elevated Temperatures*. 26th Midyear meeting of AIChE. May 9, 1961.

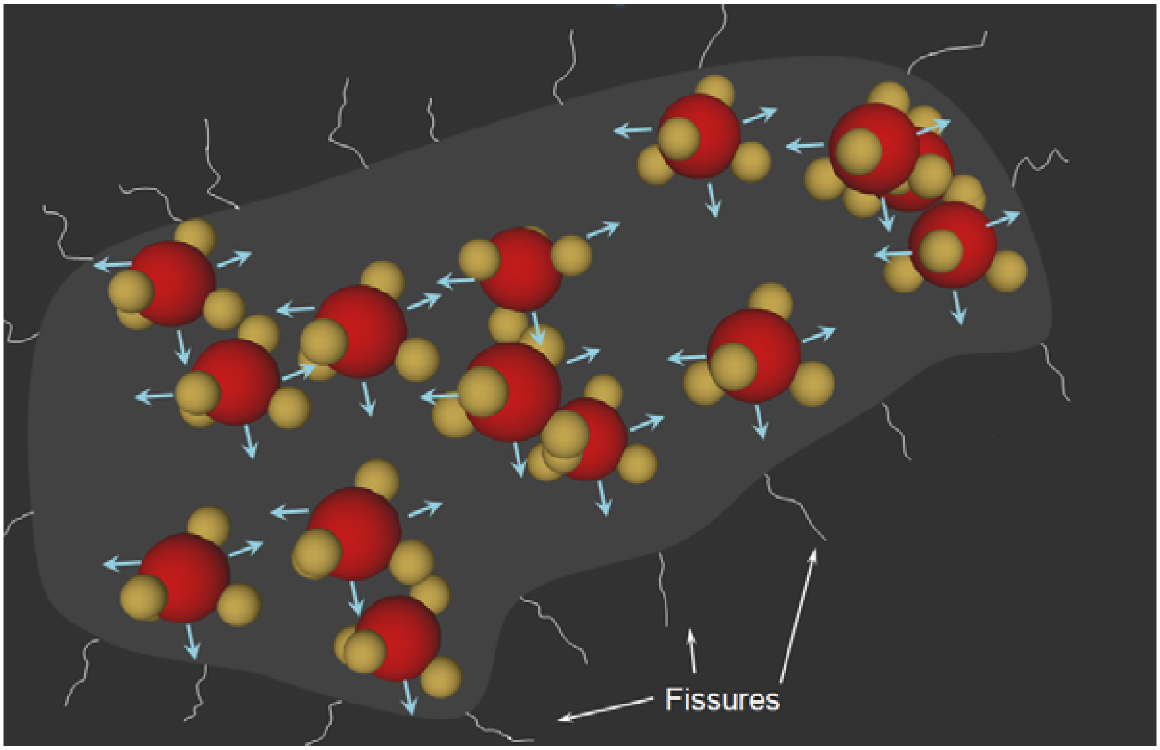


Figure 13. Methane Fissures. When methane molecules cannot diffuse out of the steel, they accumulate inside of the steel, creating high pressure that forms fissures in steel.

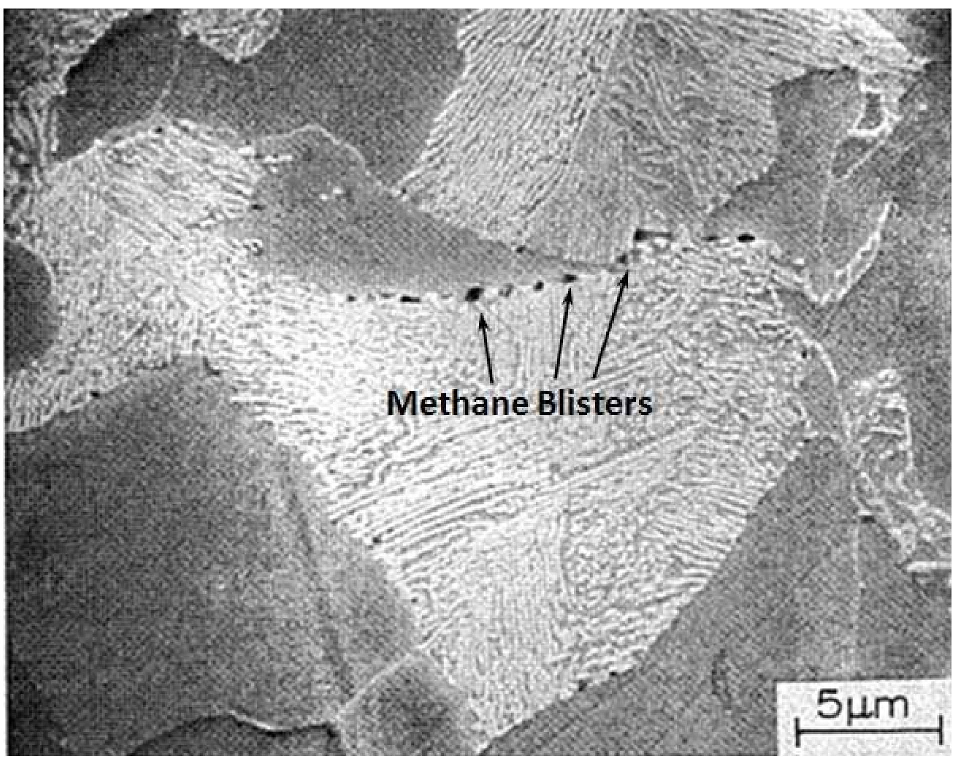
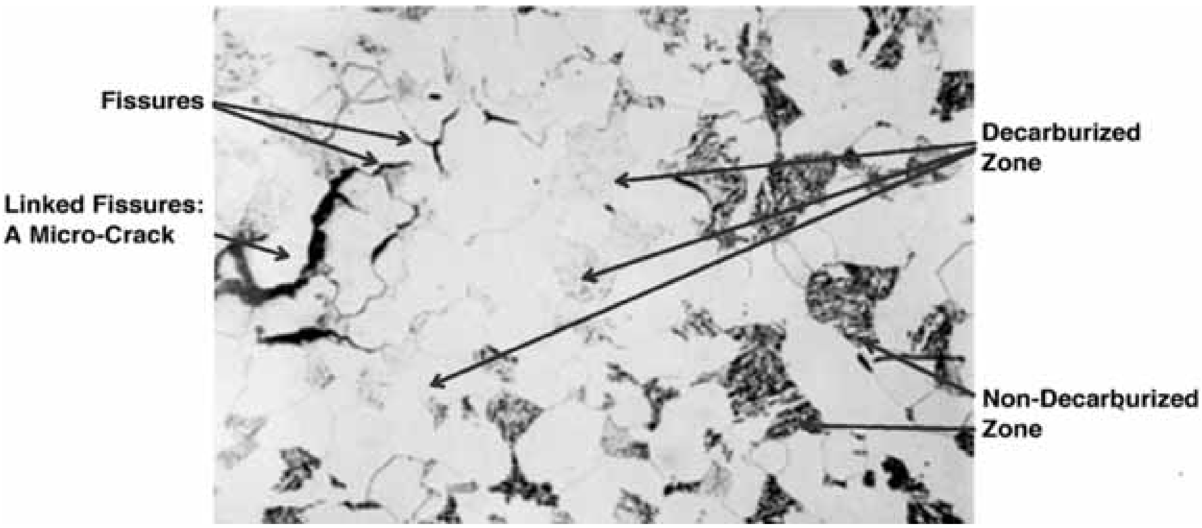


Figure 14. Methane Blisters. Accumulation of methane in steel can also form blisters in the metal.

As more fissures are formed, they can link, forming microcracks in the steel.[53] The linkage of fissures into microcracks is shown in Figure 15. Microcracks can also link to form larger cracks, which greatly weaken the steel and can lead to rupture of the vessel.[54] This process occurred in the E heat exchanger at the Tesoro Anacortes Refinery.



Source: API RP 941, Figure 2

Figure 15. Microcrack Resulting from Linked-HTHA Fissures. This image from API RP 941 shows fissures formed as a result of HTHA linked together to form a microcrack. Decarburized regions appear lighter in color (because of an absence of carbon) than unaffected regions.

[53] Lai, George. *High Temperature Corrosion and Materials Applications.* Materials Park: ASM International, 2007.

[54] *Ibid*.

4.1.1 Predicting the Occurrence of HTHA

Industry relies on a graph in API RP 941 *Steels for Hydrogen Service at Elevated Temperatures and Pressures in Petroleum Refineries and Petrochemical Plants* to predict the occurrence of HTHA in various steels. The lines in that graph are known as Nelson curves, developed in 1949 by George Nelson,[55] who created these curves based on observed industry experience with HTHA. The curves have been adjusted over the years based on additional industry experience.[56] The most recent version of the API RP 941 Nelson curves is shown in Figure 16. Industry uses these curves as a line of demarcation to predict HTHA. At temperatures above each curve, HTHA is possible for that material of construction, and at temperatures below the curve, the prediction is that HTHA will not occur for that material.

Nelson curves include consideration of these HTHA variables:

- **Material of construction**
- **Temperature**
- **Hydrogen partial pressure**

The Nelson curves predict HTHA based on process temperature, hydrogen partial pressure,[57] and material of construction. Carbon steel is represented by the lowest curve, indicating that this material is the most susceptible to HTHA when compared to the other materials of construction shown in Figure 16. For a given material of construction, the Nelson curve indicates that a higher temperature increases the probability that HTHA will occur.[58,59]

---

[55] G. A. Nelson, *Hydrogenation Plant Steels*. 1949 Proceedings, Volume 29M, API; pp. 163 -174.

[56] API Technical Report 941. *The Technical Basis Document for API RP 941*. 2008; p 127.

[57] Hydrogen partial pressure is a calculated parameter. It is the pressure that would be exerted by a single component of a gas mixture. For example, the hydrogen partial pressure of a 500 psia gas mixture in a vessel that contains 50 mole percent (mol%) hydrogen and 50 mol% propane equals 250 psia.

[58] For most materials included on the Nelson curves, increasing hydrogen partial pressure also increases the probability of HTHA. However, in some areas for some materials, the Nelson curves do not predict a higher probability of HTHA when hydrogen partial pressure is increased.

[59] Low carbon steels, which contain very little alloying additions of chromium and molybdenum, are the most susceptible to HTHA. Chromium-rich and molybdenum-rich carbides are inherently more stable than iron carbides, and they resist dissolution of carbon with hydrogen to form methane. Therefore, the alloys containing chromium and molybdenum resist HTHA at higher temperatures and hydrogen pressures. *See* CSB's E-6600E and E-6600B Metallurgical Analysis report (Appendix I).

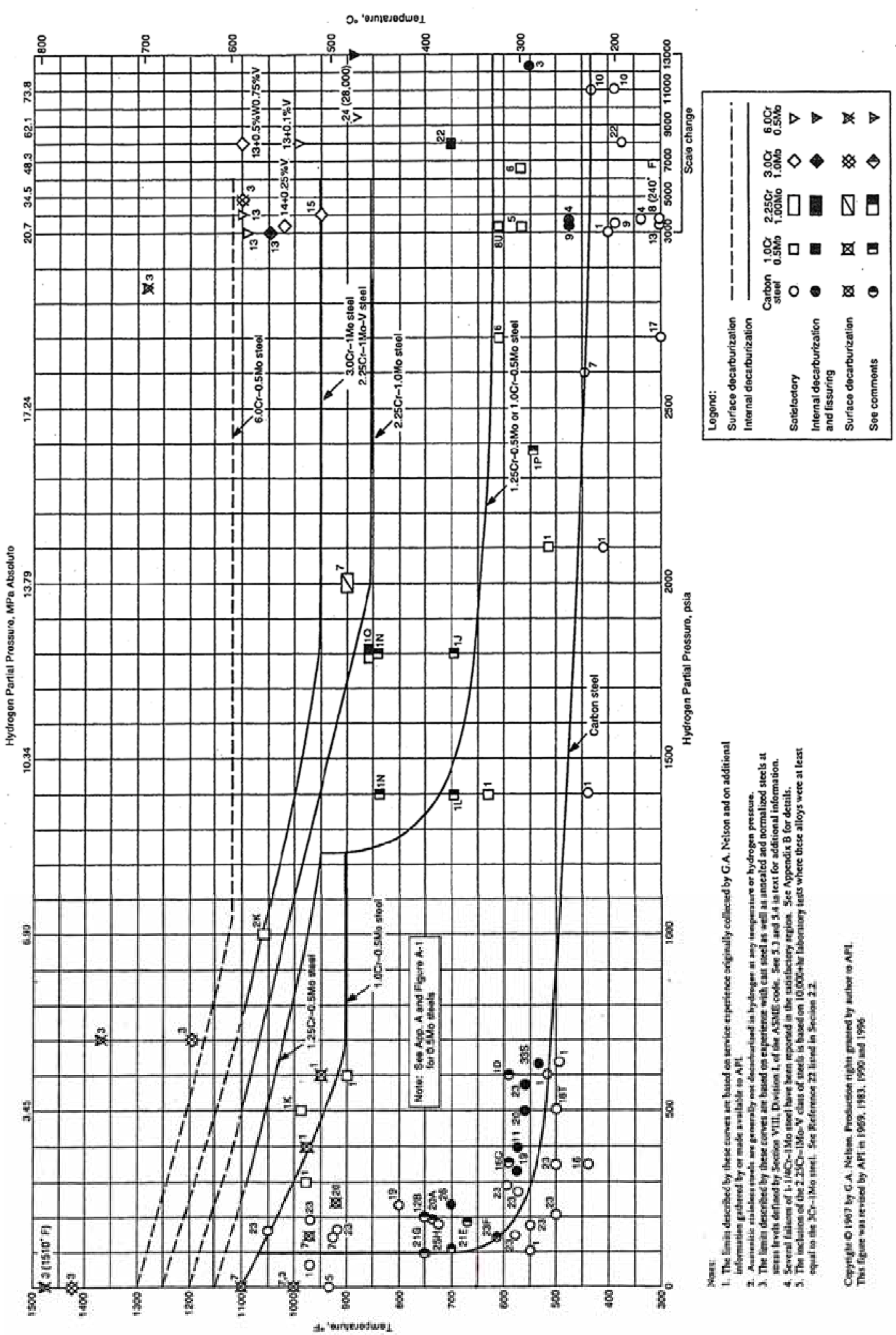


Figure 16. Nelson Curves from Current API RP 941. These Nelson curves are used to predict the occurrence of HTHA in various materials of construction.

4.1.2 Conditions that increase HTHA susceptibility

Welding performed on steel process vessels creates additional HTHA risk factors, such as residual stress.[60] Post-weld heat treatment is a method that can reduce the stress in steel that was generated from the welding process. The process of post-weld heat treatment consists of a sequence of controlled heating and cooling steps applied to the welded structure using externally applied heating elements.[61] This process gives the metal time to readjust to its original, prefabrication state[62] and removes residual stress. The carbon in the steel becomes less reactive, inhibiting the reaction with hydrogen to form methane. Chemical resistance to HTHA is thus modestly improved in post-weld heat-treated steels.[63]

As will be discussed in Section 4.2.1, the carbon steel shells of the B and E heat exchangers were not post-weld heat-treated, and therefore the steel surrounding the welds may have been high-stress areas.[64] HTHA was only found in the areas near the welds in both the B and E heat exchangers.

Post-weld heat treating is a weaker safeguard than using materials that are not susceptible to HTHA damage.

Post-weld heat treating is a manual activity and therefore low on the hierarchy of controls.[65] Consequently, it is a weaker safeguard to prevent HTHA failures than the use of materials that are not susceptible to HTHA damage.[66,67]

---

60 API Technical Report 941. *The Technical Basis Document for API RP 941.* 2008; p 163.

61 Krishnan, J. and Ahmed, Khaleel; *Post-Weld Heat Treatment- Case Studies*. BARC Newsletter. Centre for Design and Manufacture, Bhabha Atomic Research Centre, May 2002.

62 Gillissie, J.G., *Heat Treatment- What Is It?.* The National Board of Boiler and Pressure Vessel Inspections. October 1981.

63 API Technical Report 941. *The Technical Basis Document for API RP 941.* 2008; p 162.

64 Post-weld heat treatment is generally avoided unless specified as mandatory by codes or standards. Incorrect post-weld heat-treatment procedures can result in metal that is out of specification for the service. In the United States, the ASME Boiler Code is the authority that mandates post-weld heat treatment. If the code requires post-weld heat treatment, it is performed, but if the code does not specify the requirement for post-weld heat treatment, then the heat treatment is generally not performed. The ASME Boiler Code did not require post-weld heat treatment for the B and E heat exchangers. *See* 2011 ASME Boiler and Pressure Vessel Code; Paradowska A., Price J.W.H, and Dayawansa P. *Measurement of Residual Stress Distribution in Tubular Joints Considering Postweld Heat Treatment* Materials Forum Volume 30- 2006. Institute of Materials Engineering Australasia Ltd.; and Funderburk, R. Scott, *Postweld Heat Treatment.* Welding Innovation, Vol. XV, No. 2, 1998.

65 An effectiveness ranking of techniques used to control hazards and the risk they represent can be described as a hierarchy of controls – the higher up (further left) on the hierarchy, the more effective the risk reduction achieved (Figure 17).

66 Improper post-weld heat treating can lead to vessel failure. Steward, M. and Lewis, O. *Pressure Vessels Field Manual Common Operating Problems and Practical Solutions*, 2013; pp 236-237.

67 Post-weld heat treating problems include heat treating errors such as inadequate time at temperature, inadequate or excessive temperature rate, inadequate temperature, cooled too rapidly, cooled too slowly, and cooled to the wrong temperature. Canale, L., Mesquita, R., and Totten, G., *Failure Analysis of Heat Treated Steel Components*, 2008; pp 106-109.

Despite the improved HTHA resistance of post-weld heat-treated vessels compared with non-post-weld heat-treated vessels, upgrading vessel materials to inherently safer materials of construction is a better approach to prevent equipment failure from HTHA. This approach is discussed further in Section 4.1.3.

4.1.3 Inherently Safer Design

As defined in the Center for Chemical Process Safety (CCPS)[68] book *Inherently Safer Chemical Processes, 2nd ed.*, inherently safer design is the process of identifying and implementing inherent safety in a specific context that is permanent and inseparable from the process.[69] In the book *Guidelines for Engineering Design for Process Safety, 2nd ed.*, the CCPS states that "inherently safer design solutions eliminate or mitigate the hazard by using materials and process conditions that are less hazardous."[70]

Inherently safer technologies are relative; a technology can be described as inherently safer only when compared to a different technology with regard to a specific hazard or risk.[71] A technology can be inherently safer with respect to one risk but not inherently safer from another risk. Consequently, it is important to carry out a comprehensive documented hazard analysis to identify the individual and overall risks in a process and assess how the risks can be effectively minimized to control hazards. An inherently safer systems or hierarchy of control review details a list of choices that offer varying degrees of inherently safer implementation. The review should include risks of personal injury, environmental harm, and lost production, as well as an evaluation of economic feasibility.[72]

It is simpler, less expensive, and more effective to introduce inherently safer features during the design process of a facility rather than after the process is already operating.[73] Process upgrades, rebuilds, and repairs offer additional opportunities to implement inherently safer design concepts. Conducting a comprehensive hazard review to determine risks and identify ways to eliminate or reduce those risks constitutes an important step in implementing an inherently safer process.

---

[68] The Center for Chemical Process Safety (CCPS) is a corporate membership organization that identifies and addresses process safety needs within the chemical, pharmaceutical, and petroleum industries.

[69] Center for Chemical Process Safety (CCPS). *Inherently Safer Chemical Processes – A Life Cycle Approach*. 2009; section 2.2.

[70] *Ibid* at Section 5.1.1.

[71] *Ibid* at Section 5.2.

[72] *Ibid* at p 184.

[73] Kletz, Trevor and Amyotte, Paul. *Process Plants: A Handbook for Inherently Safer Design*. 2010; p 14.

An effectiveness ranking of techniques used to control hazards and their associated risks can be described as a hierarchy of controls. As depicted in Figure 17, the further left on the hierarchy continuum, the more effective the technique is in reducing risk. All concepts in the hierarchy of controls should be included in the process of risk assessment and reduction. Upgrading the equipment material of construction to a more HTHA-resistant steel is a high-ranking, inherently safer choice in material selection. Holding other variables constant, upgrading the material of construction can eliminate the potential for HTHA. As previously discussed, post-weld heat treating to modestly reduce HTHA susceptibility is low on the hierarchy of controls and thus is a weaker safeguard to prevent HTHA failures than the use of materials that are not susceptible to HTHA damage.

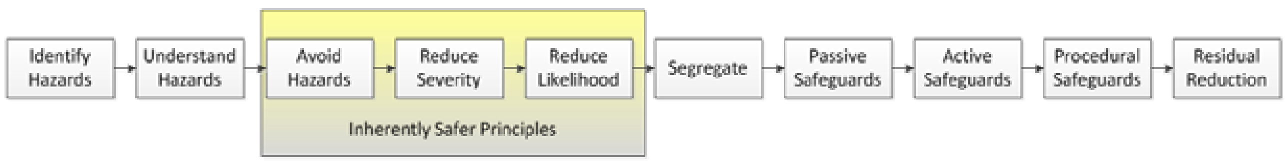


Figure 17. Hierarchy of Controls. The highlighted boxes reflect inherently safer controls, based on *Process Plants: A Handbook for Inherently Safer Design Second Edition*; Kletz, Trevor Amyotte, Paul; CRC Press 2010.

Since the April 2010 incident, Tesoro has installed new NHT heat exchangers, incorporating aspects of an inherently safer design.[74] As discussed in Section 4.4.1.3, the materials of construction of two heat exchangers have been upgraded to significantly reduce the potential for HTHA.

74 While the material of construction is upgraded in the new exchangers, portions of the heat exchangers that are manufactured with carbon steel are still designed to operate at temperatures higher than 400 ºF.

4.1.4 HTHA Inspection Strategy Limitations

While inspection is an important mechanical integrity program component, there are significant limitations with relying solely on inspection strategies to prevent equipment failure from HTHA. For example, refinery equipment must already be damaged by HTHA for equipment inspection to identify HTHA. HTHA damage is also extremely difficult to identify by conducting an inspection. API RP 941 includes a discussion of these difficulties:

> High temperature hydrogen attack is a difficult inspection challenge. The early stages of attack with fissures, or even small cracks, can be difficult to detect. The advanced stage of attack with significant cracking is much easier to detect, but at that point there is already a higher likelihood of equipment failure.[75]

Some existing inspection methods attempt to identify HTHA, as described in Appendix E. However, inspection should not be solely relied on to identify and control HTHA. Inspection results can be unreliable and misleading. Successful identification of HTHA is highly dependent on the specific techniques employed and the skill of the inspector, and few inspectors have this level of expertise.[76]

Inspection thus ranks very low on the hierarchy of controls. API RP 571 *Damage Mechanisms Affecting Fixed Equipment in the Refining Industry* implicitly supports the concept of inherently safer design by describing material selection to avoid HTHA failures noting, "300 Series SS, as well as 5Cr, 9Cr and 12Cr alloys, are not susceptible to HTHA at conditions normally seen in refinery units."[77]

---

75 API RP 941. *Steels for Hydrogen Service at Elevated Temperatures and Pressures in Petroleum Refineries and Petrochemical Plants. 2008*; p 11.

76 "HTHA is dangerous, difficult to detect and can be missed. The reliability of HTHA inspections depends on the skill of the inspector." *See:* Birring, A., Ultrasonic Testing - Detection of Hydrogen Attack, *See:* http://www.nde.com/hydrogen.htm, (accessed June 13, 2013).

77 API RP 571. *Damage Mechanisms Affecting Fixed Equipment in the Refining Industry.* 2003; p "5-83".

4.2 Tesoro Heat Exchanger Failure

4.2.1 NHT Heat Exchanger Construction

The NHT heat exchangers were constructed in 1971 and installed and placed in service in Anacortes. The two banks of three heat exchangers were metallurgically identical; the pressure containing "shell" base material for each heat exchanger in the bank was specified based on the design operating conditions.

Exchanger	Shell-Side Materials of Construction
A/D	Mn-0.5Mo steel (SA-302-B), factory clad[78] with 1/8" thick Type 304 stainless steel.
B/E	Carbon steel (SA-515-70), factory clad with 1/8" thick Type 316 stainless steel applied to the 4' Section 4 (Can 4) as shown in Figure 18.[79]
C/F	Carbon steel (SA-515-70).

The general construction of each heat exchanger shell consisted of a series of four steel sections, called "Cans" welded to form a cylinder (exchanger shell). This construction required a longitudinal weld to form each "Can" or section, and three circumferential welds to join the four sections end to end. The B and E heat exchanger design is shown in Figure 18.

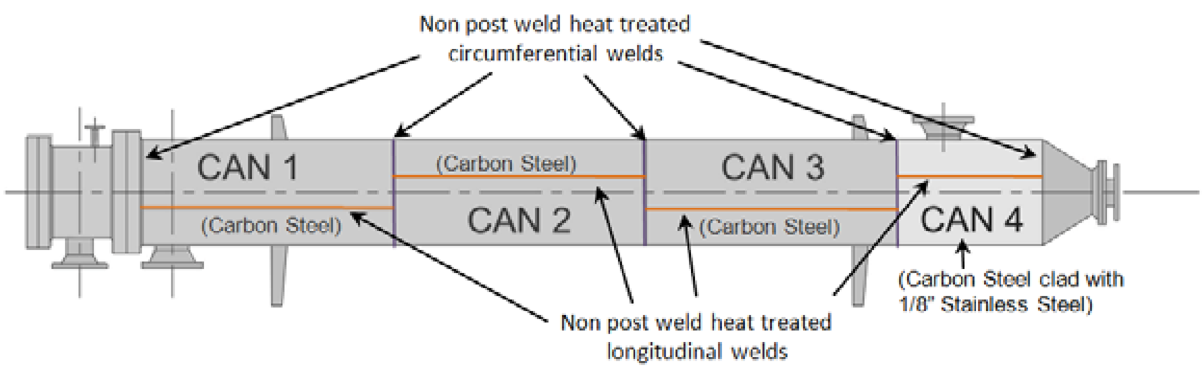


Figure 18. Fabrication Layout of the B and E Heat Exchangers

Design data representing anticipated normal operation and the API RP 941 Nelson curves were used to select materials of construction for the NHT heat exchangers. Carbon steel was selected for the B and E heat exchangers because the design temperatures were below the carbon steel Nelson curve. "Can" 4 of the B and E heat exchangers, the hottest portion of the heat exchangers, was lined on the interior surface with a layer of Type 316 stainless steel on top of the carbon steel. The interior stainless steel was applied in a process known as "cladding." The stainless steel was selected for protection against another damage

[78] Cladding is a process used to join dissimilar metals together to form a single metal piece.
[79] The remaining portions of the exchanger shell (Cans 1, 2, and 3) did not have a 316 stainless steel cladding.

mechanism called sulfidation corrosion.[80] Although protection from sulfidation corrosion is the intent of the stainless steel cladding, the cladding also can be used to reduce the risk of HTHA. The stainless steel cladding reduces the effective hydrogen partial pressure that is acting on the carbon steel beneath the cladding.[81]

The welding construction method used to manufacture the B and E heat exchangers resulted in a large heat-affected zone (HAZ).[82] An example of the welds used to construct the E heat exchanger is shown in a cross-section micrograph in Figure 19.[83] The top of the micrograph is the outside of the heat exchanger shell carbon steel wall.[84]

---

[80] Sulfidation is a damage mechanism that causes thinning in iron-containing materials, such as steel, because of the reaction between sulfur compounds and iron at temperatures ranging from 450 °F to 800 °F. This damage mechanism causes the metal to gradually thin over time.

[81] API RP 941. *Steels for Hydrogen Service at Elevated Temperatures and Pressures in Petroleum Refineries and Petrochemical Plants.* 2008; p 10.

[82] The process of welding requires substantial heat that alters the material properties of the material near the weld. This affected area near the weld is commonly referred to as the “heat-affected zone” or “HAZ”, shown in Figure 19.

[83] Beta Laboratory, Beta Lab No.M10198, Tesoro Ls2 And Ls2/Cs2 Tee Findings, October 13, 2010 (Appendix H)

[84] Figure 19 also shows the elements of a typical weld in the B and E heat exchangers.

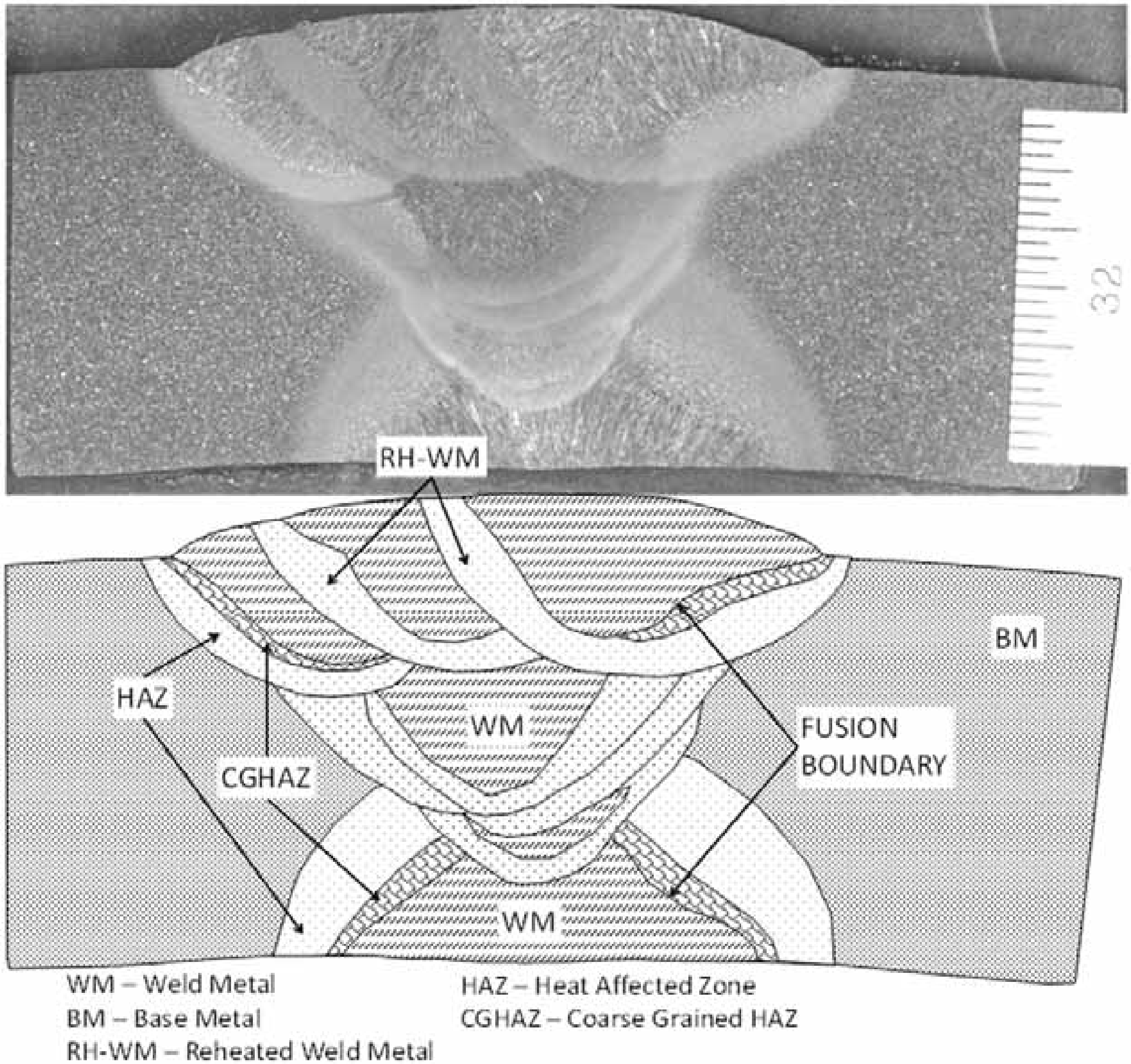


Figure 19. Cross-Section of Sample NHT Heat Exchanger Weld.[85] The cross-section of a multipass weld in the upper graphic is typical of the heat exchangers, and the schematic in the lower graphic defines the terms associated with the weld.

The welds in the B and E heat exchanger shells were not post-weld heat-treated.[86] As a result, the heat-affected zones illustrated in Figure 19 were likely high-stress areas where HTHA damage ultimately accumulated.

[85] *See* Appendix I, Figure 5.

[86] Some components of the heat exchangers were post-weld heat-treated, where wall thickness was at least one inch.

4.2.2 Post-Incident Metallurgical Analysis

BETA Laboratory, located in Mayfield Village, Ohio, conducted metallurgical testing of the B and E heat exchangers through an agreement among Tesoro, the Washington Division of Occupational Safety and Health (DOSH), and the CSB. BETA Laboratory compiled a series of reports, included in Appendix H, on the failed heat exchanger (E) and the exemplar heat exchanger (B)[87] that was removed from service after the accident at Tesoro. Test results indicate that the E heat exchanger failed at the heat-affected zones of the welds surrounding and within "Can" 3, as illustrated in Figure 20.

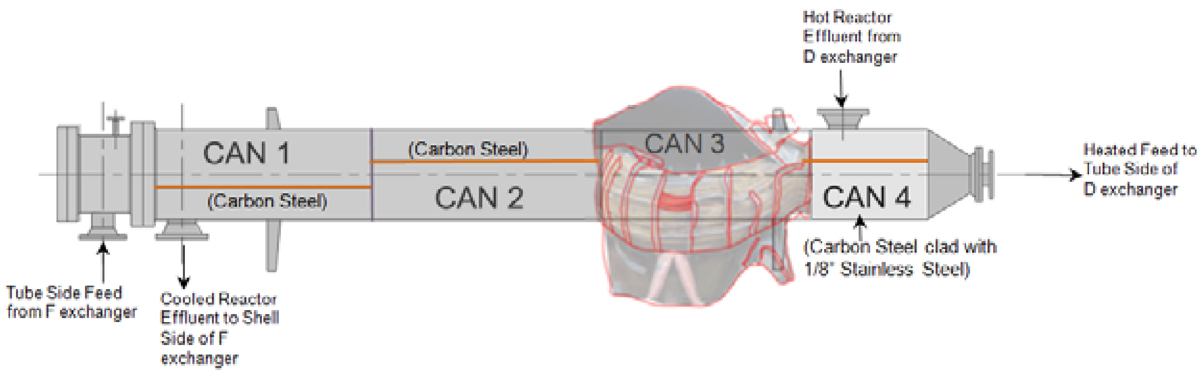


Figure 20. E Heat Exchanger Failure Schematic

The CSB contracted with the National Institute of Standards and Technology (NIST)[88] to perform an independent analysis of the BETA Laboratory reports and to prepare a report that states a professional opinion of the failure mechanism that caused the rupture of the E heat exchanger.[89] NIST metallurgical experts conducted the analysis.

HTHA was the immediate cause of the heat exchanger failure.

NIST determined that the metallurgical damage that caused the failure of the E heat exchanger was a result of HTHA, with other possible contributing co-mechanisms such as hydrogen-induced cold cracking that may have served as HTHA initiation points in the heat affected zones. The full metallurgical analysis is included in Appendix I.

The documented HTHA damage for the failed E heat exchanger is extensive. Damage is evident in the base metal but only in the heat-affected zone adjacent to welds and along fusion boundaries

[87] The B exchanger was used as an exemplar during metallurgical testing because it experienced nearly identical process conditions and had the same geometry and materials as the E exchanger.

[88] NIST is a non-regulatory federal agency in the U.S. Department of Commerce. The NIST mission is to promote US innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance the economic security of the nation and improve the quality of life of citizens. *See* http://www.nist.gov/public_affairs/general_information.cfm (accessed December 30, 2013).

[89] *See* CSB's E-6600E and E-6600B Metallurgical Analysis report (Appendix I).

in the welds. No HTHA damage is evident in the base metal outside of the heat-affected zone.[90] Because the fracture paths followed the narrow damaged regions along the welds, much of the damage in these regions was incorporated into the fracture surfaces during the failure as these damaged regions connected to form the macro-fracture.

Similar HTHA damage is also evident and documented in the exemplar B heat exchanger that was unaffected by the incident. The HTHA damage in this heat exchanger is similar to the damage documented in the uncompromised portions of the E heat exchanger. Long and deep subsurface cracks are evident. In the case of the B heat exchanger, one circumferential weld heat-affected zone crack extends over 50 percent of the way around the circumference and more than one third of the way through the thickness of the heat exchanger shell wall,[91] as shown in Figure 21 and Figure 22.

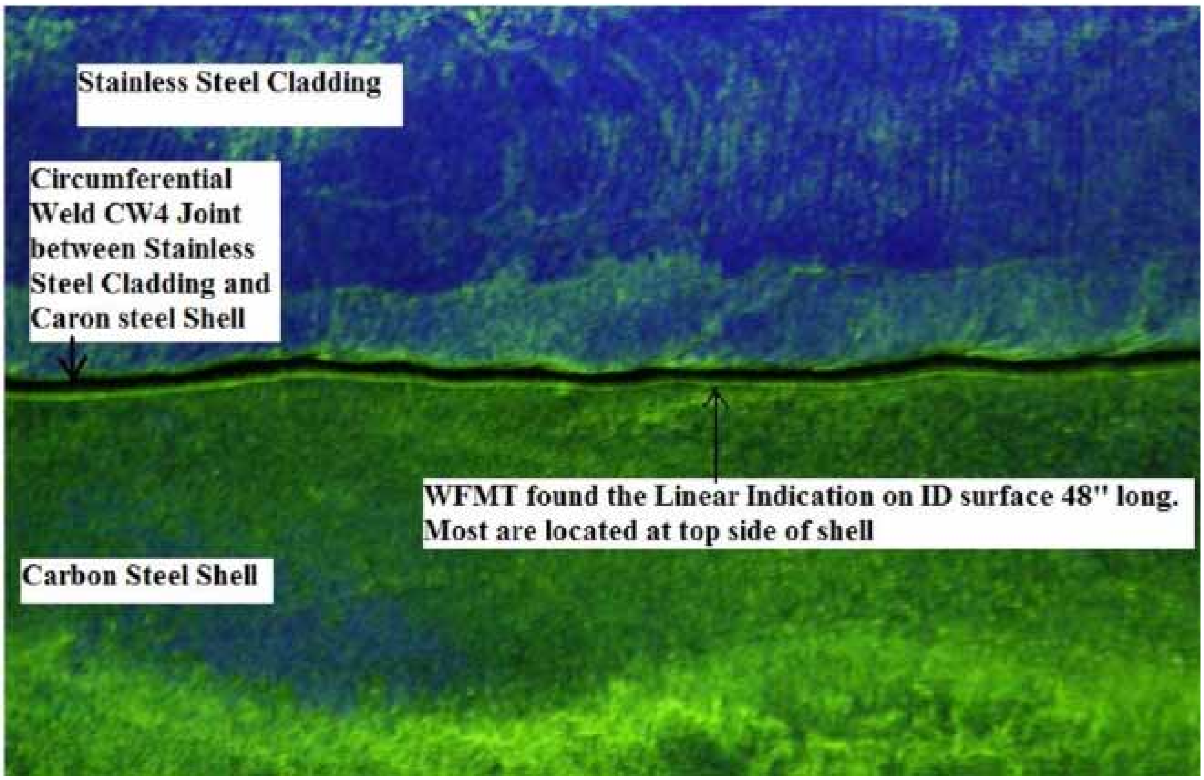


Figure 21. Circumferential Weld Damage in the B Heat Exchanger. This photograph from the Spectrum inspection report on the B heat exchanger (Appendix G) shows the large crack directly downstream of the stainless steel clad portion of the heat exchanger. (The light green line below the dark black area is the crack; the dark portion is the edge of the stainless steel cladding.) This macrocrack formed in the high-stress region near the weld because of the linkage of microcracks and fissures caused by HTHA.

[90] *See* Appendix J

[91] *See* CSB's E-6600E and E-6600B Metallurgical Analysis report (Appendix I).

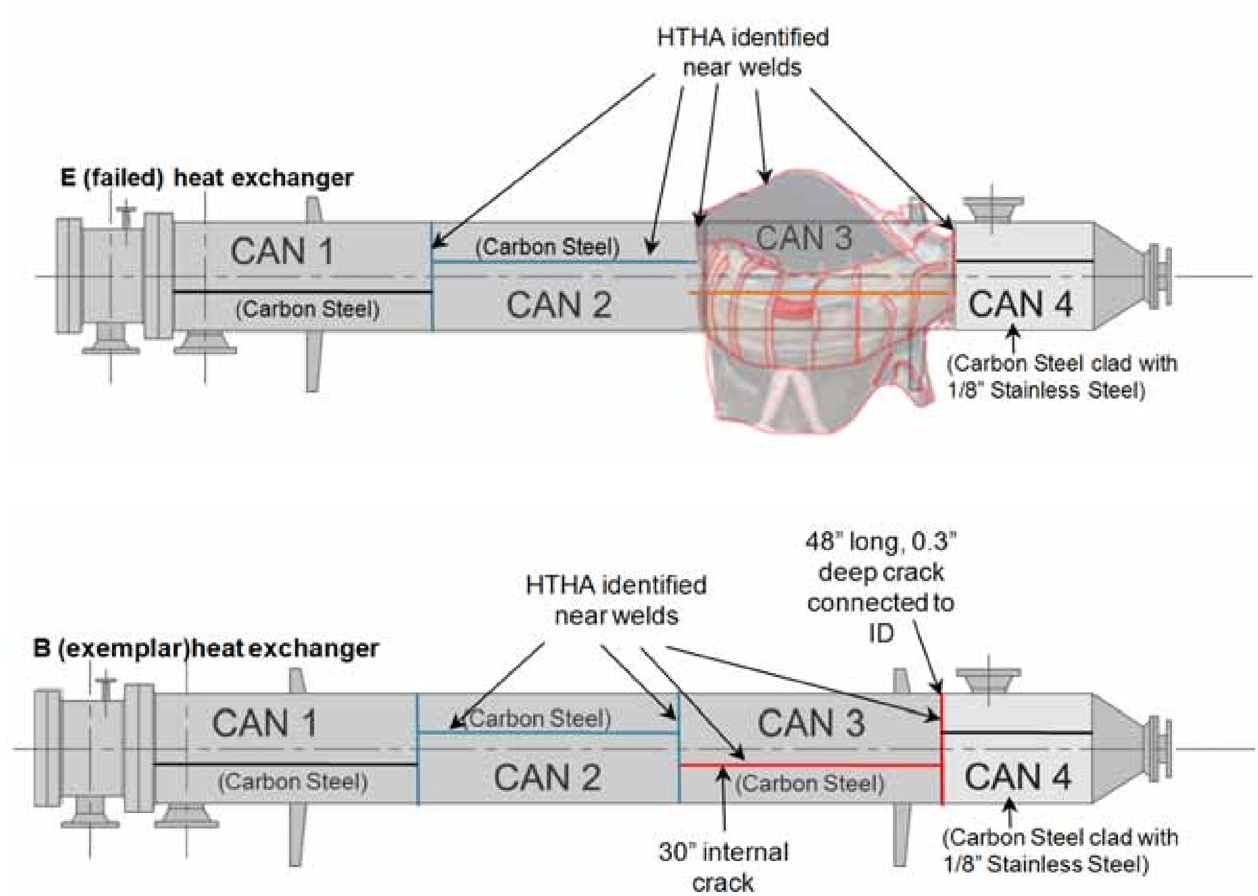


Figure 22. Comparison of Damage Locations in the B and E Heat Exchangers. Severe HTHA damage is found in the B heat exchanger in the same locations where the E heat exchanger ruptured.

NIST determined that without the HTHA damage, it is unlikely that the E heat exchanger would have ruptured under the conditions that occurred during the April 2010 start-up. However, both the B and E heat exchangers were severely degraded and had the potential to suffer a catastrophic rupture because of the advanced stages of HTHA evident in both heat exchangers.

4.3 Timing of the Incident

Process data indicate that the D/E/F tube outlet temperature increased about 75 °F over a span of three minutes immediately before the rupture, as graphed in Figure 23. The CSB compared these changes in temperatures to those from the previous three startups. This magnitude of temperature increase is typical compared to the previous startups (Appendix B) and is likely explained by the difficulty of trying to maintain process control by manually operating large isolation block valves that were not designed as flow control valves.[92]

The E heat exchanger was in a severely degraded mechanical condition because of long-term cracking damage from HTHA. In addition to the increased mechanical stress from the startup of the A/B/C heat exchangers, this momentary increasing temperature appears to have been sufficient to cause the actual material strength of the critically weakened heat exchanger to be exceeded, rupturing the E heat exchanger at its weakest point – the area of the heat exchanger that was most damaged by HTHA. This scenario is the most likely explanation of the timing of the failure of the heat exchanger during the A/B/C heat exchanger startup, but it did not cause the failure.

[92] A block valve is a manually operated valve that is normally fully open or fully closed. Block valves are typically designed for tight shutoff when closed and for minimal obstruction of flow when open. These valves are not designed to throttle or control flow.

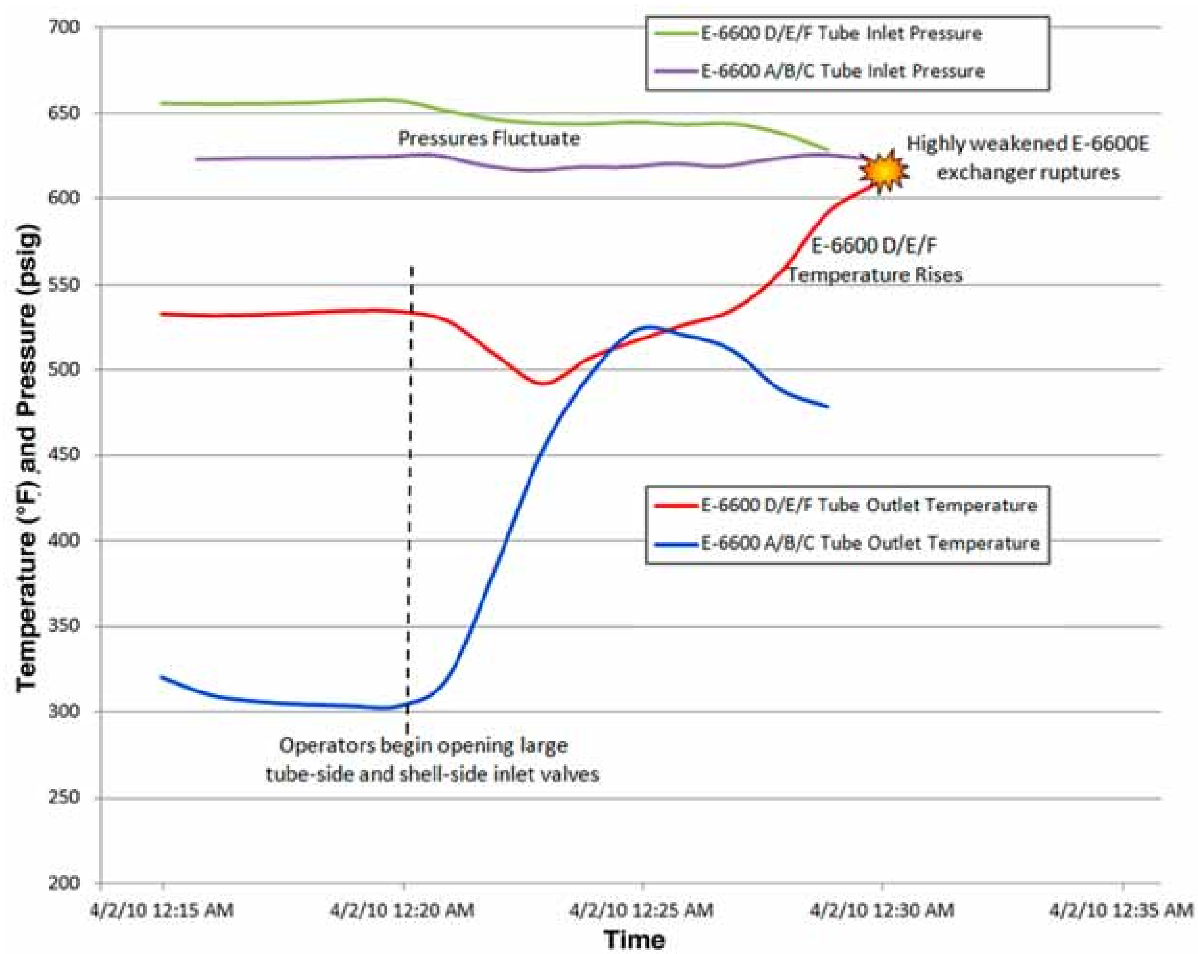


Figure 23. Temperature and Pressure Trends before the Anacortes Incident

4.3.1 NHT Heat Exchanger Startup Conditions

The CSB examined startup activities and process data at the time of the incident and concluded that no equipment mechanical integrity code parameters were exceeded. Temperature trends from the time when the A/B/C heat exchanger bank was coming on-line were compared to those from the three previous startups (as explained in Appendix B). All of the temperature trends are similar. The maximum allowable working pressure of the E heat exchanger was 655 psig at 650 ºF. The operating data indicate that the design temperature of 650 ºF was not exceeded before the rupture.

The E heat exchanger was protected from excessive pressure by a pressure relief valve on a downstream vessel, which was set to relieve the pressure at 585 psig.[93] Operating data indicate that the pressure relief valve was not challenged and did not open before the incident. The relief valve was inspected and tested after the incident, and it opened at the designated set pressure.

93 This relief valve is located further downstream in the process. As a result the exchanger pressure is higher than the relief valve set pressure. This pressure difference is accounted for by the engineering design and documented in the relief system calculations.

As a result of this analysis, the CSB excluded improper operation of the NHT heat exchangers during startup as a plausible contributing cause of the incident.

4.4 Process Conditions of the B and E Heat Exchangers

In refineries and chemical plants, key temperatures, pressures, flow rates, and other data are typically measured using a distributed control system (DCS). This system tracks and records data reported to the system via instrumentation in the plant and can visibly display important variables to control room operators. Operators also can manually record data from field instrumentation that does not report to the DCS.

Tesoro monitored temperatures and pressures of the process fluid entering and exiting the NHT heat exchanger banks, via both local field instrumentation and instrumentation that reported to the DCS. The locations of the temperature (TI) and pressure (PI) indicators are shown in Figure 24.

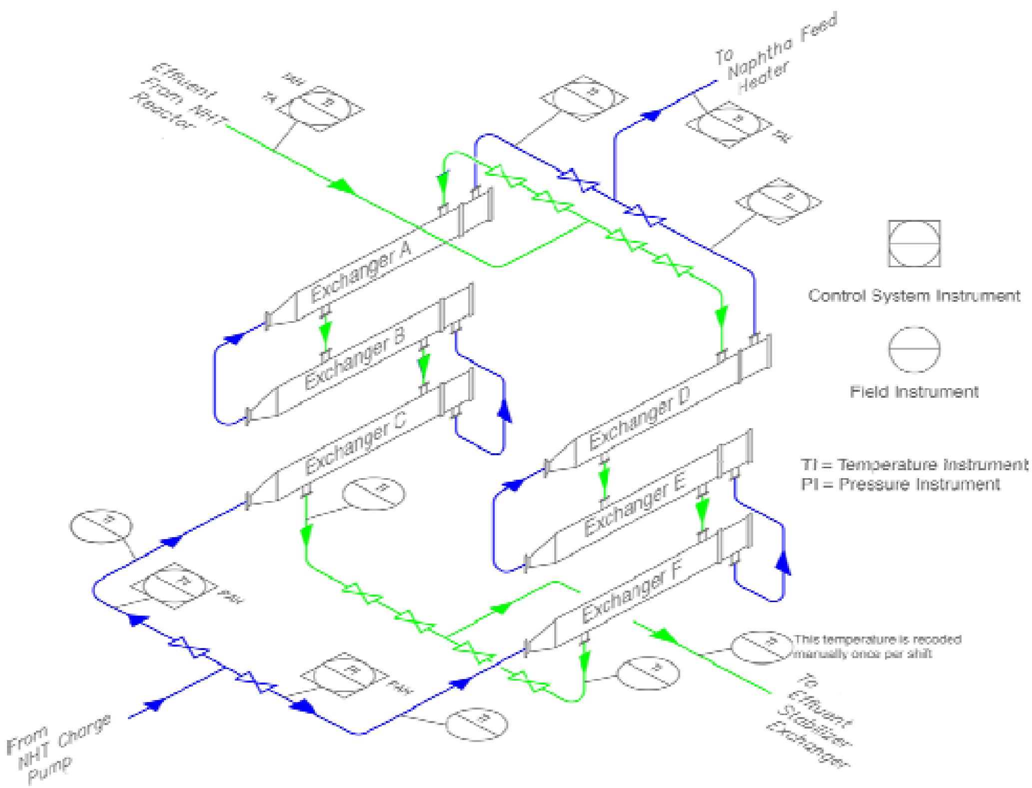


Figure 24. Temperature and Pressure Indicators for the NHT Heat Exchanger Banks. This isometric process flow view depicts the lack of temperature indication on both the shell-side and tube-side of the B and E heat exchanger inlets and outlets.

Although some temperature and pressure measurements were taken surrounding the NHT heat exchanger banks, no temperature measurements were made between the heat exchangers. Thus, Tesoro did not know the operating temperature of the process fluid entering and exiting the B and E heat exchangers.[94] Had Shell Oil or Tesoro performed a technical evaluation or installed instrumentation to monitor temperatures at these locations, a better evaluation of potential HTHA hazards could have been performed, and more effective safeguards could have been implemented.

The B and E heat exchangers lacked instrumentation to monitor shell-side inlet temperatures.

4.4.1 CSB Modeling of the NHT Heat Exchangers

Because of the minimal temperature measurements of the NHT heat exchanger banks, the CSB performed process modeling to estimate the operating temperatures and hydrogen partial pressures of the B and E heat exchangers by using computer-based chemical process design software packages.[95] The model required the use of several assumptions, such as fouling distribution, because of a lack of both process and fouling data gathered by Shell Oil and Tesoro. Consequently, all model results are estimates of the actual process conditions experienced by the NHT heat exchangers. The CSB used the model to estimate the operating conditions of each heat exchanger based on the available Tesoro operating data, including temperatures, pressures, flow rates, and fluid composition data. The model development process and associated results are described in Appendix C. A summary of the modeling results is depicted in Figure 25, Figure 26, and Figure 27.

[94] A single external surface temperature measurement of 455 ºF was taken in October 1998 on the inlet to either the B or E exchanger.

[95] Aspen HYSYS and Aspen Exchanger Design and Rating.

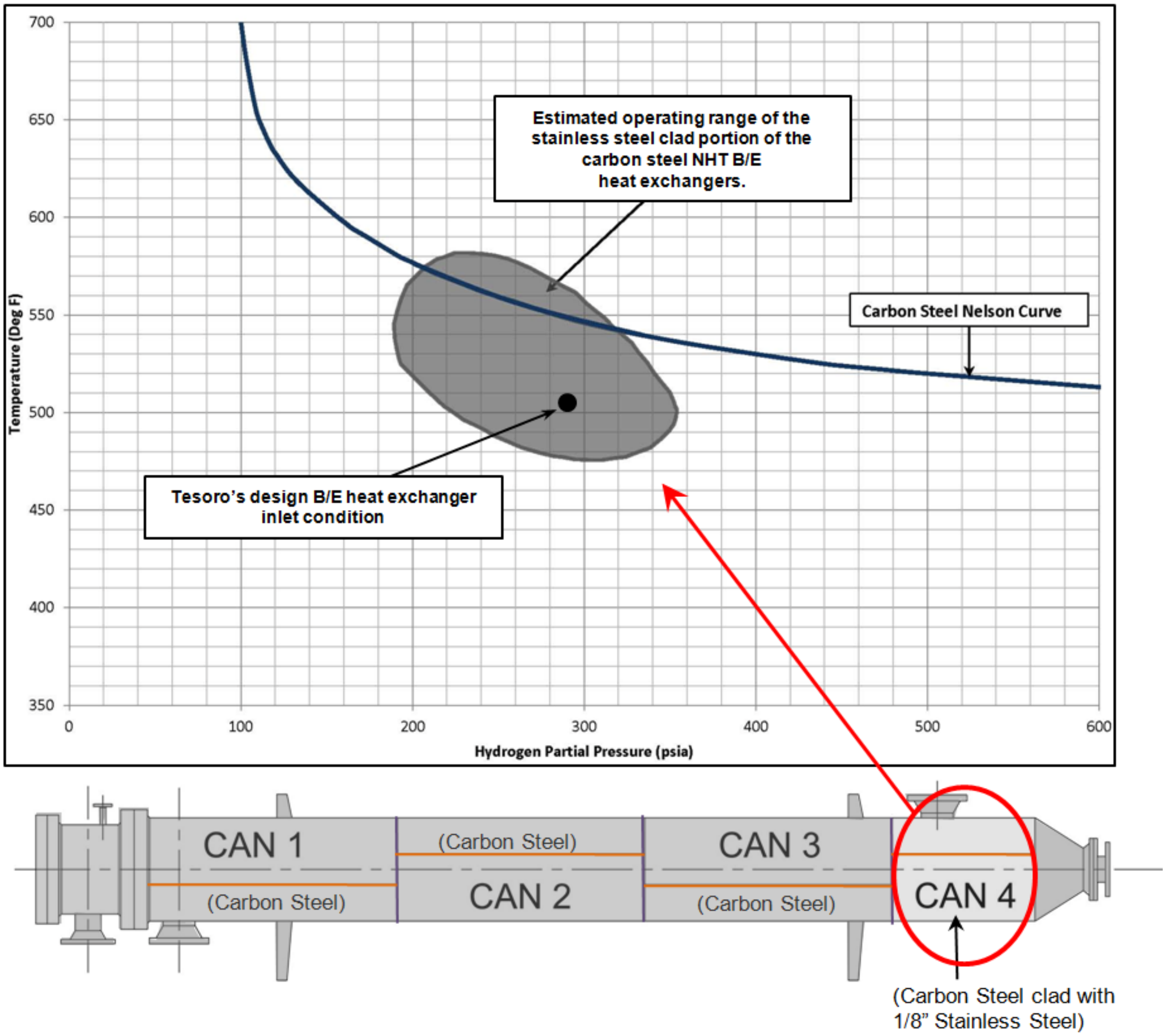


Figure 25. Model Results for Can 4. The stainless-steel-clad portion of the carbon steel B and E heat exchangers was estimated to occasionally operate above the carbon steel Nelson curve. No HTHA was found in this region, likely because stainless steel cladding reduced the potential for HTHA in the carbon steel beneath it. Tesoro's design B and E process condition used for HTHA evaluation (504 °F and 291 psia hydrogen partial pressure) did not represent the entire range of heat exchanger operating conditions.

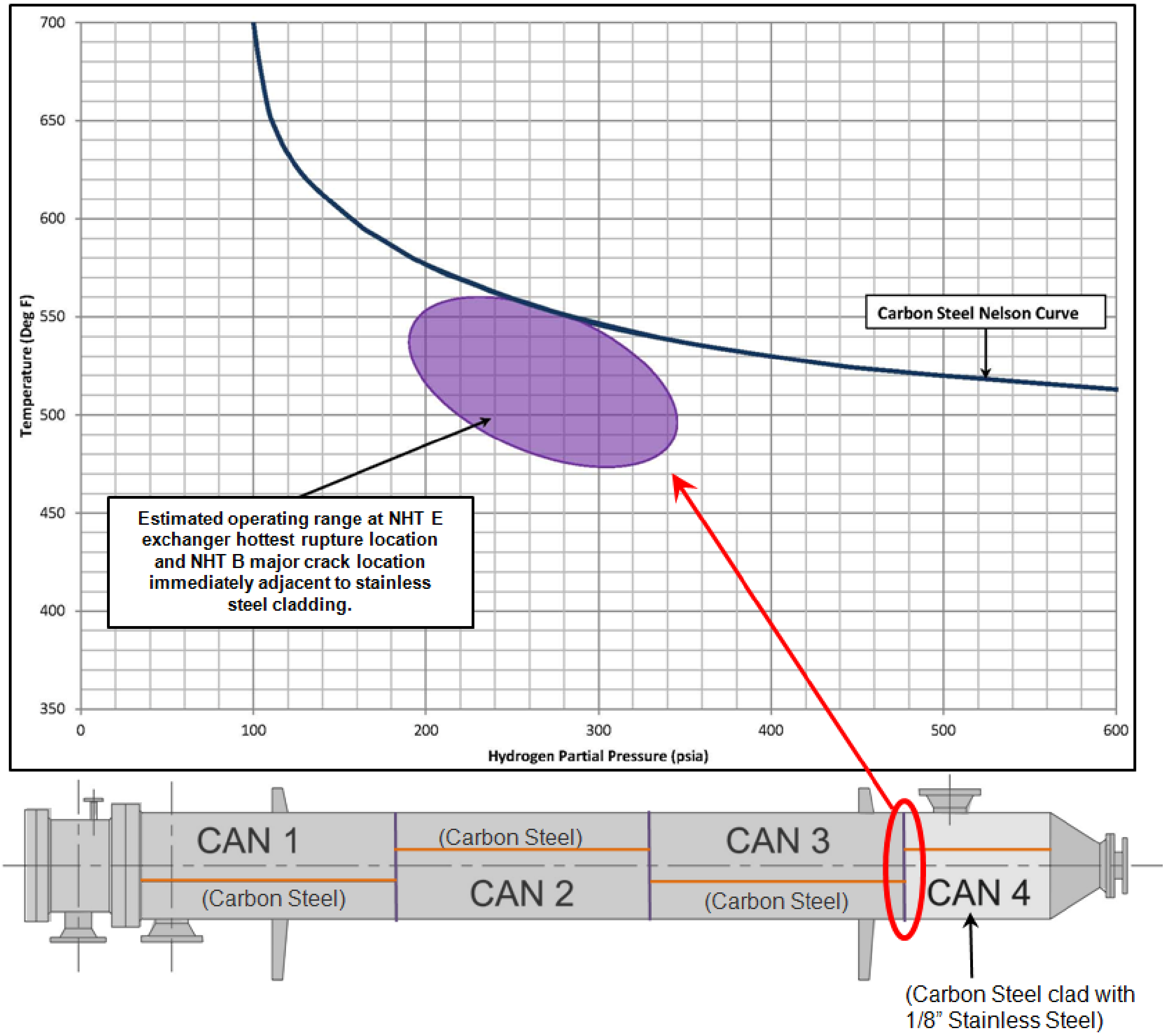


Figure 26. Model Results for the Weld Downstream of Can 4. The circumferential weld immediately downstream of the stainless-steel-clad portion of the carbon steel B and E heat exchangers was estimated to operate just below the carbon steel Nelson curve. Extensive HTHA was found in this region, the hottest rupture location of the E heat exchanger and the major crack location of the B heat exchanger.

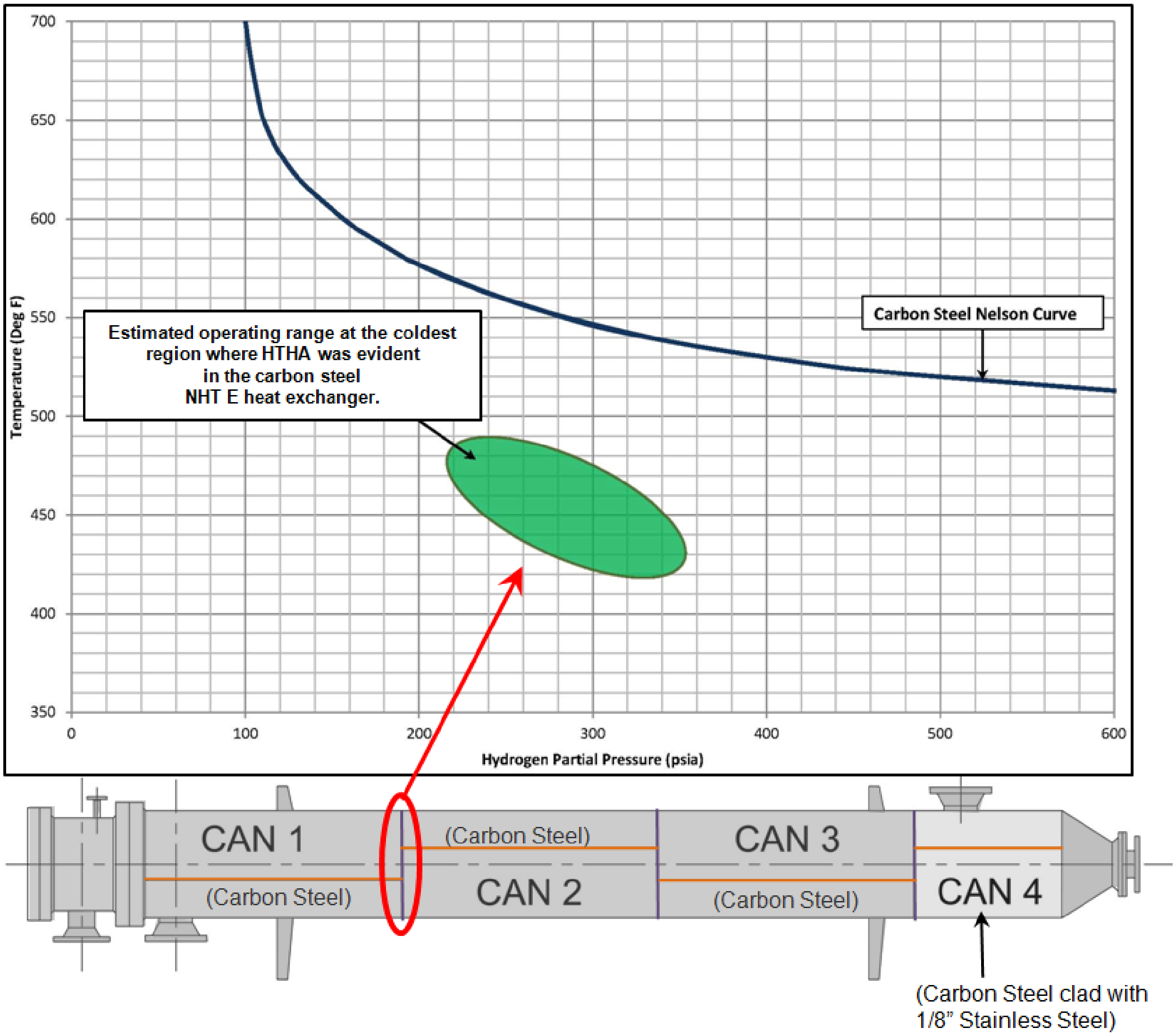


Figure 27. Model Results for the Coldest Region of the E Heat Exchanger. The coldest region of the E heat exchanger with evident HTHA was estimated to operate as much as 120 ^{0}F below the carbon steel Nelson curve.

4.4.1.1 HTHA Occurred Below the Nelson Curve

HTHA was found in locations that were estimated to operate up to 120 ^{0}F below the carbon steel Nelson curve.

CSB process modeling estimates demonstrated that the hottest portion of the B and E heat exchangers with evident HTHA, the circumferential weld between "Can" 3 and "Can" 4, operated below the carbon steel Nelson curve. HTHA was also identified at the circumferential welds between "Can" 2 and "Can" 3, and also between "Can" 1 and "Can" 2. Modeling results also indicate that the coldest region in the E heat exchanger[96] with identified HTHA was estimated to have operated up to 120 °F below the carbon steel Nelson curve. This finding suggests that the long-standing industry carbon steel Nelson curve is inaccurate—it cannot be relied on to prevent HTHA equipment failures, and it cannot be reliably used to predict HTHA equipment damage.

4.4.1.2 Estimate That a Portion of the B and E Heat Exchangers Operated Above the Nelson Curve

The CSB modeling analysis estimated that during operation while fouled, the stainless-steel-clad portion of the B and E heat exchangers at times likely operated above the carbon steel Nelson curve. This section was not damaged by HTHA, probably because the stainless steel cladding protected the carbon steel beneath it. As discussed in Section 5.3.3, operation near or above the carbon steel Nelson curve should have triggered an inspection for HTHA by Tesoro, but the company never performed such an inspection.

4.4.1.3 Tesoro's Replacement Heat Exchangers

Since the April 2010 incident, Tesoro has installed new NHT heat exchangers with upgraded materials of construction to significantly reduce the potential for HTHA.[97] In addition, an advanced process control system is in place to minimize fouling. The heat exchangers are also constructed using only one bank of exchangers. The entire NHT unit now must be shut down for cleaning, eliminating the hazards of online switching and creating a much safer approach for maintenance. The new heat exchangers also incorporate additional instrumentation to allow the monitoring of each heat exchanger for fouling and decrease the likelihood of operation in HTHA-susceptible conditions.

[96] HTHA was not conclusively identified in the B heat exchanger in this region. Only a limited metallurgical analysis was performed on the seam between Can 1 and Can 2 of the B heat exchanger.

[97] Although the materials of construction are upgraded in the new exchangers, portions of the heat exchangers that use carbon steel are designed to operate at temperatures of more than 400 °F.

5.0 Organizational Deficiencies

Similar to the results of the CSB investigation of the disastrous March 2005 explosion at the BP Texas City site, the CSB identified deficiencies in the process safety culture and organization at the Tesoro Anacortes Refinery that contributed to the April 2, 2010, incident. At the time of the incident, deficiencies in the Tesoro process safety culture and organization coincided, with catastrophic consequences. The organizational deficiency allowed many personnel in a hazardous region, and the process safety culture problems led to a failure to control HTHA hazards, resulting in a major fire and the loss of seven lives.

5.1 NHT Heat Exchanger Flanges – A History of Leaking

During startup following cleaning, the NHT heat exchangers would frequently leak from flanges, occasionally resulting in fires that created hazardous conditions for workers. This hazard had persisted for more than a decade; the CSB found that the earliest documentation of these leaks was from 1997, when Shell Oil owned the refinery.

Over the years, Tesoro attempted maintenance and engineering solutions to stop the heat exchanger leaks. In 2008, management and labor even jointly conducted a triangle of prevention (TOP)[98] investigation that analyzed, in part, the NHT heat exchanger leaks. However, these attempts did not effectively resolve the problem of the heat exchangers leaking during startup; as a result, various operational techniques were developed to accommodate the fact that the leaking would typically cease once the heat exchangers stabilized at their normal operating temperatures. The leaks were very hazardous as the hot naphtha was highly flammable[99] and had the potential to be operating above its autoignition temperature. However, because these leaks were never effectively prevented, the leaks from the NHT heat exchangers during startup became an accepted and normalized condition at Tesoro.

> **Tesoro accepted and normalized the hazardous condition of frequent leaks during exchanger startup.**

[98] The TOP program is a joint union-management workplace safety program that applies the knowledge of the workforce to understand and eliminate workplace hazards.

[99] The flash point is defined as the minimum temperature at which a liquid gives off sufficient vapor to form an ignitable mixture with air near the surface. The Tesoro Material Safety Data Sheets (MSDSs) for naphtha list its flash point as -7.1 ºF. Liquids with a flash point of less than 23 ºF fall into the highest hazard category of the Globally Harmonized System of Classification and Labeling of Chemicals (known as the GHS). See: https://www.osha.gov/dsg/hazcom/ghs.html#3.1 (accessed December 31, 2013).

5.1.1 Incident Report That Demonstrates Normalization of Hazardous Conditions

The CSB identified an incident report describing a startup of the NHT D/E/F heat exchanger banks in March 2009, a year before the April 2010 incident, that resulted in the exposure of workers to hazards from both hot steam and leaking hydrocarbons while they put the NHT heat exchangers back in service. This incident report demonstrates the normalization of hazardous conditions that had been established at the refinery.

The 2009 report states that the "exchangers leaked substantially" and that the leaks were "steady streams" flowing from each of the three heat exchangers being put in service. The incident report then describes how workers responded to the leaks by continuing the startup, while wearing only standard refinery personal protective equipment, to reach the desired heat exchanger temperatures. This long-standing practice was used to stop atmospheric hydrocarbon releases from the NHT heat exchangers. The report states that "[s]team lances were positioned at all leak locations." Tesoro employees "continued the startup of the heat exchangers while monitoring leak status .…" Eventually, the target exchanger temperatures were achieved, and the leaks stopped.

This continuation of the startup – despite the exposure of workers to significant hazards – demonstrates the normalization of the extremely hazardous NHT heat exchanger leaks. The leaking of high-temperature, highly flammable process fluids constitutes a serious process safety incident. However, during the 2009 incident, the refinery alarm was not sounded; an emergency response team was not activated; the leak was not isolated from the unit; and the unit was not shut down. The incident report also did not address the need for permanent corrections to stop the leaks. Although Tesoro did make additional attempts to correct the heat exchanger leaks as discussed in Section 5.1.4, ultimately these efforts were unsuccessful and the CSB found that leaks did occur during the startup of the NHT heat exchangers on the night of the April 2010 incident.

5.1.2 TOP Investigation of Fires

In 2008, a TOP investigation team was assembled to begin what would become a ten month investigation into a series of loss of containment incidents at the Tesoro Anacortes Refinery, including some that resulted in fires. In all, fourteen refinery incidents that occurred between May 2003 and December 2007 were investigated during this process. The TOP team investigation included the frequent leaks from the NHT heat exchangers during startup.

The findings of the Tesoro TOP investigation team included the following:

- Tesoro classified incidents involving incipient fires[100] as "level 1" incidents that are reported but do not require investigation. The 2008 TOP investigation was launched after multiple level 1

[100] In 29 CFR 1910.155(c)(26), OSHA defines "incipient stage fire" as a fire that is in the initial or beginning stage and that can controlled or extinguished by portable fire extinguishers, a class II standpipe, or small hose systems without the need for protective clothing or breathing apparatus.

incidents appeared to have common causal factors. The report noted that it was very difficult to complete a proper TOP investigation when many of the incidents were so far in the past.

- NHT heat exchanger leaks were common during startup. However, because the leaks tended to stop after operating temperatures were reached, incident reports were sometimes not filed. The incidents were treated as "normal" startup events, and steam lances were considered to be acceptable leak mitigation. The TOP investigation team noted complacency at the refinery because these events were so common and also cited a growing lack of concern toward activating emergency response.
- A Tesoro mechanical engineer had at one time actively pursued mitigation of NHT heat exchanger leaks. Procedural changes for startup and shutdown were made, and the heat exchanger gasket surfaces were repaired. However, the engineer left Tesoro, and no further progress was made because of a combination of poor communication and a lack of implementation tracking.
- Only one of the fourteen incidents investigated had prompted a previous TOP investigation, even though five of the fourteen investigated incidents involved fires in process units. The TOP investigation team concluded that this complacency in investigation practices caused associated complacency in the workforce toward process-related fires.

5.1.3 MOCs Did not Effectively Control Hazardous Conditions

A contributing factor to the presence of some of the six additional personnel in the NHT unit at the time of the April 2010 incident was likely the need for them to assist with steam lance use in anticipation of leaks during startup.[101] Relying on steam suppression to mitigate leaks during NHT heat exchanger startups was a common practice and was part of the startup procedure. In October 2009, Tesoro approved a Management of Change (MOC) to install two new permanent steam stations near the NHT heat exchangers, shown in Figure 28.[102]

101 The CSB identified four steam lances near the NHT heat exchangers following the April 2010 incident. Three of the four steam lances were likely active at the time of the incident.

102 The "Purpose" of the change was to "Provide improved response time and safety when responding to flange fires in the vicinity of the E-6600 exchanger structure." However, the steam equipment was installed in the immediate vicinity of the exchangers and nothing prohibited this steam suppression equipment from being used to mitigate a leak from the exchangers. The project to install additional steam suppression equipment was competed in January 2010. One of the new steam stations is shown in Figure 28.

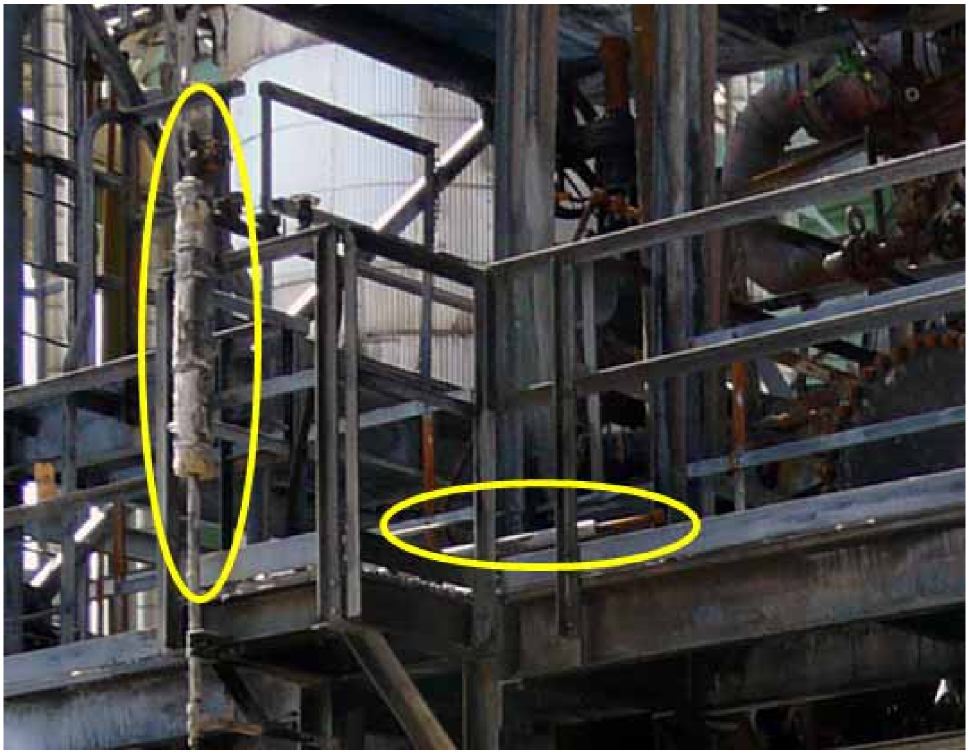


Figure 28. Steam Station and Steam Lance. This post-incident photograph shows a new steam station (left) with a connected steam lance (right).

MOC is one of the 14 elements of the state of Washington PSM regulations.[103] Although the PSM regulations impose a general requirement to perform a PHA [104] at least every 5 years, a formal hazard evaluation is not required for an MOC. The Tesoro MOC policy states, "Management of Change helps ensure that changes to a process do not inadvertently introduce new hazards or unknowingly increase the risk of existing hazards." However, Tesoro decided that a hazard evaluation of the addition of steam stations was not required under their procedures because additional steam stations only involved a minor change to a utility system. Yet, the installation of the additional steam equipment enhanced the ability of the field operator(s) to confront hazardous leaks and extinguish fires in the area of the NHT heat exchangers, and the safety implications of these activities were not considered.

[103] MOC is one of the 14 elements of the WAC rules for PSM of highly hazardous chemicals. *See* http://www.lni.wa.gov/wisha/rules/hazardouschemicals/#WAC296-67-045 (accessed December 25, 2013). MOC is also required by EPA RMP (See http://www.epa.gov/oem/content/lawsregs/rmpover.htm. (accessed December 25, 2013)) and is an element of the federal OSHA PSM regulations (*See* https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=STANDARDS&p_id=9760 (accessed December 25, 2013).

[104] A PHA is a hazard evaluation to identify, evaluate, and control the hazards of a process. Facilities that process a threshold quantity of hazardous materials, such as the Tesoro Anacortes Refinery, are required to conduct a PHA per the WAC Title296 Chapter 67, Safety standards for PSM of highly hazardous chemicals (1992). *See:* http://apps.leg.wa.gov/wac/default.aspx?cite=296-67 (accessed September 29, 2013) PHAs are also required by the federal EPA RMP.

Good practice guidelines such as those published by the CCPS advise that a hazard assessment should be performed during MOC reviews.[105] Tesoro should have conducted a formal hazard evaluation for the MOC and should have considered more robust alternatives to steam lances such as protecting workers by effectively correcting the mechanical problems that were causing the leaks.

Washington PSM regulations require MOC reviews to consider the impact of proposed changes on operating procedures.[106] However, operating procedures were not reviewed or modified as part of the MOC review conducted for the new steam suppression equipment. The existing NHT heat exchanger startup procedure only addressed field tasks for a single NHT outside operator. The procedure instructed the operator to have a steam hose (lance) ready in case a leak developed and to warm the heat exchangers slowly to prevent leaks, but if leaks did occur, to continue the startup as follows:

> Keep an active steam hose on hand in case of leaks.
>
> Slowly heating the bundle up to prevent leaks.
>
> Heating the exchanger too fast can cause leaks. If the heads begin to leak, they will usually reseal themselves as they come up to temperature.

When the ability to use multiple steam lances on the NHT heat exchanger leaks was provided, the operating procedure was not updated to reflect the ability for, and likely presence of, additional personnel to operate those steam lances. In addition, no guidance was developed or provided to establish how large a leak or fire the field operator(s) was expected to fight and no evaluation was made to assure there was proper allowance for emergency egress from a large leak or fire. Tesoro did not view the NHT heat exchanger startup and history of leaks as high hazard activity—a reflection of the normalization of the hazardous conditions.

5.1.4 Unsuccessful Tesoro Attempts to Prevent Heat Exchanger Flange Leaks

Tesoro sporadically made attempts to prevent the leaking of the NHT heat exchangers. These attempts included: gasket modifications, changes to torque and bolting practices, resurfacing of flange surfaces, and the installation of warm-up piping to smooth the transition from cold to hot equipment during heat exchanger startup. Following the severe leaks from the NHT heat exchangers during the March 2009 startup, in August 2009 Tesoro installed a different type of gasket in the NHT heat exchangers. During the startup that followed, Tesoro records indicate that no leaks from the heat exchangers occurred. Tesoro representatives told the CSB that this startup was evidence of "success" in correcting the NHT heat

[105] An important aspect of an MOC is assessing the hazards associated with proposed changes. The MOC team should determine the level of hazard evaluation needed for specific types of changes, but site management may decide that formal hazard evaluations are necessary for certain types of changes. The MOC process should provide sufficient information about the change to conduct a hazard evaluation. Center for Chemical Process Safety (CCPS). *Guidelines for the Management of Change for Process Safety*. 2008; pp 52-54.

[106] Modification to operating procedures is part of the MOC requirements addressed by the WAC process safety management regulations. *See* http://www.lni.wa.gov/wisha/rules/hazardouschemicals/#WAC296-67-045 (accessed December 25, 2013).

exchanger leaks. However, this was the last startup before the April 2010 incident, and a single successful startup without leaks is not evidence of long-term success.[107] One of the four steam lances likely used for leak mitigation on the night of the April 2010 incident is shown in Figure 29.

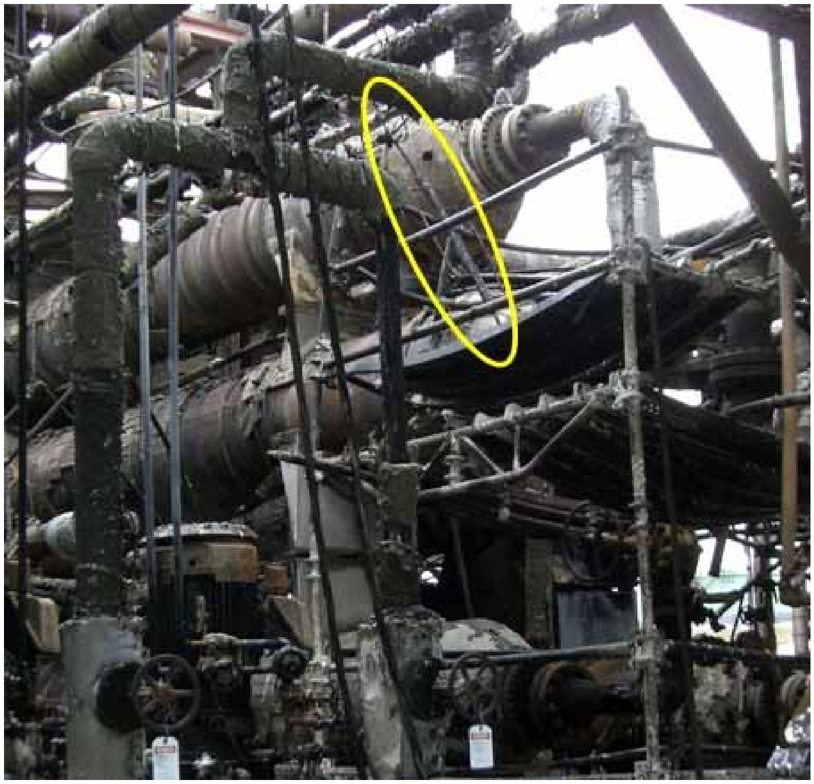


Figure 29. Post-Incident Steam Lance. This photograph shows a steam lance that was likely used during the startup.

In addition, the Tesoro Anacortes Refinery has a history of incidents related to gasket failures.[108] Despite industry best practices that require use of new heat exchanger gaskets, Tesoro documents indicate that the company noted that the new NHT heat exchanger gaskets, installed to prevent future startup leaks, could be re-used after subsequent cleaning cycles.[109] In contrast, gasket manufacturer guidance and industry

[107] On the night of the April 2010 incident, two different operators reported two leaks during the startup of the heat exchangers. One leak was reported just before the incident.

[108] Tesoro incident reports document a history of gasket failures at the refinery. A variety of causes were identified for these past failures including loose bolts, damaged gaskets, installation of the wrong gasket, defective gaskets, and other installation-related causes. The Tesoro 2008 TOP investigation identified a contributing cause to the fires in the NHT unit was that "[f]langes and/or gaskets may have been damaged due to poor access and high maintenance frequency."

[109] The notation indicated that the gasket vendor informed Tesoro that these gaskets could be re-used. Maintenance records indicate that the job plan did call for new gaskets.

best practice guidance indicate that new gaskets should be installed and that gaskets should not be re-used.[110,111]

Regardless, Tesoro's perceived "success" in resolving the NHT heat exchanger leaks in August 2009 did not result in the presence of fewer personnel during the April 2010 startup. In fact, Tesoro normalization of the hazardous NHT heat exchanger leaks ultimately contributed to the presence of a significant number of additional workers near the NHT heat exchangers at the time of the incident and thus a larger number of fatalities as a result of the heat exchanger failure.

5.2 Hazardous Nonroutine Work

Nonroutine work can be a highly hazardous operation. Work is performed on equipment that might or might not be shut down while adjacent equipment containing hazardous process material continues to operate. This type of operation places maintenance and operations personnel at risk. The CCPS provides the following guidance:

> Experience indicates that many accidents do not occur during "normal" operation but, rather, during such nonroutine modes of operation.[112]
>
> By its nature, nonroutine work carries with it the potential for unrecognized hazards that sometimes has led to a catastrophic incident.[113]
>
> During the period 1970 to 1989, 60 to 75% of major incidents in continuous processes occurred during "non-routine" modes of operation; i.e., in operating phases other than the continuous operation of the process after start-up.[114]

The 1989 Phillips Houston Chemical Complex fire and explosion, which killed 23 workers, expedited issuance of the PSM standard. Similar to the April 2010 Tesoro Anacortes Refinery incident, it involved the performance of hazardous nonroutine work in a running process unit.[115]

---

[110] When a flanged joint is opened, the gasket should be not be re-used. A new gasket should always be installed. Mannan, S. *Lee's Loss Prevention in the Process Industries, Hazard Identification, Assessment and Control*. Chapter 21, "Equipment Maintenance and Modification." p 25.

[111] Lamons. *Gasket Handbook*. 2012; p 113. *See* http://www.lamons.com/public/pdf/lit_reference/LamonsGasketHandbook2012.pdf (accessed December 27, 2013).

[112] Center for Chemical Process Safety (CCPS). *Revalidating Process Hazard Analyses*. 2001; pp 31-32.

[113] Center for Chemical Process Safety (CCPS). *Guidelines for Auditing Process Safety Management Systems*. 2011; p 393.

[114] Center for Chemical Process Safety (CCPS), *Guidelines for Hazard Evaluation Procedures*. 2008; p 257.

[115] U.S. Department of Labor. *A Report to the President: Phillips 66 Company Houston Chemical Complex Explosion and Fire*. April 1990; p 21.

The state of Washington's PSM regulations also stress the importance of employers identifying the hazards of nonroutine work in process areas and then communicating such hazards to those employees performing the work.[116]

Tesoro acknowledged both the potential hazards and relevance of nonroutine work to the Anacortes refinery incident in its own investigation report on the April 2010 incident.

> Continuous petroleum or chemical processes operate most effectively when they are in a steady state. Non-routine activities, including startup or shutdown, can create additional risks because parameters such as flow, temperature and pressure are in a state of flux.[117]

5.2.1 CSB Investigation of Tosco Avon Refinery

On February 23, 1999, a fire occurred in the crude unit at the Tosco Corporation's Avon oil refinery in Martinez, California.[118] Workers were attempting to replace piping attached to a 150-foot-tall distillation column[119] while the process unit was in operation. During removal of the piping, naphtha was released onto the hot distillation column and ignited. The flames engulfed five workers located at different heights on the column. Four workers were killed, and one worker sustained serious injuries.

The CSB investigated the incident and determined that the refinery's management system did not recognize or control the serious hazards posed by performing nonroutine repair work while the crude processing unit remained in operation.[120] Although the piping replacement activities at Tosco were dissimilar to starting up the heat exchanger bank at the Tesoro refinery's NHT unit, both involved hazardous nonroutine work.

A key conclusion and recommendation from the CSB 1999 Tosco investigation addressed the importance of advance planning and thorough hazard evaluations for the safe performance of higher hazard

[116] *See* WAC 296-67-291 Appendix C, *Compliance guidelines and recommendations for process safety management (nonmandatory)* http://www.lni.wa.gov/WISHA/Rules/hazardouschemicals/default.htm#WAC296-67-021 (accessed December 3, 2013).

[117] *See* TOP Investigation Team Report. *Naphtha Hydrotreater E-6600E Failure, 12:35 a.m., April 2, 2010, Anacortes Refinery, Washington.* p 21. http://www.tsocorp.com/stellent/groups/corpcomm/documents/gt_contribution/001347.pdf (accessed December 3, 2013).

[118] Ultramar Diamond Shamrock Corporation purchased the Avon oil refinery in September 2000 and renamed it the Golden Eagle Refinery. Tesoro purchased the Golden Eagle Refinery in 2002 and was the final party to respond to the CSB site-based safety recommendations from the 1999 Tosco incident.

[119] A distillation column is an oil refinery processing vessel that separates preheated hydrocarbon mixtures into various components based on boiling point. The separated components are referred to as fractions or cuts. Inside the column some trays draw off the fractions as liquid hydrocarbon products (such as naphtha), and piping transports them to storage or other units for further processing.

[120] CSB Investigation Report, Refinery Fire Incident – Tosco Avon Refinery, March 2001. *See* http://www.csb.gov/assets/1/19/Tosco_Final_Report.pdf (accessed December 4, 2013).

nonroutine work. Management has the obligation to identify hazards, implement effective controls and limit personnel exposure to higher-hazard work – but not meeting this obligation is a common failing, identified in both the Tesoro and Tosco investigations, that led to the catastrophic incidents. The CCPS recommends that companies considering tasks that entail employee access to hazardous areas should "minimize the number of people in harm's way should an incident occur."[121]

The likelihood of leaks occurring during the startup of the NHT heat exchangers made returning them to service a serious hazard to the workers involved. Similar to the Tosco incident, the serious hazards could have been more effectively controlled through the use of hazard evaluation techniques and more effective management control of the nonroutine work.

Unlike Tosco, Tesoro had years to evaluate the hazards and effectively control the frequent NHT heat exchanger leaks. Multiple incident reports were developed and hazard reviews were conducted. Each of these events presented opportunities for Tesoro to recognize the hazardous nonroutine work and effectively control the hazards. However, Tesoro never effectively corrected the hazardous startups and failed to limit access to a minimum number of essential personnel.

5.2.2 NHT Heat Exchanger Cleaning and Startup

While in operation, the NHT heat exchangers fouled, reducing heat transfer between the tube-side and shell-side process fluids. This reduction in heat transfer both increased shell-side outlet temperatures and decreased tube-side outlet temperatures. To maintain process requirements, the heat exchangers were periodically cleaned. Tesoro accomplished this task with hazardous nonroutine work, cleaning one bank of heat exchangers at a time while the remainder of the process continued to operate.

During this nonroutine work, one bank of heat exchangers was isolated, opened, and cleaned, while the other bank of heat exchangers remained in operation. This maintenance activity typically lasted at least three days. During some of the cleaning operations – for example, when the tubes were removed from the heat exchanger to facilitate the cleaning – contractors and specialized equipment were needed in the unit. In the past, this operation involved as many as fourteen personnel in the NHT unit at one time while the other heat exchanger bank and the remainder of the process continued to operate around them.

5.2.3 Tesoro Failure to Control Heat Exchanger Startup Hazards

On April 1, 2010, Tesoro operations staff began implementing the procedure to startup the clean A/B/C heat exchanger bank. The startup procedure only described roles for the two NHT operators normally assigned to a shift, one in the control room and one outside in the field. However, additional outside operators from other units frequently assisted in the heat exchanger startup. In addition to responding to potential leaks, supplemental personnel were sometimes requested to assist in the NHT heat exchanger startup operations because of the difficult labor-intensive process involved. When starting up a bank of

[121] Minimize the number of people in harm's way should an incident occur. *See* Center for Chemical Process Safety (CCPS). *Guidelines for Risk Based Process Safety*. 2007; p 296.

NHT heat exchangers, the operator was required to open several large block valves to introduce the process fluid to the heat exchanger bank that was shut down. The block valves were located on three different levels of the NHT structure, as illustrated in Figure 30. The geared mechanisms that opened and closed these valves were of a type referred to as “long-winded” because they were physically demanding, requiring over a hundred turns (by hand) of large wheels to fully open the valves. In addition, the heat exchanger procedures required deliberate and coordinated manipulation of these valves. As a result, startup by only the one official NHT outside operator was complex and difficult, and additional personnel often assisted with the heat exchanger bank startups.

Figure 30. Unit structure (left) and manual block valve (right)

Tesoro routinely relied on additional staff members during NHT heat exchanger startups but never assessed the risks or made any attempts to control them. Tesoro did not conduct an MOC to consider the risks of these organizational changes, despite its policy that required the performance of such a risk assessment.[122]

---

[122] The performance of a MOC review to examine the safety implications of organizational change is not required by either the federal OSHA PSM standard or the Washington PSM regulation. Although it is noted that Tesoro MOC procedures went beyond regulatory requirements, its failure to apply its own policy to circumstances that should trigger a MOOC review underscores the need for a PSM regulatory revision to help ensure that needed MOOC safety reviews are not voluntary. In the 2007 BP Texas City investigation report, the CSB recommended to the federal OSHA that it revise the PSM standard to require MOC reviews for organizational changes, including staffing changes. In response, OSHA sent a memorandum in 2009 to its Regional Administrators, stating the new agency position that changes to operating procedures that include organizational changes are subject to MOC requirements, even though they are not explicitly applicable. In August 2013, the CSB Board voted that the OSHA response was “open-unacceptable.” In December 2013, OSHA published a Request for Information (RFI) as a step in the rule-making process to revise the chemical accident prevention regulations, including the PSM standard. The RFI seeks public input on whether to revise the PSM standard to explicitly

The Tesoro MOC policy includes a requirement for Management of Organizational Change (MOOC), which recognizes that "… changes in an organization can … sometimes result[] in unrecognized negative effects." For examples, an MOOC is needed in the case of staffing modifications, changes in maintenance practices, and shifting of personnel roles and responsibilities – all typical practices used at the refinery to provide additional operators from other units to assist in startup of the NHT heat exchangers. The MOOC policy includes provisions for providing "[c]lear documentation and communication of why the change is necessary" and "[a] clear understanding of the risks involved and application of effective measures to reduce, eliminate, or mitigate those risks." The Tesoro MOOC policy covers "non-routine tasks" and includes requirements for the following:

> Document all identified risks; include methods to reduce, eliminate or mitigate them […]
>
> Review the risks involved with the changes. Ensure discussions include human factors, competence, workload issues, and sufficient resources to ensure the change can be carried out safely.

In post-incident interviews, Tesoro employees described the number of employees in the unit at the time of the explosion (seven workers) as unusually high. Yet, the CSB learned that it was not unusual for a shift supervisor to enlist one to four additional staff members from other units to perform the hazardous nonroutine work associated with the NHT heat exchanger startups. Although some employees might have perceived this as positive (e.g., reflection on individual willingness to help), the practice actually exposes a poor company process safety culture. Tesoro required operators who did not have defined roles in the procedure to assist with the startup, a hazardous activity with a long history of incidents.

An effective PSM system would have corrected the problems with known leaks and fires and would have controlled all aspects of hazardous nonroutine work. This approach would include taking proactive measures to eliminate worker exposure hazards and limiting access to only the minimum personnel needed to perform the tasks.[123] The use of more personnel than the number called for in the procedure exposed more workers to the high-hazard activity. This higher level of risk to workers should have been identified in NHT unit procedural reviews, PHAs, or an organizational MOOC.

---

require MOC reviews for organizational changes, citing the BP Texas City CSB recommendations. See: (https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=FEDERAL_REGISTER&p_id=24053) (accessed January 3, 2014). While the CSB welcomes this positive step, it is important to note that more timely proactive federal PSM revisions requiring MOOC reviews would also require similar PSM revisions in Washington's State Plan OSHA program. If implemented, the revised regulations would have required a safety review of staffing changes for the NHT exchanger startup and could have had a preventive impact.

[123] Minimize the number of people in harm's way should an incident occur. Center for Chemical Process Safety (CCPS), *Guidelines for Risk Based Process Safety*; 2007; p.296.

For example, in such a review, Tesoro could have recommended automating the NHT heat exchanger startup or redesigning the heat exchangers to a single bank so that online switching was not possible. Automation could have limited the role of the single outside NHT operator and minimized exposure to hazards. With automation, the task for the outside operator could have been reduced to simply opening the primary isolation block valves for the A/B/C heat exchangers. If the heat exchanger leaks had been corrected, there would no longer be a need for multiple operators to be actively prepared to mitigate a leak or fire during the startup, and the single necessary operator could leave the immediate area. The remainder of the startup could have been performed by the automatic system and controlled remotely by the NHT operator in the control room. Such approaches could have eliminated the need to station personnel in the immediate vicinity of the heat exchangers. Since the incident, Tesoro has redesigned the NHT heat exchangers to create a single heat exchanger bank. Now, online switching is not possible, and automated startup can be used to minimize hazards to personnel. If Tesoro had taken such an approach before the incident, the consequences of the April 2010 incident could have been significantly reduced.

Post-incident, Tesoro replaced the NHT heat exchangers with a single exchanger bank.

With the new design, online switching is not possible, and automated startup can be used to minimize hazards to personnel.

5.3 Process Hazard Analyses Failed to Prevent or Reduce the Consequences

CSB process modeling estimates suggest that HTHA occurred at the Tesoro Anacortes Refinery at temperatures and hydrogen partial pressures below the carbon steel Nelson curve. However, the CSB has found that both Shell Oil and Tesoro had many opportunities to prevent the damage caused to the B and E heat exchangers by HTHA long before the April 2010 catastrophic failure. Such opportunities included the following:

- DMHRs to predict potential HTHA damage
- Verification of operating conditions
- PHAs to identify hazards, evaluate safeguards, and assess considerations for inherently safer design.

The PSM-required PHAs[124] conducted on the NHT heat exchangers failed to prevent the April 2010 incident or to reduce the consequences by limiting personnel access to potentially dangerous areas during the hazardous startup activity. The Shell Oil and Tesoro PHAs conducted on the Anacortes refinery NHT unit failed to accomplish the following:

- Effectively evaluate and control hazardous nonroutine operations
- Effectively evaluate and control the frequent leaks during startup
- Restrict or limit the number of personnel present during the hazardous nonroutine startup of the NHT heat exchangers
- Identify effective safeguards to control hazards from damage mechanisms such as HTHA.

5.3.1 Hazardous Nonroutine Operations

None of the Anacortes refinery PHAs effectively evaluated and controlled hazards associated with the nonroutine work necessary to periodically clean the NHT heat exchangers. The Washington PSM regulations address the need for nonroutine operations to be evaluated and require that at least one member of the PHA team has expertise in nonroutine tasks.[125] The CCPS describes the importance of PHA evaluations, as well as the hazardous potential and frequent problems of PHAs that lack sufficient analysis of nonroutine work as follows:[126]

[124] A PHA is a hazard evaluation to identify, evaluate, and control the hazards of a process. Facilities that process a threshold quantity of hazardous materials, such as the Tesoro Anacortes Refinery, are required to conduct a PHA per the WAC, Title 296, Chapter 67, Safety standards for process safety management of highly hazardous chemicals (1992). See: http://apps.leg.wa.gov/wac/default.aspx?cite=296-67 (accessed September 29, 2013). PHAs are also required by the federal EPA Risk Management Program.

[125] *See* WAC 296-67-291 Appendix C--Compliance guidelines and recommendations for process safety management (nonmandatory) http://www.lni.wa.gov/WISHA/Rules/hazardouschemicals/default.htm#WAC296-67-021 (accessed December 3, 2013).

[126] Center for Chemical Process Safety (CCPS). *Revalidating Process Hazard Analyses*. 2001; pp 31-32.

> It is not uncommon for initial PHAs of continuous processes to focus only on normal operations, failing to address nonroutine, critical operating modes such as startup, shutdown, preparation for maintenance, emergency operations, emergency shutdown, and other activities whose characteristics may differ considerably from normal operations.
>
> Experience indicates that many accidents do not occur during "normal" operation but, rather, during such nonroutine modes of operation. Consequently, it is important that a PHA evaluate the hazards of a process during nonroutine as well as normal (routine) operating modes.

The 1996 Shell Oil PHA for the NHT unit did not evaluate or identify any issues related to nonroutine hazardous work associated with the frequent NHT heat exchanger cleaning operations. The 2006 Tesoro NHT unit PHA revalidation identified startup as a nonroutine operation but noted that existing procedures were adequately addressing nonroutine work.

5.3.2 Access Was Not Controlled During Hazardous NHT Heat Exchanger Startup

The 1996 Shell Oil NHT unit PHA did not identify or analyze leaks from the NHT heat exchangers, and no recommendations were made to prevent these leaks. The 2001[127] and 2006 Tesoro NHT unit PHA revalidations also did not mention the frequent leaks from the NHT heat exchangers.[128] The 2010 Tesoro NHT unit PHA team reviewed the March 2009 NHT heat exchanger startup incident where a steady stream of flammable hydrocarbons leaked from the exchangers near workers. In its evaluation of this incident, the PHA team reviewed unspecified "administrative controls" and determined that they were "in place and effective." However, the CSB identified no administrative controls in place to minimize the number of workers present or their exposure to these startup hazards. In April 2010, less than two months after the PHA team determined that the "administrative controls" were in place and effective, seven workers were asked to be present during the hazardous nonroutine startup of the NHT heat exchangers. According to the Tesoro procedure, a single field operator should have conducted this startup work.

[127] The 2001 PHA revalidation conducted by Tesoro did not raise issues related to the NHT heat exchangers. The only mention of these exchangers is in the process description.

[128] The 2008 TOP investigation of fires in the Anacortes refinery NHT unit concluded that complacency about exchanger leaks was a contributing factor in allowing the problem to persist.

5.3.3 Failure to Effectively Identify and Evaluate HTHA Hazards

During the 38 years that the NHT heat exchangers were in operation, the Anacortes Refinery had many opportunities to prevent the April 2010 incident by identifying and effectively controlling the potential for HTHA in the B and E heat exchangers. Both Shell Oil and Tesoro performed DMHRs, commonly known as corrosion reviews, of the Anacortes refinery's process equipment to determine the susceptibility to damage mechanisms such as HTHA.[129] The first documented corrosion study for the NHT unit occurred in 1990, with subsequent studies in 1999, 2003, and 2008.[130]

A problem common to all of the DHMRs conducted over the 20 years before the April 2010 incident is an inaccurate understanding the extent of stainless steel cladding covering the inside surface of the of the B and E heat exchanger shell wall. Each damage mechanism review documents that the B and E heat exchangers had a protective 316 stainless steel cladding covering the carbon steel wall. However as shown in Section 4.2.1, the 316 stainless steel cladding was installed only on the hottest section (Can 4) of the heat exchanger. The other three sections of the B and E heat exchanger shell walls were carbon steel without any protective cladding.

The 1999 and 2003 DMHRs document both recognition of the need for proper materials of construction and a good understanding of the need to determine accurate equipment operating conditions:

> The prevention of HTHA begins with proper materials selection for the anticipated process conditions, i.e., hydrogen partial pressure and temperature. Careful review of these process variables must be made not only for normal operation but also for any other routine or non-routine mode of operation to determine the controlling set of conditions for the materials selection.
>
> Off-normal conditions must be considered in addition to normal operating conditions.

Despite this recognition that the full range of operating conditions should be determined, none of the DMHRs requested that a technical evaluation, such as process simulation, be conducted for estimation or required that instrumentation be installed to measure the full range of operating conditions of the B and E heat exchangers. There were no temperature instruments installed on the B and E heat exchangers, and the hydrogen partial pressure is a parameter that must be calculated. Because these values were not

[129] Corrosion reviews consist of a process-by-process review of the plant for the susceptibility of API RP 571 damage mechanisms. A process flow diagram is marked up with process variables (temperature, flow, pressure, etc.) and evaluated based on current operating data and past equipment repair history.

[130] The 1990 review occurred while Shell Oil still owned the refinery, and was conducted by Shell Oil employees and the Shell Westhollow Corporation of Texas. Following the purchase of the refinery in 1998, Tesoro contracted with Shell Westhollow for preparation of the 1999 and 2003 study. The 2008 study was conducted by Lloyd's Register Capstone.

rigorously evaluated, the Tesoro and Shell damage mechanism hazard reviews relied on design data that did not reflect all operating conditions.

DMHRs were conducted in 1990, 1999, 2003, and 2008. Highlights of the analyses related to HTHA and the NHT heat exchangers are summarized in Figure 31.

DMHR	Author	Significant HTHA Information and CSB Findings
January 1990[131]	Shell Oil Company	• **DMHR:** HTHA inspection of carbon steel is never required for operation more than 25 °F below carbon steel Nelson curve. • **DMHR:** Inspection is required every 2 to 3 years if operation is less than 25 °F below carbon steel Nelson curve. • **CSB:** No specific recommendations are made for B and E heat exchangers. • **CSB:** Entire shells of B and E heat exchangers are listed as fully clad in Type 316 stainless steel, a material resistant to HTHA. However, only the hottest section (Can 4) of the heat exchanger is clad in Type 316 stainless steel. [132]
March 1999 Reviewed again in September 2003	Shell Oil Company	• **DMHR:** HTHA occurs before it is detectable. • **DMHR:** HTHA control requires knowing and accommodating actual operating conditions. • **DMHR:** In many older units operation of the reactors and heat exchangers up to the HTHA limits is economically attractive. • **DMHR:** Operating close to the Nelson curves requires very close control and monitoring of operating parameters, coupled with frequent inspection for HTHA. • **CSB:** The B and E heat exchanger shells are considered members of the same HTHA operating condition – based risk group as the A/D heat exchangers. However, no specific guidance is offered for the B and E heat exchangers. • **CSB:** Entire shells of B and E heat exchangers are listed as fully clad in Type 316 stainless steel, a material resistant to HTHA. However, only the hottest section (Can 4) of the heat exchanger is clad in Type 316 stainless steel.
October 2008	Lloyd's Register Capstone	• **DMHR:** HTHA not a concern since operating conditions are below the Nelson curve. • **CSB:** Tesoro process engineering provides B and E heat exchanger shell-side temperatures. The values are lower than design, implying less risk of HTHA: Capstone data: 500 °F → (B and E shell-side) → 350 °F Design: 504 °F → (B and E shell-side) → 405 °F Capstone data: hydrogen partial pressure → 240 psia Design: hydrogen partial pressure → 291 psia

Figure 31. DMHR and CSB Findings on Anacortes HTHA and Heat Exchangers (1990–2008)

[131] Recommendations reviewed in December 1993

[132] API RP 941. *Steels for Hydrogen Service at Elevated Temperatures and Pressures in Petroleum Refineries and Petrochemical Plants.* Figure 1, Note 2, August 2008. Section 5.5 of API RP 941 states that it is not advisable to take credit for the presence of a stainless steel cladding. However, the CSB learned that some experts were less concerned about HTHA in the B and E exchangers when information provided to them indicates a Type 316 stainless steel cladding is present.

None of these DMHRs conducted in the 20 years before the incident identified the potential danger of HTHA in the B and E heat exchangers because they primarily relied on design data instead of measured process conditions.[133] Although all of these design data indicated operation below the Nelson curve, CSB modeling estimated that the hottest portions (Can 4) of the heat exchangers at times operated above the Nelson curve. As a result, the B and E heat exchangers were never inspected for HTHA and more HTHA-resistant materials were never considered until after the April 2010 incident. It is vitally important to fully understand actual operating conditions of refinery processes to ensure that all damage mechanism hazards are adequately analyzed.

5.3.3.1 Insufficient Process Instrumentation

An important factor in determining HTHA susceptibility is operating temperature. The Anacortes refinery HTHA inspection procedure "required" instrumentation to ensure and periodically document that the operation was appropriately monitored. However, for the instrumentation to be "required" a determination first had to be made that the process equipment was operating within 25°F or 25 psia[134] of the appropriate Nelson curve. The procedure did not clarify how to make such a determination (which would necessitate accurate measurement capability) without already having an accurate measurement. The procedure stated the following:

> Accurate measurements/determinations of temperature and hydrogen partial pressure should be made routinely and the records maintained to provide assurance that operating conditions remain compatible with Nelson Curve limits.
> Such measurements/determinations/records are required for equipment/piping that operate[s] within 25°F or 25 psia of the appropriate Nelson Curve.[135]

No temperature instrumentation was on the B or E heat exchangers. Figure 32 shows where temperature and pressure measurement instruments were located on the heat exchanger banks. Intermediate temperature and pressure instrumentation was nonexistent. This hazard evaluation barrier adversely affected all DMHRs at the Anacortes refinery. The operating temperature was unknown at the B and E heat exchangers, specifically as it increased significantly from heat exchanger fouling. With these key data absent from the analysis, the technicians, engineers, and damage mechanism experts relied on design operating conditions.

[133] The 2008 Capstone review used a partial pressure of 240 psia based on a modeling effort associated with an engineering project. Also, as previously noted in Section 4.4, a single external surface temperature measurement of 455 ºF was taken in October 1998 on the inlet to either the B or E heat exchanger.

[134] Absolute pressure measured in units of pounds force per square inch, or pounds per square inch absolute (psia).

[135] Although dated January 30, 2006 this procedure appears to have been developed by Shell Oil. The accuracy of the data used to develop the Nelson curve is described as being +/- 20 ºF. The procedure also describes the benefit of stainless steel cladding on the inside surface of equipment to prevent HTHA damage.

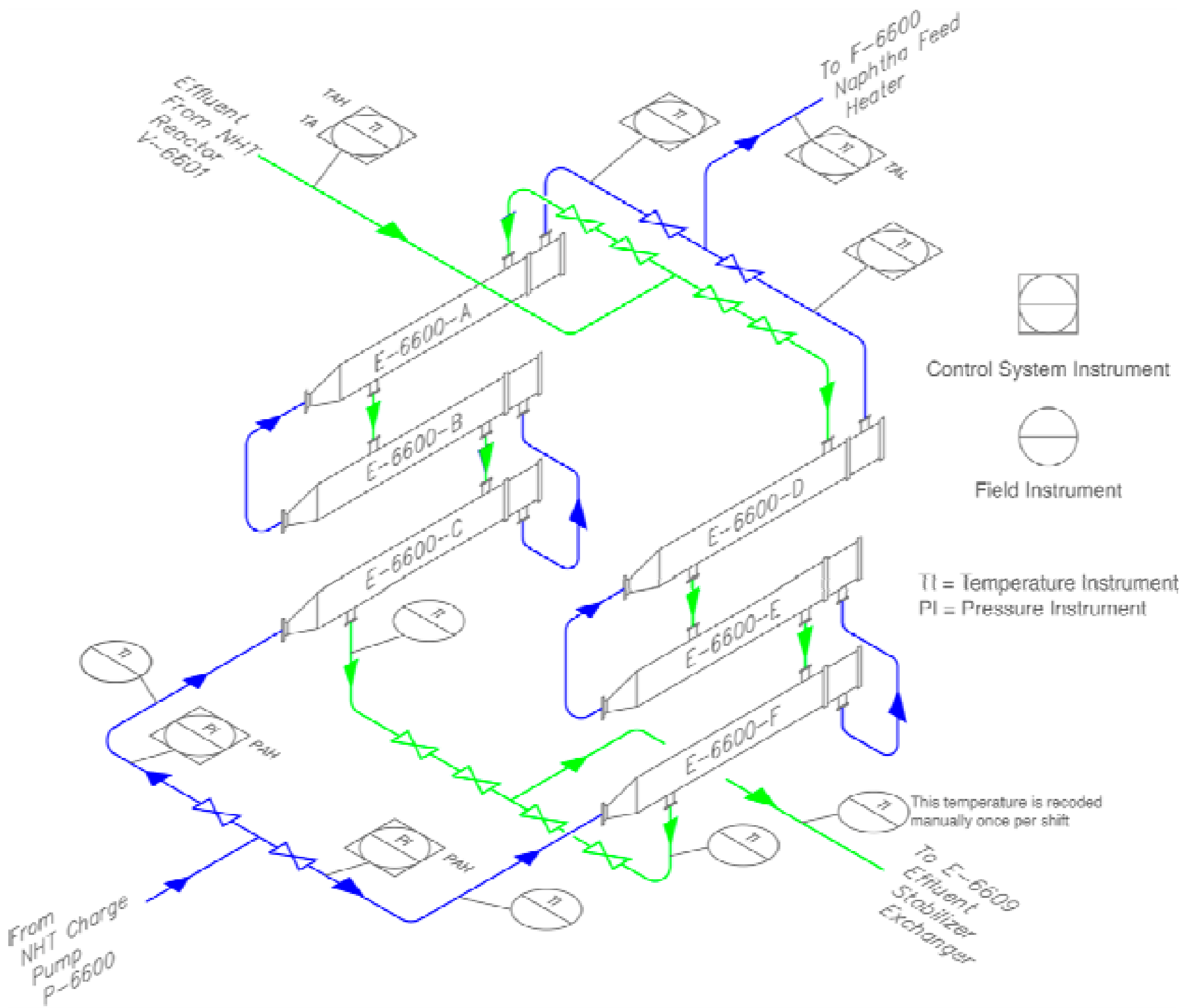


Figure 32. Temperature and Pressure Instruments on the NHT Heat Exchanger Banks. This isometric process flow view shows the lack of temperature indication on both shell-side and tube-side of the E and B heat exchanger inlets and outlets.

5.3.4 HTHA Hazards Were Not Effectively Controlled

In 1995,[136] Shell Oil completed a project PHA related to process modifications that could increase the hydrogen partial pressure in the NHT heat exchangers; however, no consideration, evaluation, or recommendation was made to account for the impact of this change on the potential for heat exchanger damage from HTHA.

The initial NHT unit PHA completed by Shell Oil in 1996 identified the potential for HTHA in the NHT heat exchangers. The PHA cited ineffective, non-specific, judgment-based qualitative safeguards such as the facility's inspection program, unit monitoring, procedures, practices, and limits on key and critical

[136] When this project was implemented, a Management of Change (MOC) review was also conducted. The MOC did not consider or evaluate the potential impact of increased hydrogen partial pressure on equipment susceptibility to HTHA.

variables for temperature (based on the Nelson curve) as safeguards. However, the B and E heat exchangers were never inspected for HTHA, no instrumentation was in place to monitor the inlet temperature of the B or E heat exchangers for Nelson curve limits, and no procedures or practices were in place to provide effective protection from HTHA. The effectiveness of these safeguards was neither evaluated nor documented; instead, the PHA merely listed general safeguards. If the adequacy of these safeguards had been analyzed, improved safeguards to protect against HTHA-related failure of the B and E heat exchangers could have been recommended.

The 2001[137] and 2006 Tesoro PHA revalidations do not address or modify the analysis from the 1996 Shell Oil PHA. In the 2001 PHA Tesoro included a review of the corrosion control program and a specific mechanical integrity checklist associated with the corrosion program. In 2006, the Tesoro corrosion program was still using these documents. However, in the 2006 PHA, Tesoro discontinued a review of these mechanical integrity programs in part because they were “not a legal requirement.” The following CCPS guidance on mechanical integrity does not recommend a focus on minimum compliance with regulation and notes:

> …[A] compliance-only program may miss out on many of the benefits of a more holistic approach, such as reduced risks for employees, the neighboring community, and the facility.[138]
>
> … the more holistic approach helps to ensure compliance with governing regulations and, ultimately, often turns out to be less expensive than the minimum compliance effort would have been.[139]

5.3.4.1 PHA Assumptions That Contributed to Ineffective Control of HTHA Hazards

For the sixteen year period starting in 1996 and ending in 2012, Shell Oil and Tesoro conducted PHAs at the Anacortes refinery that used a set of assumptions for the hazard scenarios and risk assessments generated by the PHA team. The purpose of these assumptions was documented as helping the team to assess “the worst credible scenarios not the worst imaginable scenarios.” However, based on the CSB investigation of the April 2010 incident, the use of these assumptions contributed to PHAs that were not effective in controlling process hazards.

The CSB determined that several of the Tesoro process unit PHA assumptions, shown in boxes in the rest of this section, could lead to ineffective evaluation of significant hazards and proposed safeguards associated with the immediate causes of the April 2010 incident.

[137] The 2001 PHA revalidation conducted by Tesoro did not raise any issues related to the NHT heat exchangers. The only mention of these exchangers is in the process description.

[138] Center for Chemical Process Safety (CCPS). *Guidelines for Mechanical Integrity Systems*. 2006; pp 3-5

[139] *Ibid* at 5.

Tesoro's PHA assumptions included:

Corrosion Inspection Program

Assumption: The System has a corrosion inspection program. Leaks or loss of containment due to corrosion of pipes and vessels is not credible for pipes and vessels included in these programs.

This assumption likely adversely influenced the evaluation of damage mechanism hazards and contributed to these hazards being ineffectively evaluated during the PHA. Equipment damage is a significant causal factor for loss of containment, and loss of containment is a primary process hazard. The immediate cause of the April 2010 incident was a damage mechanism – HTHA – that the Shell Oil PHA team in 1996 did not effectively evaluate. The 1996 PHA team significantly underestimated the risk of NHT heat exchanger failure. The frequency was appropriately estimated as being less than three percent, which was considered a "Low" frequency in the Shell Oil methodology. However, the consequence of the scenario was determined to be "Low to Medium" and significantly less than the actual consequence of the April 2010 incident. A "Low to Medium" consequence, according to the Shell Oil guidance documents, would include the following:

- A hydrocarbon release of a few hundred to 2,000 pounds;
- Moderate property damage in the $500,000 to $2 million range;
- Some recordable injuries[140] to workers; or
- Moderate disruption to refinery operations, with a return to operation within a few weeks.

As previously noted, to control HTHA hazards the 1996 Shell Oil NHT unit PHA team cited non-specific, judgment-based qualitative safeguards, such as the facility's inspection program, unit monitoring, procedures, practices, and limits on key and critical variables for temperature (based on the Nelson curve) as safeguards. None of these safeguards were effective, and they did not prevent the catastrophic E heat exchanger failure as a result of HTHA damage.

The 1996 Shell Oil NHT unit PHA was revalidated by Tesoro in 2001 and 2006, but these PHA teams did not address or modify the analysis from the 1996 Shell Oil NHT unit PHA.

The Tesoro 2007 PSM and RMP compliance audit indicated that previous PHAs at the Tesoro Anacortes Refinery lacked sufficient detail and did not identify all of the hazards of the process.[141] As a result, in

[140] OSHA provides the following as examples of recordable injuries, "Cut, puncture, laceration, abrasion, fracture, bruise, contusion, chipped tooth, amputation, insect bite, electrocution, or a thermal, chemical, electrical, or radiation burn. Sprain and strain injuries to muscles, joints, and connective tissues are classified as injuries when they result from a slip, trip, fall or other similar accidents." *See* https://www.osha.gov/recordkeeping/new-osha300form1-1-04.pdf (accessed January 2, 2014).

[141] The compliance audit was conducted pursuant to the requirements in 40 CFR 68.79 and to the OSHA PSM Standard, 29 CFR 1910.119, paragraph (o) triennial compliance audit requirement. As an example of the lack of detail in the 2006 Tesoro NHT unit PHA, the 2007 audit compared the NHT unit PHA to the Alkylation unit

2010 Tesoro conducted a new PHA that was a complete line-by-line evaluation. The 2010 NHT unit PHA evaluated hazards associated with the NHT heat exchangers in February 2010, just 38 days before the April 2010 incident. With the "assumptions" still being used and, notably, the corrosion control and mechanical integrity programs no longer being reviewed as part of the PHA program, the 2010 Tesoro NHT unit PHA team did not identify the potential hazard of B or E heat exchanger shell failure because of HTHA damage.[142]

Inspection and Maintenance Program

Assumption: The equipment is inspected per the plant preventive maintenance standards, and maintenance is performed promptly.

Using this assumption contributed to PHA teams not effectively evaluating proposed inspection-related or maintenance-related safeguards. The 1996 Shell Oil NHT unit PHA stated that the inspection program was a safeguard to prevent HTHA failure of the NHT heat exchangers. However, the B and E heat exchangers were never inspected for potential HTHA damage.

Materials of Construction

Assumption: The materials of construction of piping, gaskets, vessels, and valves have been correctly selected according to Shell design standards.

Using this assumption contributed to the PHA teams not considering any hazards caused by materials of construction, such as HTHA damage of carbon steel equipment, or recommending inherently safer materials such as 300 series stainless steel to mitigate hazards such as HTHA.[143]

PHA. The 2007 audit found that although the Alkylation unit had approximately half the complexity of the NHT unit, the Alkylation unit PHA conducted four times more hazard evaluation scenarios and made nearly 15 times more recommendations than the 2006 Tesoro NHT unit PHA.

[142] The term "shell" in this context refers to the pressure containing carbon steel wall of the heat exchanger. The 2010 Tesoro NHT unit PHA did identify HTHA as a possible hazard for the tube side of the B and E exchangers. Heat exchangers of this design have process flow through two sides, separated by mechanical design. Heat is transferred from one side to the other in order to exchange heat. Flow on the inside of the tubes through the heat exchanger is commonly referred to as "tube-side", while flow on the outside of the tubes is called "shell-side". The B and E exchangers had HTHA damage to the pressure containing portion on the shell-side. The 2010 Tesoro NHT unit PHA did not identify HTHA as a hazard where HTHA occurred on the shell-side of the exchanger.

[143] As previously discussed, API RP 571 identifies inherently safer materials to prevent HTHA noting, "300 Series SS, as well as 5Cr, 9Cr and 12Cr alloys, are not susceptible to HTHA at conditions normally seen in refinery units." *See* API RP 571. *Damage Mechanisms Affecting Fixed Equipment in the Refining Industry.* 2003; p "5-83".

5.4 CSB Conclusions on Organizational Deficiencies

For years, management at the refinery under both Shell Oil and Tesoro failed to effectively evaluate the potential for HTHA in the B and E heat exchangers. External corrosion experts repeatedly and erroneously assumed that heat exchanger design conditions were representative of actual process operating conditions despite knowing that these heat exchangers experienced severe heat transfer performance deterioration and required frequent cleaning.

Tesoro management also allowed worker exposure to hazards from fires and significant hydrocarbon leaks during startup of the NHT heat exchangers to become an accepted "normal" practice. Relying on steam suppression to mitigate leaks during NHT heat exchanger startups was a common and acceptable practice and was part of the startup procedure. Tesoro made attempts to correct the heat exchanger design problem that caused the leaks that sometimes resulted in fires, but ultimately these were ineffective. Additional employees were frequently brought in to assist the NHT field operator with the labor-intensive heat exchanger startup and hydrocarbon leak mitigation. On the night of the incident seven workers were performing the role that procedurally was intended for a single outside operator.

Well-known industrial safety and accident analysis experts James Reason and Andrew Hopkins indicate that safety culture is defined by collective practices, arguing that this is a useful definition because it suggests a practical way to create cultural change. More succinctly, safety culture can be defined as "the way we do things around here."[144,145]

Employees respond to issues that capture the attention of leaders.[146] Hopkins notes that leadership qualities that minimize, downplay, or deny risk will erode a process safety culture. A culture of risk denial can include the following characteristics:

- Belief that it cannot happen here
- Normalization of deviance (normalization of hazardous conditions)
- Ad hoc criteria for danger
- Downgrading intermittent warnings
- Burden (onus) of proof – requiring proof of danger rather than proof of safety
- Group think (eliminates minority voices in deference to consensus)[147]

Several of these characteristics were identified during the CSB investigation of the Tesoro Anacortes April 2010 incident, including normalization of hazardous conditions and a misplaced burden of proof of

[144] Hopkins, Andrew, 2005. *Safety, Culture and Risk; The Organisational Causes of Disasters*. Sydney, New South Wales: CCH Australia Limited. P 7.

[145] Center for Chemical Process Safety (CCPS), *Guidelines for Risk Based Process Safety*. 2007; p 40.

[146] Hopkins, Andrew. *Safety, Culture and Risk.* 2005; p 8.

[147] *Ibid* at 20-22.

safety.[148] It is an important distinction that a company culture, including its process safety culture, is the embodiment of its practices and not the sum of its beliefs. Consequently, a process safety culture can be objectively measured by examining the process safety practices and outcomes. The practices of the Tesoro Anacortes Refinery – use of excessive number of personnel to participate in hazardous activities, lack of verification of actual process conditions, normalization of hazardous leaks of the NHT heat exchangers, and PHA assumptions that contributed to ineffective hazard evaluation of major hazards – are all indications of a deficient process safety culture at the Tesoro Anacortes refinery.

[148] Burden of proof means to require proof of danger rather than proof of safety. It is applicable to the process safety culture at the Anacortes refinery and is shown through the repeated use of design data to evaluate the NHT exchangers for HTHA susceptibility. Rather than obtain data on actual operating conditions, Shell Oil and Tesoro corrosion experts were allowed to repeatedly rely on design operating conditions. Such design operating conditions were readily available, but there was no instrumentation to obtain actual operating conditions for the B or E exchangers. Refinery management did not require that these experts obtain data on and use the actual operating conditions to prove safety when reaching their conclusion that the B and E exchangers were not susceptible to HTHA damage.

6.0 Industry Codes and Standards

6.1 API RP 941 Operating Limits and Material Selection for HTHA

API RP 941 is the industry guidance document that describes how to predict and manage HTHA. API RP 941 was initially published in 1970 to communicate broadly industry's experience with HTHA – both HTHA occurrences and conditions where HTHA did not occur.

6.1.1 No Minimum Requirements to Prevent HTHA

As discussed in Section 4.1.1, industry uses the Nelson curves as lines of demarcation to predict HTHA. Above each curve, HTHA is possible for that material of construction, and below the curve, the prediction is that HTHA will not occur. Industry also uses these curves to select materials of construction based on the anticipated operating conditions and to create an HTHA inspection and prevention program. However, API RP 941 is written permissively, and there are no minimum requirements for refiners to take any action to prevent HTHA failures.[149] Specifically, there are no user requirements as follows:

- There are no minimum requirements for users to perform HTHA susceptibility evaluations;
- There are no requirements for users to select inherently safer materials of construction; and
- There are no minimum requirements for users to verify process operating conditions of equipment that is potentially susceptible to HTHA.

6.1.2 History of the Nelson Curves

The Nelson curves are based on industry experience with HTHA and were first developed in 1949 by George Nelson,[150] who gathered the original data to create the Nelson curves. After his death, none of his original data were found; only the information contained on the actual Nelson curves was available to API and the rest of industry.[151] On the basis of the Nelson curves, in 1970 the API published API RP 941 *Steels for Hydrogen Service at Elevated Temperatures and Pressures in Petroleum Refineries and Petrochemical Plants*.[152]

API RP 941 contains a submittal sheet for companies to report their experience with HTHA.[153] It tasks the company reporting HTHA equipment damage to provide a limited and simplistic history of operating conditions. API requests only the average and maximum process and metal temperature and a single

[149] API RP 941 uses the term "should" 27 times and the word "shall" once. As used in a standard, "shall" denotes a minimum requirement to conform to the standard, while "should" denotes a recommendation which is advised but not required to conform to the standard.

[150] G. A. Nelson, "Operating Limits and Incubation Times for Steels in Hydrogen Service," Proceedings, 1965, Volume 45, American Petroleum Institute, Washington, D.C. pp. 190-195.

[151] API TR 941. *The Technical Basis Document for API RP 941*. 2008; p 128.

[152] *Ibid* at 127.

[153] HTHA experience includes both reports of HTHA damage and equipment that was not damaged by HTHA.

value for hydrogen partial pressure to represent equipment operating conditions. API provides very limited instructions on completing the datasheet to report HTHA equipment damage. There is no assurance that the data are representative of actual operating conditions. The datasheet reported to API does not ensure that the data cover the life of the equipment versus the year, month, or even week before equipment failure. The use of a single hydrogen partial pressure value does not ensure that the variability of the process is appropriately represented by the data reported.

As demonstrated in the CSB analysis of the B and E heat exchanger operating conditions in Section 4.4.1, refinery equipment often operates at a range of temperatures and hydrogen partial pressures. The API RP 941 technical report acknowledges this, stating that the authors "find it difficult to obtain accurate operating data and material damage assessments."[154] In addition, not all companies report their HTHA failures to API (for example, Tesoro did not formally report the failure information to API following the April 2010 incident). Furthermore, the consequences of HTHA equipment damage, such as a multi-fatality incident, are not included as part of the data submitted to API. These are significant weaknesses in relying on empirical, self-reported data.

6.1.3 Industry Critiques of Nelson Curves

The applicability and accuracy of the Nelson curves have been called into question within the refining industry. Two comprehensive reports analyze the Nelson curves: the Hydrogen Attack Project and API TR 941, *The Technical Basis Document for API RP 941*.

The Hydrogen Attack Project is a report by the Materials Property Council[155] and the API.[156] The report presents a history of HTHA analysis, the Nelson curves, and API RP 941. The report highlights problems in obtaining accurate data on operating conditions, analogous to the problems that the CSB identified at Tesoro, stating:

> The only really reliable way to get an equipment exposure temperature is to properly measure the actual temperature of the component. Many times the process thermocouples are not well located for measuring the temperature of a particular component or in the case of exchangers, a particular exchanger in a multi-exchanger train. The design and/or process flow diagrams may not provide a very good estimate of actual operating temperatures.[157]

[154] API TR 941. *The Technical Basis Document for API RP 941*. 2008; pp 45-46.

[155] The Materials Properties Council (est. 1966) was founded by the American Society of Mechanical Engineers, ASM International, ASTM and the Engineering Foundation and supported by industry, technical organizations, codes and standards developers, and government agencies in order to provide valid data on the engineering properties of metals. See: http://www.forengineers.org/mpc/index.html (accessed November 21, 2013).

[156] Hydrogen Attack Project, Materials Property Council / American Petroleum Institute, undated.

[157] In this context, the term "train" is synonymous with "bank" and is used to describe multiple heat exchangers in series. Hydrogen Attack Project, Materials Property Council / American Petroleum Institute, p 19, undated.

API TR 941 was issued as the technical basis document for API RP 941.[158] This technical report addresses several possible limitations of the Nelson curves, such as the location and shape of the curves.[159] API TR 941 acknowledges that there is still more to learn about HTHA, stating "We are still far from being able to make quantitative predictions about the behavior of steels subject to HTHA."[160]

Important variables that affect HTHA but are not reflected in the Nelson curves include:

- **Stress**
- **Carbide stability**
- **Grain size**
- **Type of weld**
- **Time in operation**

Critics of the Nelson curves also contend that, although the Nelson curves are easy to apply, their simplicity minimizes their effectiveness.[161] Critics of the curves say that HTHA is a complex phenomenon. The risk of HTHA is a function of more than solely the three variables described by the Nelson curves (material of construction, temperature, and hydrogen partial pressure).[162] Other variables that are not addressed by the curves affect the potential for HTHA, such as stress,[163] carbide stability,[164,165] grain size,[166] type of weld,[167] and time in operation.[168]

[158] API Technical Report 941. *The Technical Basis Document for API RP 941.* 2008.

[159] *Ibid* at 2.

[160] *Ibid* at 45.

[161] Van der Burg, M.W.D., Van der Giessen, E., and Tvergaard, V. "A continuum damage analysis of hydrogen attack in a 2.25Cr-1Mo pressure vessel," Materials Science and Engineering A241 (1998) 1-13, p1.

[162] *Ibid* at 12.

[163] API RP 941. *Steels for Hydrogen Service at Elevated Temperatures and Pressures in Petroleum Refineries and Petrochemical Plants.* 2008; Section 3.2.

[164] A carbide is an intermetallic compound containing carbon. There are many possible combinations of carbon and other atoms (such as iron, titanium, niobium, vanadium) that combine to form carbides in steel. Each of these carbides has an effect on the properties of the steel.

[165] Van der Burg, M.W.D, Van der Giessen, E., and Tvergaard, V. "A continuum damage analysis of hydrogen attack in a 2.25Cr-1Mo pressure vessel," Materials Science and Engineering A241 (1998) 1-13, p12.

[166] Grain size is a fundamental characteristic of steel microstructure, indicating the size of each individual crystalline packet of iron atoms (known as a "grain").

[167] Manna, G., P. Castello, and F. Harskamp. "Testing of welded 2.25CrMo steel, in hot, high-pressure hydrogen under creep conditions" Engineering Fracture Mechanics 74 (2007) 956-968, p.956.

[168] Shewmon, Paul. *Hydrogen Attack of Carbon Steel.* Metallurgical Transactions A Vol 7A February 1976, p 280.

API TR 941 warns that applying API RP 941 has become less conservative as equipment is pushed to the limits of the Nelson curves for economic reasons.[169] API TR 941 notes the following:

> The concept of a simple boundary between safe and unsafe operating conditions in hydrogen for common alloys, of the type depicted by the Nelson curves should not be expected. Certainly material composition, heat treatment and stress are well accepted as variables that influence behavior.
>
> Experience shows damage accumulation is time dependent. However, the methods of detection and quantification of damage are so inadequate, operating conditions so poorly recorded, failure analyses so cursory and materials characterization so primitive, that life prediction is on shaky grounds today.[170]

6.1.4 Unreliable Carbon Steel Nelson Curve

As discussed in Section 4.4.1, CSB process modeling of the Tesoro NHT heat exchangers estimates that HTHA occurred below the carbon steel Nelson curve.

As previously discussed, post-incident analysis of the NHT heat exchangers determined that damage from HTHA was occurring in portions of the B and E heat exchangers that were estimated to have operated below the carbon steel Nelson curve. The coldest region in the E heat exchanger with identified HTHA was estimated to operate up to 120 °F below the carbon steel Nelson curve. This finding indicates that the industry developed carbon steel Nelson curve is inaccurate and cannot be relied on to prevent HTHA equipment failures or to predict HTHA equipment damage.

> **The carbon steel Nelson curve is inaccurate and cannot be relied on to prevent equipment failures due to HTHA.**

[169] API Technical Report 941. *The Technical Basis Document for API RP 941* . 2008; p 45.

[170] API Technical Report 941. *The Technical Basis Document for API RP 941*. 2008; p 47.

6.1.4.1 ExxonMobil HTHA Incident Below the Carbon Steel Nelson Curve

ExxonMobil also experienced equipment damage from HTHA at process conditions that were noted as being immediately below the carbon steel Nelson curve.[171] Similar to Tesoro, the ExxonMobil incident included damage to a heat exchanger of a hydrotreating unit.[172] This failure has many similarities to the Tesoro April 2010 incident and further highlights that the carbon steel Nelson curves cannot be relied upon to prevent HTHA equipment failures.[173] Similar to the Tesoro April 2010 incident, cracking was observed in non-PWHT carbon steel constructed in the early 1970's and operating at conditions reported as being below the Nelson curve.[174] The ExxonMobil HTHA failure also occurred adjacent to weld seams in the heat affected zone of the vessel.[175]

6.1.4.2 Other Industry Reports of HTHA Damage to Equipment that Operated Below the Carbon Steel Nelson Curve

The CSB has learned of at least eight recent refinery incidents where HTHA reportedly occurred below the carbon steel Nelson curve. In addition to the ExxonMobil incident, Valero, Shell, and ConocoPhillips have all reported incidents to the API 941 committee where the companies have concluded that equipment operating below the carbon steel Nelson curve was damaged by HTHA. Valero reported three incidents at their Corpus Christi refinery and one incident at their Texas City refinery. Shell reported at least two equipment components in one process unit had HTHA below the carbon steel Nelson curve. In addition, ConocoPhillips reported an incident of HTHA below the carbon steel Nelson curve at one facility. In 2011, API issued an industry alert on HTHA in refinery service.[176] The API alert noted multiple incidents of carbon steel equipment at operating conditions where carbon steel was previously thought to be resistant to HTHA. These refinery incidents and the subsequent API response strongly suggest an industry-wide problem with the carbon steel Nelson curve.

6.1.5 Essential Adjustments Are Needed to API RP 941

Although the potential consequences of HTHA-related failure can be catastrophic, API RP 941 currently imposes no substantive requirements on users. API RP 941 should require companies to verify the actual operating conditions of equipment that is potentially susceptible to HTHA. In addition, API RP 941 should incorporate the principles of the hierarchy of controls and inherently safer design to prevent equipment failures from HTHA. The CSB has identified at least eight incidents in refineries where HTHA equipment damage was found at operating conditions below the carbon steel Nelson Curve.

---

171 McLaughlin, J., Krynicki, J., and Bruno, T. *Cracking of non-PWHT'd Carbon Steel Operating at Conditions Immediately Below the Nelson Curve.* ExxonMobil Research and Engineering Company, Proceedings of the ASME 2010 Pressure Vessels & Piping Division, 2010; pp 18-22.

172 *Ibid.*

173 *Ibid.*

174 *Ibid.*

175 *Ibid.*

176 *See*: http://www.api.org/publications-standards-and-statistics/hidden-pages/industry-alert (accessed January 19, 2014).

Furthermore, CSB modeling of the Tesoro Anacortes refinery NHT heat exchangers suggests the E heat exchanger failed from HTHA damage that occurred below the Nelson curve. In support of inherent safety to prevent equipment failures from HTHA, the CSB proposes a new boundary for the carbon steel Nelson curve in Figure 33. This boundary would prohibit carbon steel equipment at process conditions that API has identified as susceptible to HTHA, above 400 ^{0}F.[177]

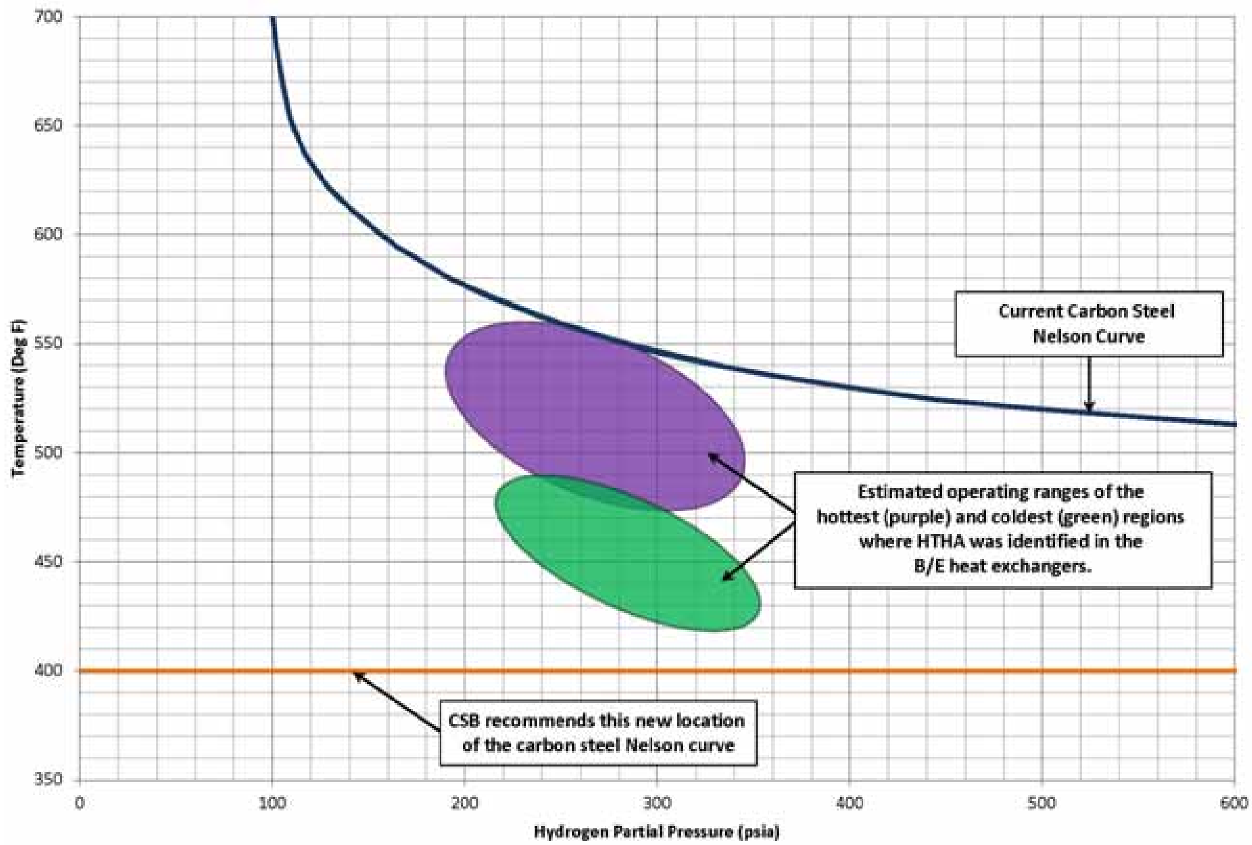


Figure 33. CSB Modeling Results of HTHA and the Nelson Curve at the Tesoro Anacortes Refinery. CSB modeling estimates suggest that HTHA occurred in the B and E heat exchangers below the carbon steel Nelson curve. The CSB recommends that the carbon steel Nelson curve be relocated as shown to prevent HTHA in carbon steel.

177 API Technical Report 941. *The Technical Basis Document for API RP 941*. 2008; p 6.

6.1.6 ANSI Z10, Exemplifies Standards Clarity

As previously stated, API RP 941 is written permissively with no minimum requirements to prevent HTHA failures. In contrast, the American National Standards Institute[178] (ANSI) Occupational Health and Safety Management Systems standard, ANSI/AIHA Z10-2012 (Z10), provides an improved example of how to clearly define obligations in a standard document.[179] Z10 makes use of both “should” and “shall” language as well as explicit document formatting to differentiate mandatory requirements from voluntary recommendations. The following specification addresses the format, which is illustrated in Figure 34.

> This [Z10] standard is formatted into two columns to help distinguish requirements from recommended practices and explanatory information. Requirements are in the left column and are identified by the word ‘shall.’ An organization that chooses to conform to this standard is expected to fulfill these requirements. The text in the right hand column uses the word ‘should’ to describe recommended practices, or explanatory notes to the requirements on the left. This use of the terms ‘shall’ and ‘should’ to identify requirements and distinguish them from recommendations and explanatory notes is common practice in ANSI and international standards.[180]

[178] ANSI is a group comprised of government agencies, organizations, companies, academic and international bodies, and individuals that oversees the development and use of industry guidelines and standards. For more information *see* http://www.ansi.org/about_ansi/overview/overview.aspx?menuid=1 (accessed January 27, 2014).

[179] Z10 was developed by over 50 organizations and included representation workers (USW), regulators (OSHA), and industry (API). Section 5.1.2 requires the use of the hierarchy of controls to achieve risk reduction for identified hazards. ANSI/AIHA Z10-2012. *Occupational Health and Safety Management Systems*. 2012; p x, xi, 15.

[180] ANSI/AIHA Z10-2012. *American National Standard - Occupational Health and Safety Management Systems*. June 27, 2012; p.ix.

5.1.3.2 Process Verification
The organization shall have processes in place to verify that changes in facilities, documentation, personnel and operations are evaluated and managed to ensure safety and health risks arising from these changes are controlled.

E5.1.3.2: These types of processes are sometimes referred to as Management of Change.

The Management of Change process should take into consideration relevant items such as:

- technology, equipment, work practices and procedures
- design specifications and raw materials
- organizational or staffing changes standards or regulations

Management of Change includes changes being made in existing operations, products, or services.

Source: ANSI/AIHA Z10-2012, p.17

Figure 34. Example of ANSI Z10 Obligations Formatting

6.2 API RP 580 Risk Based Inspection / API 581 Risk Based Inspection Technology

API intends for risk-based inspection (RBI) to be a process that enables optimization of inspection efforts by balancing the time between inspections against the risks of equipment failure caused by the known damage mechanisms.[181]

API RP 581, *Risk-Based Inspection Technology* is used in conjunction with API RP 580, *Risk-Based Inspection.* API RP 580 is the API standard for developing an RBI program. API RP 581 is the API standard for implementing an RBI program.

Unlike API RP 941, API RP 581 predicts the susceptibility of HTHA risk versus equipment service time. This time-based increase in risk is based on a mathematical model, associating risk with the type of steel. The API RP 581 model represents an early attempt to address the shortcomings of the empirical Nelson curves. However, API RP 581 lacks specific direction to ensure that users employ appropriate actual operating conditions. As a result, the CSB found that using the Tesoro design operating conditions and 38 years of operation yields a result that the B and E heat exchangers have a "Low Susceptibility" to HTHA.[182]

[181] Risk Based Inspection (RBI) Best Practice: *The Technical Specification for Ensuring Successful Implementation*. by Ron Selva B.Sc., C.Eng., F. I. Mech. E; 13th International Conference on Pressure Vessel & Piping Technology, 20-23 May 2012, London, Keynote Paper – Technical Session: Managing Risk

[182] API 581 defines three levels of HTHA susceptibility; Low, Medium, and High. Using the E exchanger design operating conditions of a hydrogen partial pressure of 291 psi and a temperature of 504 ºF along with 38 years of continuous service (333,108 hours) into equation 2.51 from API RP 581 results in a HTHA susceptibility parameter of 4.53. The minimum value for "Low" HTHA susceptibility is greater than or equal to 4.53.

Like API RP 941, API RP 581 is written permissively, so there are no minimum requirements to prevent HTHA failures. There are 19 uses of "shall" in RP 581, but none are substantive—nearly all the uses of "shall" appear in formulas or requirements for damage factor or in inspection effectiveness calculations that are themselves non-mandatory. There are three uses of "shall" in the HTHA section, but again these are employed for calculations that are permissive—such as "the following procedure may be used" or if HTHA is detected, "fitness for service should be performed." An instructive example of the permissiveness of API RP 581 is that the document provides important guidance for conditions that would make equipment susceptible to HTHA damage. However, if the equipment is identified as meeting the criteria that would indicate HTHA is a credible damage mechanism, the guidance provided by API RP 581 is that the equipment "should" be evaluated for HTHA susceptibility.

7.0 Regulatory Oversight of Petroleum Refineries in Washington

As addressed in the recently released CSB draft Chevron Regulatory Report, many regions around the world such as the United Kingdom (UK) and Australia have implemented regulatory regimes for high hazards consisting of both prescriptive[183] and goal-setting elements[184] that place the duty on the owner or operator of the facility, known as the duty holder,[185] to demonstrate to the regulator that they have reduced risks to as low as reasonably practicable, or ALARP. This approach is known as the safety case regime. The CSB determined that there are key features of an effective major accident prevention regulatory approach such as the safety case (illustrated in Figure 35):

- Duty Holder Safety Responsibility, including a Written Case for Safety
- Continuous Risk Reduction to ALARP
- Adaptability and Continuous Improvement
- Active Workforce Participation
- Process Safety Indicators that Drive Performance
- Regulatory Assessment, Verification, and Intervention; and
- Independent, Competent, Well-Funded Regulator.

The findings, analysis, and conclusions of the draft CSB Chevron Regulatory Report are applicable to the CSB Tesoro investigation and are incorporated into this report by reference. The draft Chevron Regulatory Report can be accessed in Appendix F.

The United States has persisted in the use of a more activity-based[186] regulatory approach that does not adequately engage companies and their employees in continuous improvement and risk reduction. The CSB has found that the existing regulatory regime for onshore petroleum refineries in Washington:

- relies on a framework that is primarily activity-based without a risk reduction target;
- does not effectively involve the workforce in hazard analysis and prevention of major accidents; and
- does not employ a sufficient number of staff members with the technical expertise needed to provide sufficient oversight of petroleum refineries.

---

[183] A prescriptive regulation or standard describes the specific means or activity-based actions to be taken for hazard abatement and compliance.

[184] Performance or goal-based regulations state the objective to be obtained (such as risk reduction or hazard abatement) without describing the specific means of obtaining that objective.

[185] Duty holders are considered to be "those who create and/or have the greatest control of the risks associated with a particular activity. Those who create the risks at the workplace are responsible for controlling them." UK Health and Safety Executive, *Planning to do business in the UK offshore oil and gas industry? What you should know about health and safety;* October 2011; p 2. http://www.hse.gov.uk/offshore/guidance/entrants.pdf (accessed June 5, 2013).

[186] Activity-based standards and regulations require the mere completion of an activity and do not focus on the effectiveness of major accident prevention or risk reduction.

Figure 35. Key Safety Case Attributes

7.1 Background

The occurrence of a number of large accidents, including a massive explosion and fire at the Phillips 66 Company's Houston Chemical Complex in Pasadena, Texas, resulting in 23 fatalities, and the 1984 toxic release in Bhopal, India, which caused several thousand known fatalities, resulted not only in the creation of the CSB but also in the first federal regulations specifically designed to prevent major chemical accidents that threaten workers, the public, and the environment. One of these regulations is the OSHA PSM standard, which was adopted in 1992. This standard applies to a process[187] involving a chemical at or above the listed threshold quantity (also known as a highly hazardous chemical), or flammables in a quantity of 10,000 pounds or more.[188] It contains broad requirements to implement management systems,

[187] The PSM standard defines "process" as "any activity involving a highly hazardous chemical including any use, storage, manufacturing, handling, or the on-site movement of such chemicals, or combination of these activities." 29 CFR §1910.119(b) (1992).

[188] 29 CFR §1910.119(a)(1) (1992). This standard also applies to the manufacture of explosives and pyrotechnics in any quantity [29 CFR §1910.109(k)(2) & (3)].

identify and control hazards, and prevent "catastrophic releases of highly hazardous chemicals." [189] Many processes in a petroleum refinery are subject to the PSM standard.

> **The frequent occurrence of refinery accidents demonstrates the pressing need to examine the current regulatory structure.**

As discussed in the draft Chevron Regulatory Report, the CSB has concluded that the frequent occurrence of refinery accidents demonstrates the pressing need to examine the current regulatory structure in place in the US. Despite the fact that the nation's roughly 150 petroleum refineries represent only a small fraction of the thousands of industrial and chemical facilities in the US, the CSB has noted a considerable number of significant and deadly incidents at refineries over the last decade. In 2012 alone, the CSB tracked 125 significant incidents at US petroleum refineries.[190] Three of these incidents took place in the state of Washington.

7.2 L&I Division of Occupational Safety and Health (DOSH)

Section 18 of the Occupational Safety and Health Act of 1970 (OSHAct) encourages states to develop and operate their own job safety and health programs, referred to informally as an OSHA State Plan. OSHA approves and monitors State Plans and provides as much as 50 percent of an approved plan's operating costs. These programs must be "at least as effective in providing safety and healthful employment" as the federal PSM standard.[191] DOSH administers an approved state occupational Safety and Health Plan in accordance with the OSHAct and enforces Washington's PSM standard under the Washington Administrative Code (WAC).[192] Although most State Plan states are funded through a state general fund, DOSH is funded mostly by an insurance group and by federal OSHA. Unlike the California Division of Occupational Safety and Health (Cal/OSHA), DOSH does not have a dedicated PSM unit; rather, it currently employs four PSM specialists, including one chemical engineer, to regulate nearly 270 PSM-covered facilities in the state, including five petroleum refineries. One of those specialists has previous refinery experience; the other three have experience with ammonia facilities and chemical manufacturing.

[189] Preamble to Process Safety Management of Highly Hazardous Chemicals; Explosives and Blasting Agents. Section 1 – I. Background (March 4, 1992). *See* http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=PREAMBLES&p_id=1039 (accessed May 10, 2013).

[190] These incidents were reported to the Department of Energy and/or the National Response Center and examined by the CSB's Incident Screening Department.

[191] 29 U.S.C. §667(c)(2) (1970). https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_id=2743&p_table=OSHACT (accessed September 24, 2013).

[192] The Washington PSM standard is established under Title 296, Section 67 of the Washington Administrative Code (WAC).

7.2.1 Causal Findings Comparing PSM and the Safety Case Regulatory Approach

The findings in this report identify a number of weaknesses with Tesoro process safety performance. In many of these causal issues, the existing Washington PSM regulations did not require Tesoro to perform at a more effective level to control hazards and prevent incidents. In Figure 36 below, the CSB identifies the causal issues which highlight the gaps within the Washington and federal PSM regulations, and how each issue is more effectively managed in the safety case regulatory regime. In this section of the report, some of these examples will be examined in relation to key features of an effective regulatory approach such as the safety case.

Process Safety Concept	Causal Finding	Washington and Federal PSM Regulation and Enforcement	Safety Case Regulatory Regime
MOC	Tesoro added steam stations in the vicinity of the heat exchanger structure. This equipment enhanced the ability of the field operator(s) to confront hazardous leaks and extinguish fires in the area of the NHT heat exchangers, and the safety implications of these activities were not considered. The MOC developed by Tesoro did not evaluate or control hazards associated with the heat exchanger leaks, emergency egress, or with how the steam equipment would be used. Although affected, heat exchanger startup procedures were not reviewed or modified to account for the change.	The MOC element requires implementation of written procedures to manage changes that shall address the impact of the change on health and safety; however the element is activity based rather than performance based and there is no requirement to control hazards. There is no WAC PSM requirement to actually control hazards through the MOC process. Current regulations allowed Tesoro's narrow focus in looking at the change as a minor modification to a utility system rather than taking a broader view of how the change could impact the overall process.	The duty holder is required to drive risk to ALARP. Demonstration of MOC effectiveness in managing major accident hazard risk is a key requirement of the safety case. The mere existence of MOC written procedures is insufficient under the safety case regulatory regime.

Process Safety Concept	Causal Finding	Washington and Federal PSM Regulation and Enforcement	Safety Case Regulatory Regime
PHA	PHAs in 1996, 2001, and 2006 cited ineffective, non-specific, judgment-based, qualitative safeguards to prevent equipment failure from HTHA. However, the effectiveness of these safeguards was neither evaluated nor documented; instead the PHA merely listed them.	Although the PHA element requires addressing the control of hazards, it does not require addressing the effectiveness of the controls or using the hierarchy of controls. For example, the standard would not require the use of improved materials of construction or inherently safer design to mitigate corrosion hazards.	The safety case regime requires use of the most effective practical safeguards to achieve ALARP. The safety case requires the use of inherently safer design and the hierarchy of controls.[193]
PHA	The 2010 Tesoro NHT unit PHA failed to identify HTHA as a hazard for the shell of the B and E heat exchangers.	DMHRs are not required by the PSM regulation. The PHA element does not require consideration of RAGAGEPs such as API RP 571, *Damage Mechanisms Affecting Fixed Equipment in the Refining Industry*. Washington L&I did not cite Tesoro for this issue.	In the UK, the Health and Safety Executive (HSE) has worked with industry to develop guidance on DMHRs in the UK offshore petrochemical industry. The implementation of best practice standards referenced by a duty holder's safety case report may be enforced by the regulator to achieve ALARP.

[193] According to the HSE, essential considerations for determining whether a duty holder has reduced risks to ALARP include "the adoption of inherently safer designs…". HSE. *The Safety Report Assessment Manual, Sections 8 to 15*. p 30. http://www.hse.gov.uk/comah/sram/s8-15.pdf (accessed October 30, 2013). The HSE also notes that the guidance to Control of Major Accidents Hazards (COMAH) Regulation 4 (General Duty) "describes the application of all measures necessary to reduce risk of a major accident to ALARP based on a hierarchical approach (inherent safety, prevention, control, mitigation)." *Ibid* at 8.

Process Safety Concept	Causal Finding	Washington and Federal PSM Regulation and Enforcement	Safety Case Regulatory Regime
PHA	PHAs identified HTHA as a hazard for the B and E heat exchangers, but ineffective safeguards failed to control the hazard. L&I did not effectively review the PHAs before the incident.	WAC does not require submission of the PHA to L&I to be reviewed for sufficiency and acceptance. L&I does not have a sufficient number of technically qualified PSM personnel to perform effective reviews of PHAs.	Under the safety case regulatory regime, the PHA is part of the report submitted to the regulator for acceptance. The duty holder is required to drive risk to ALARP. Effective safety case regulatory regimes employ sufficient numbers of technically competent personnel to assess, verify, and intervene as necessary.
PHA	In the 2006 NHT unit PHA, Tesoro discontinued a review of their corrosion control and mechanical integrity programs in part because they were “not a legal requirement.” Tesoro conducted the optional review ineffectively and then ended it when they determined it was not strictly required.	There is no requirement in the PSM regulation for a performance based DMHR.	By shifting the responsibility for risk management to the duty holder, the safety case would require continual risk reduction and performance of an effective DMHR. This review is not just an activity but must meet the goal of preventing equipment failures.

Process Safety Concept	**Causal Finding**	**Washington and Federal PSM Regulation and Enforcement**	**Safety Case Regulatory Regime**
Incident Investigation	There was a history of leaks and fires on the NHT heat exchangers during startup, as identified in a Tesoro investigation report. Tesoro attempted to address the problems, but the hazard was never controlled.	Washington PSM regulations require incident investigation and preparation of a report, but do not require recommendations or control of hazards identified in the investigation. Although the regulations do not require recommendations to be developed, if recommendations are made the regulation requires them to be resolved.	Investigation of incidents is required to demonstrate legal compliance with framework legislation. The ALARP requirement would require remedial action including cross-company learning from incident investigations. The HSE can require safety case duty holder compliance with investigation report recommendations.
Nonroutine Work	Tesoro failed to perform an evaluation of the higher hazards of the nonroutine work of starting up a bank of heat exchangers. Tesoro also did not define or control the number of workers required to perform the startup.	Although the WAC PSM regulation contains guidance on ways to control hazards when performing nonroutine work, compliance is not mandatory. The WAC regulations do not require either a hazard evaluation of nonroutine work or limitations on essential personnel during higher-hazard activities.	The safety case regulatory regime would require incorporation of good-practice guidance to achieve ALARP, such as the CCPS *Risk Based Process Safety* guidelines that address nonroutine work.

Process Safety Concept	Causal Finding	Washington and Federal PSM Regulation and Enforcement	Safety Case Regulatory Regime
Mechanical Integrity	API RP 941 has no minimum requirements to control, identify, or prevent the occurrence of HTHA in process equipment.	The mechanical integrity element of PSM requires that employers follow RAGAGEPs for inspection and testing procedures. However, API RP 941 has no minimum requirements. Post-incident, L&I cited Tesoro for insufficient testing and inspection procedures for the heat exchangers but did not specifically reference API RP 941 or HTHA.	In a safety case regime, the regulator can reject the use of weak and inadequate standards referenced in a safety case report (by rejecting the report) and can require more rigorous performance to achieve ALARP.
Inherently Safer Design	The B and E heat exchangers were constructed of carbon steel – the most HTHA-susceptible material of construction used by industry. API RP 571 identifies materials that are not susceptible to HTHA.	Neither Washington nor federal OSHA requires the use or implementation of inherently safer design.	The safety case regulatory regime requires the implementation of inherently safer systems analysis.[194]

[194] According to the HSE, essential considerations for determining whether a duty holder has reduced risks to ALARP include "the adoption of inherently safer designs…". HSE. *The Safety Report Assessment Manual, Sections 8 to 15.* p 30. http://www.hse.gov.uk/comah/sram/s8-15.pdf (accessed October 30, 2013). The HSE also notes that the guidance to COMAH Regulation 4 (General Duty) "describes the application of all measures necessary to reduce risk of a major accident to ALARP based on a hierarchical approach (inherent safety, prevention, control, mitigation)." *Ibid* at 8.

Process Safety Concept	Causal Finding	Washington and Federal PSM Regulation and Enforcement	Safety Case Regulatory Regime
Process Safety Indicators	For more than a decade during startup following cleaning, the NHT heat exchangers would frequently leak from flanges, occasionally resulting in fires that created hazardous conditions for workers.	Federally and in the state of Washington, neither the PSM nor RMP regulations require companies to utilize or report process safety indicators.	Process safety indicators that drive performance are a key feature of the Safety Case regime. Publicly reported indicators can reveal critical safety areas that must be targeted for improvement to prevent accidents.

Figure 36. Gaps Within the Washington and Federal PSM Regulations. Causal findings highlight the gaps within the Washington and federal PSM regulations and how the process safety concept relating to each finding is more effectively managed in a safety case regulatory regime.

7.3 OSHA National Emphasis Program

7.3.1 Federal National Emphasis Program

In a 1992 compliance directive,[195] OSHA stated that the primary enforcement model for the PSM standard would be planned, comprehensive, and resource-intensive Program Quality Verification (PQV) inspections.[196] These inspections consisted of the following three parts:

1. determining whether the elements of a PSM program are in place
2. evaluating whether the programs comply with the requirements of the standard, and
3. verifying compliance with the standard through interviews, data sampling, and field observations.

The CSB noted in its BP Texas City Final Investigation Report that for the 10-year period before the Texas City incident, federal OSHA conducted no planned PQV inspections in petroleum refineries. As a result, the CSB recommended in its report that OSHA strengthen the planned enforcement of the OSHA PSM standard by developing more highly trained and experienced inspectors to conduct more comprehensive inspections similar to those under the OSHA PQV program, at facilities posing the greatest risk of a catastrophic accident.

[195] Compliance directives are the main method OSHA uses to communicate plans, inspection methods, and compliance expectations to their Compliance Safety and Health Officers (CSHOs) for enforcing a new regulation.
[196] OSHA Instruction CPL 02-02-045 (1994).

Spurred in part by recommendations in the CSB BP Texas City Final Investigation Report, OSHA adopted the Petroleum Refinery Process Safety Management NEP on June 7, 2007.[197] The NEP was a federal program that established guidelines for inspecting petroleum refineries to ensure compliance with the PSM standard. The NEP was designed to address the prevention and minimization of the consequences of catastrophic releases of toxic, reactive, flammable, or explosive chemicals in the refining industry.[198] In adopting the NEP, OSHA noted that no other industry sector in the country had experienced as many fatal or catastrophic incidents related to highly hazardous chemicals.[199]

Unlike the PQV approach to inspections, which "employs a broad, open-ended inspection strategy and uses a more global approach to identify compliance deficiencies…," the NEP "provide[d] CSHOs [Compliance Safety and Health Officers] with a tool to evaluate for compliance with the standard."[200] The tool is meant to identify "a particular set of requirements from the PSM standard from which CSHOs are to review documents, interview employees, and verify implementation for specific processes, equipment, and procedures."[201] According to CPL 03-00-004, the NEP inspections were required to be conducted by a team consisting of at least one Team Leader and one Level 1 Team Member.[202,203] Although the CSB called for an ongoing comprehensive inspection program, inspections being conducted pursuant to the NEP ended in 2011 in part because these inspections were very time consuming and resource intensive. OSHA has publicly stated[204] that NEP inspection hours were roughly 40 times greater than average OSHA inspection hours.

7.3.2 Washington State National Emphasis Program

OSHA State Plan states such as Washington were strongly encouraged but not required to adopt the NEP. However, on February 8, 2008, DOSH formally adopted the NEP through DOSH Directive 2.64[205] for the

[197] Originally Directive Number CPL 03-00-004, *Petroleum Refinery Process Safety Management National Emphasis Program*. Extended August 18, 2099 as Directive Number CPL 03-00-010 to allow more time to complete NEP inspections under the original CPL 03-00-004.

[198] https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_id=3589&p_table=DIRECTIVES, Accessed October 30, 2013.

[199] OSHA Directive number CPL 03-00-004, Section VIII, Background

[200] CPL 03-00-004, Section X(D)(1). 2007. https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_id=3589&p_table=DIRECTIVES (accessed September 24, 2013).

[201] *Ibid*

[202] CPL 03-00-004, Section X(C)(1). 2007. https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_id=3589&p_table=DIRECTIVES (accessed September 24, 2013).

[203] A Level 1 Team Member is considered to be Trained OSHA personnel with experience in the chemical processing or refining industries. CPL 03-00-004, Section X(C)(2).

[204] See Barab, Jordan. OSHA's Refinery & Chemical National Emphasis Programs. Power Point presentation made at CSB Public Hearing on Process Safety Indicators; July 20, 2012. http://www.csb.gov/UserFiles/file/Barab%20%28OSHA%29%20PowerPoint.pdf (accessed August 14, 2013). Also see Transcript of CSB Public Hearing on Safety Performance Indicators; p 52. http://www.csb.gov/assets/1/19/CSB_20Public_20Hearing.pdf (accessed August 14, 2013).

[205] DOSH Directive 2.64. Petroleum Refinery Process Safety Management. February 8, 2008. http://www.lni.wa.gov/Safety/Rules/Policies/PDFs/WRD264.pdf (accessed September 24, 2013).

five refineries[206] in the state of Washington. The stated purpose of DOSH Directive 2.64 was to "reduce or eliminate the workplace hazards associated with the catastrophic release of highly hazardous chemicals at petroleum refineries."[207] The directive required the DOSH staff to follow the compliance directions in OSHA Instruction CPL 03-00-004 when conducting NEP inspections. When CPL03-00-004 referenced another CPL, DOSH instead followed any existing equivalent DOSH policy and directives. DOSH also used WAC equivalents in place of the OSHA 1910.119 PSM standard. For example, when auditing PSM section 1910.119(j) "Mechanical Integrity," DOSH instead used WAC 296-67-037.

CPL 03-00-004 provides for a two-step NEP inspection process. The first step is a PSM compliance review based on a "static" list of inspection priority items. The second is a PSM compliance review based on a "dynamic" list of priority inspection items.[208]

The DOSH NEP team consisted of six people, including a team lead who had been with L&I since the early 1990s. The team lead had more process safety and refinery experience than the other team members. None of the team members had an engineering or metallurgy background, and the team as a whole had limited experience with PSM and with refinery operations.

[206] The five petroleum refineries in Washington are BP Cherry Point Refinery; Conoco Phillips Ferndale Refinery; Tesoro Anacortes Refinery; Shell Oil Products Refinery; and US Oil and Refining Refinery.

[207] DOSH Directive 2.64. Petroleum Refinery Process Safety Management. February 8, 2008; p 1. http://www.lni.wa.gov/Safety/Rules/Policies/PDFs/WRD264.pdf (accessed September 24, 2013).

[208] Static questions within the NEP are publicly available. The company can prepare for them. Dynamic questions are not available to the company prior to the audit. Reference: OSHA CPL 03-00-004 Section X (D)(3). (June 7, 2007). *See:* https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_id=3589&p_table=DIRECTIVES (accessed September 24, 2013).

7.3.3 Tesoro National Emphasis Program Audit

Following Washington's adoption of the federal NEP, the DOSH NEP team lead developed a proposed refinery inspection plan. To determine the focus for the NEP audit at each facility, the DOSH NEP team examined the age of each process in the refinery, hazards surrounding different process units, and past events, including near misses.

On October 7, 2008, the DOSH NEP team initiated a formal NEP audit of the Tesoro CR and NHT units. The selection of these units was based primarily on the fact that the NHT unit stood out to the team as problematic in terms of previous incidents and near misses. The Tesoro NEP Audit Report noted the following:

> Elsewhere, refinery records indicate a relatively higher incidence of process safety related events occurring in the Catalytic Reformer and Naphtha Hydrotreater (CR/NHT) process areas when compared to other units, with the possible exception of the Catalytic Cracking unit equipment when viewed in its entirety.
>
> From 2002 to 2007, the CR/NHT experienced a total of 117 records related to process safety. Of those, 36% were attributed to equipment failures, 33% human error, and the remaining 31% were attributed to failure of a process control or safeguard.
>
> Previous inspection activities at the refinery have included at least five safety and health compliance inspections since 2003. These have included scheduled inspections, complaints, and accident and near miss investigations.

The NEP team spent several weeks at the Tesoro refinery during the NEP audit. The refinery NEP inspection process was a two-step process. The first step consisted of a compliance review based on a static list of inspection priority items. The CSHO was required to follow the list verbatim. The list of questions related to various aspects of process safety, such as equipment, engineering and administrative controls, and safe work practices. The answers to these questions were the basis for determining compliance with various PSM requirements. The second step focused on a dynamic list of inspection priority items that were directed towards the specific selected process unit.[209]

7.3.3.1 Tesoro NEP Results Associated with the E Heat Exchanger

The Tesoro Anacortes NEP audit is noteworthy, as it was the only audit conducted under the federal OSHA NEP program that focused on a unit that subsequently experienced a catastrophic accident that the CSB investigated. The heat exchanger that failed, the E heat exchanger, was a fundamental component of the Tesoro NEP audit. Within the scope of the NEP nine pressure vessels were selected at random; the E

[209] OSHA Directive CPL 03-00-004, Section X, (D) (3).

heat exchanger was one of the vessels reviewed. The NEP states, "Inspection records for all nine vessels were examined and found to be in order. No citable deficiencies found."

Like the CSB, the DOSH NEP identified the issue of PHA assumptions for the PHA. Reflecting the weakness in the current PSM requirements for PHAs, DOSH mentioned the problematic nature of using the assumptions but did not cite Tesoro in this area. The NEP states the following:

> Problems were identified in the area of procedures, inspection, and testing of devices that indicate assumptions made by PHA teams inhibits identification of problematic areas.

Given the methodology used and expertise available, the mechanical integrity issues related to the failure of the E heat exchanger were not detected during the NEP audit. To prevent the April 2010 incident, the NEP audit needed to identify the susceptibility of the E heat exchanger to HTHA and to recognize that Tesoro had incorrectly concluded that it was not susceptible. The topics investigated during the NEP audit were contained in prescriptive questions for the individual unit, which resulted in a shallow technical review. For example, significant emphasis was placed on verifying the existence of basic protocols for conducting thickness monitoring. On the basis of the CSB review of the question sets applied for the Tesoro refinery, there was no mention of HTHA, corrosion studies, or failure mechanisms and no references to the API RP 571 damage mechanisms. The NEP team lead confirmed that little emphasis was placed on possible damage mechanisms that could be present, including HTHA. The NEP found the following:

> In general, the refinery maintains corrosion control documentation that attempts to identify corrosivity data and potential failure mechanisms.
>
> The inspection procedure I-08.01 addresses metallurgy and corrosion in the refinery.
>
> The refinery has a procedure for conducting corrosion awareness training of staff and managing corrosion control procedures.

Unless a member of the NEP audit team had a personal interest in metallurgical damage mechanisms, or had experience to prompt investigation into the area of metallurgy, reliance on these static and dynamic lists would not lead to the conclusion that the B and E heat exchangers were susceptible to HTHA.

The NEP inspection was formally closed on March 12, 2009; at that time, a summary of the audit findings was presented to Tesoro. The NEP inspection team identified 17 process safety code violations under Chapter 296-67 of the WAC,[210] but only two of these addressed mechanical integrity,[211] and neither related to the NHT heat exchangers or to identification or control of HTHA.

---

[210] *See* http://apps.leg.wa.gov/wac/default.aspx?cite=296-67 (accessed September 25, 2013).

[211] Mechanical integrity violations of WAC 296-67-037 were issued for the following:

a. No written procedures for controls and emergency shutdowns; 13 instances were documented in which the employer did not have written procedures for the inspection and testing of emergency equipment; and

On October 23, 2009, six months before the incident, a settlement agreement was reached between L&I and Tesoro whereby Tesoro agreed to perform a PSM compliance audit with an industry recognized PSM consultant within 60 days of the agreement date and to commit to a completed compliance audit within six months of the consultant's contract initiation date. In exchange for the audit, L&I agreed to reduce the citations from seventeen (17) to three (3) citations. Subsequently, the total penalty was reduced from $85,700 to $15,450.[212] The same consulting firm that Tesoro hired for its most recent OSHA-mandated compliance audit also conducted the audit under the settlement agreement. However, the compliance audit conducted by the consulting firm was not a comprehensive audit of the entire refinery PSM program. It was limited only to those areas covered by the fourteen eliminated citations from settlement agreement between L&I and Tesoro.

7.4 Risk Reduction and Continuous Improvement

The CSB Chevron Regulatory Report provides a detailed discussion of the advantages of implementing a safety case regulatory regime compared to the PSM standard in its current form. The safety case regulatory regime is an adaptable regulatory approach that is used by many countries throughout the world and provides the regulator with the tools needed to drive continuous improvement among facilities and to ensure that duty holders are identifying and controlling hazards and reducing risks to ALARP. The federal and state of Washington PSM standards, on the other hand, are more reactive in nature and contain activity-based requirements that do not focus on specific risk reduction; rather, the mere completion of the activities satisfies the requirements.

Highlighting the reactive nature of the Washington PSM standard, following the Tesoro incident, DOSH initially cited Tesoro for 39 willful violations and five serious violations related to the incident, with a total proposed fine of $2.39 million.[213] Four of the citations were issued to Tesoro for failing to follow recognized and generally accepted good engineering practice (RAGAGEP) for mechanical integrity under WAC 296-67-(4)(b) "such as those published by the American Petroleum Institute."[214] No RAGAGEPs were specified in the citations. RAGAGEPs are technologically focused, with no emphasis on organizational issues, human factors, or culture-based measures. OSHA developed the mechanical integrity RAGAGEP requirement to "make sure that process equipment is inspected and tested properly, and that the inspections and tests are performed in accordance with appropriate codes and standards."[215] However, as in this case, OSHA mainly enforces RAGAGEP reactively. Here, DOSH used unspecified

---

b. Documenting inspections and tests – 24 instances identified in which the employer did not document testing of emergency field devices or where the record did not identify what testing procedure was used.

212 *See* http://www.osha.gov/pls/imis/establishment.inspection_detail?id=312459290; (accessed on June 19, 2013).

213 Tesoro has appealed these citations.

214 State of Washington Department of Labor and Industries, Division of Occupational Safety and Health. *Tesoro Citation – Notice Inspection.* October 1, 2010; p 9. http://www.lni.wa.gov/Main/Docs/TesoroCitation-NoticeInspectionNo314251315.pdf (accessed September 25, 2013).

215 OSHA. Preamble to 29 CFR Part 1910, Process Safety Management of Highly Hazardous Chemicals, Section 3, Title III. Summary and Explanation of the Final Rule, 1992. Available at http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=PREAMBLES&p_id=1041 (accessed June 6, 2013).

RAGAGEPs to issue a citation to Tesoro post-incident, rather than working to drive continuous improvement and risk reduction through preventative NEP inspections. Although many OSHA inspectors have cited to RAGAGEPs following NEP refinery audits, DOSH did not cite any RAGAGEPs for mechanical integrity following its NEP audit of the Tesoro refinery in 2008.

Similar to OSHAct Section 5(a)(1), also known as the General Duty Clause, the WAC requires employers to provide employees a workplace "free from recognized hazards[216] that are causing, or are likely to cause, serious injury or death."[217] Similar to federal OSHA, DOSH may use this provision following an incident to cite a company for hazards not addressed by the regulations, but these citations are often difficult to prove especially if the regulator lacks industry-specific expertise, and are resource intensive to sustain. DOSH did not cite Tesoro for General Duty Clause violations following the April 2010 incident.

Washington's Safety Standards for Process Safety Management of Highly Hazardous Chemicals were established to "prevent[] or minimiz[e][] the consequences of catastrophic releases of toxic, reactive, flammable, or explosive chemicals."[218] Washington's PSM standard contains many activity-based elements that are almost identical to those in the federal PSM standard. For example, an employer must perform a PHA "appropriate to the complexity of the process and shall identify, evaluate, and control the hazards involved in the process."[219] This language does not support the principle of ALARP and makes no mention of reduction of risk or continuous improvement. As a result, PHAs may satisfy Washington's PSM requirement by merely listing safeguards, and there is no requirement to evaluate or document the effectiveness of those safeguards, or to show that the safeguards reduce risks.

Following the April 2010 incident DOSH issued two citations to Tesoro for its 2006 PHA revalidation.[220] One of these citations was dismissed and the second citation addressed Tesoro's failure to establish and implement written procedures to manage the change made by discontinuing the PHA revalidation system that included mechanical integrity and corrosion control review in 2006.[221] However, as discussed in Section 5.3, PHAs conducted on the NHT unit cited non-specific, judgment-based qualitative safeguards that in light of the April 2010 incident were not effective. If the Washington PSM standard had required an evaluation and documentation of safeguard effectiveness, Shell Oil and Tesoro would have been obligated to conduct this analysis, and DOSH inspectors could have relied on the regulation for support during inspections.

---

[216] According to L&I, "A hazard is recognized if it is commonly known in the employer's industry, or if there is evidence that the employer knew or should have known of the existence of the hazard, or if it can be established that any reasonable person would have recognized the hazard." 296 WAC 800-11005 (2012).

[217] 296 WAC 800-11005 (2012). http://www.lni.wa.gov/wisha/rules/corerules/PDFs/296-800-110.pdf (accessed September 26, 2013).

[218] 26 WAC 67-001(1) (1992).

[219] 26 WAC 67-017(1) (1992).

[220] Under appeal, citation item 1-37 was dismissed.

[221] In the 2001 PHA, Tesoro included a review of the corrosion control program and a specific mechanical integrity checklist associated with the corrosion program. In 2006, Tesoro excluded these items because they were being used in the DMHR and it was "not a legal requirement" for PHAs.

Tesoro conducted a PHA for the NHT unit between February 1, 2010, and May 21, 2010. Despite the fact that the PHA was being conducted at the time of the April 2010 incident, the PHA failed to identify significant hazards associated with the immediate causes of the incident, including damage mechanisms such as HTHA. The PHA also took credit for inspection safeguards that did not exist. The PHA failed to address HTHA damage in the B or E heat exchangers on the shell-side and the PHA used inspection as a safeguard to mitigate HTHA consequences on the tube side. As discussed in Section 5.3.3, no inspection for HTHA was ever conducted on the B or E heat exchangers. No evaluation was documented to demonstrate the effectiveness of the inspection safeguards claimed by the PHA team; that is a manual activity and thus low in the hierarchy of controls. The PHA analysis concluded that the worst consequence resulting from a loss of primary containment (catastrophic failure of the E heat exchanger) was a disabling injury and substantially understated the actual consequence of seven worker fatalities. The combination of understating the consequence and overstating the safeguards resulted in underestimating the risk of a catastrophic failure of the E heat exchanger, despite the fact that the incident took place 50 days before completion of the PHA.

> **Tesoro's NHT unit PHAs cited non-specific, judgment-based, qualitative safeguards that were not effective in major accident prevention.**
>
> **A PHA may inadequately assess the risk of major hazards under the current regulatory system.**

In a safety case regulatory regime, a risk assessment such as this would be part of the safety case report submitted to the regulator to demonstrate and ensure that the hazards are adequately identified and that risks are being reduced to ALARP. If the hazards are not sufficiently identified and controlled, the regulator may reject the safety case document and require improvements and further risk reduction. In this case, because mere completion of the PHA satisfied the PSM requirements, DOSH did not analyze or address Tesoro's failure to adequately identify and control hazards. In addition, DOSH did not issue any post-incident citations to Tesoro regarding its 2010 NHT unit PHA.

The existing regulatory approaches in the US and Washington, such as the PSM and RMP programs, do not require companies to reduce risks to ALARP. While the Clean Air Act (CAA) directed the EPA to promulgate the RMP regulations "to provide, to the greatest extent practicable, for the prevention and detection of accidental releases of regulated substances,"[222] there is no RMP ALARP requirement. Under both the PSM and RMP regulations, an employer must "control" hazards when conducting a PHA of a covered process. However, there is no requirement to address the effectiveness of the controls or the

[222] 42 U.S.C. §7412(r)(7)(B)(i)

hierarchy of controls. Thus, a PHA that meets the regulatory requirements might still inadequately identify or mitigate major hazard risks. In addition, there is no requirement to submit PHAs to the regulator, and the regulator is not responsible for assessing the quality of the PHA or the proposed safeguards.

The Tesoro PHA goals encourage the PHA team to identify high-consequence, low-frequency hazards that are possible but might not be realized. The company's PHA goal supports the principle of ALARP. The Tesoro PHA policy states the following:

> In the end, the reduction of RISK is the goal.
>
> Any improvement in a layer of protection that is permanent and inseparable, and not easily weakened or removed from the system, is considered to be a process safety improvement in an inherently safer direction.
>
> Can the Likelihood be reduced?
>
> If the Hazard cannot be removed, and Consequences cannot be reduced, then what can be done to reduce the likelihood of the event(s) occurring?

None of the Tesoro PHA teams ever considered applying the principles of inherently safer design by upgrading the heat exchangers before the incident; yet, following the April 2, 2010, incident, more HTHA-resistant materials were used for the replacement equipment. In conducting its PHA of the NHT unit, which was required under the state of Washington PSM standard,[223] Tesoro did not address inherently safer design or implement effective safeguards to prevent HTHA. However, there is no Washington (or federal) PSM requirement to consider inherently safer design or to evaluate the effectiveness of safeguards. Thus, Tesoro was never cited for failure to evaluate or implement inherently safer design or for the PHA claim of HTHA inspection as a safeguard despite the company never inspecting the E heat exchanger for possible presence of HTHA.

Under a safety case regulatory regime, Tesoro would be required to apply the hierarchy of controls and inherently safer design to achieve ALARP. As detailed in the CSB Chevron Regulatory Report, the safety case report must demonstrate how inherently safer design concepts were applied in the design decisions that were taken. This principle applies to all life cycle stages of a facility, and includes materials selection and corrosion management in the design.[224]

[223] Under WAC 296-67-001 Process safety management of highly hazardous chemicals. See: http://www.lni.wa.gov/wisha/rules/hazardouschemicals/default.htm#WAC296-67-001 (accessed September 28, 2013).

[224] HSE. *Assessment Principles for Offshore Safety Cases (APOSC);* March 2006; p 7. http://www.hse.gov.uk/offshore/aposc190306.pdf (accessed August 6, 2013).

7.5 Workforce Participation

As the CSB noted in its Chevron Interim and draft Chevron Regulatory Reports, workforce participation is a key element of process safety and effective major accident prevention. The CCPS lists workforce involvement as one of 20 essential management components necessary to reduce process safety risks and prevent major chemical accidents.[225] In one of its publications, the CCPS states that workforce participation leads to worker empowerment, management responsiveness, and process safety performance improvement.[226] The OSHA PSM standard provides for participation by workers and their representatives. It requires employers to consult with employees and their representatives on the performance and development of PHAs and on the development of the 13 remaining PSM elements, and to develop a written plan of action regarding the implementation of the employee participation required under this section.[227] However, other regions such as the UK go further to ensure effective worker participation by specifying the election of safety representatives by the workers to serve many functions related to health and safety, including investigating complaints and accidents and conducting inspections.[228] UK regulations also require employers to establish a safety committee when one is requested by at least two health and safety representatives.[229]

Like the federal PSM standard, the WAC provides for workforce participation in a company's PSM program and has implemented language identical to that contained in the federal PSM standard.[230] However, throughout its investigation of the Tesoro incident, the CSB has seen that the Tesoro refinery workforce and its representative, the United Steelworkers Union (USW), expressed concerns regarding the NHT unit that were not adequately addressed by Tesoro managers in the lead-up to the incident. During a 2006 PHA revalidation on the NHT unit at the Tesoro Anacortes Refinery, workers noted 31 near misses in the NHT unit in the last 5 years because of many possible factors, including too many outside tasks and continual rotation of the field and control room operators. The PHA team requested a review of experience and training for NHT operators to address these workload concerns. A manager at the refinery closed the action item with one simple statement: "Experience levels of teams, where and when individuals are trained on the NHT are managed by team supervisor." The action item was closed without resolution of the concerns expressed by the Tesoro workers on the PHA team.

> **Concerns raised by NHT unit workers were not adequately addressed by Tesoro management.**

---

[225] CCPS. *Guidelines for Risk Based Process Safety;* March 2007; p liv.

[226] *Ibid* at 125.

[227] 29 CFR §1910.119(c) (2012).

[228] *See*: the Safety Representatives and Safety Committees Regulations, 1977, and the Health and Safety (Consultation with Employees) Regulations 1996.

[229] *Ibid.*

[230] See: WAC §296-67-009 (1992). http://apps.leg.wa.gov/wac/default.aspx?cite=296-67-009 (accessed September 26, 2013).

7.6 Funding and Regulator Competency

The CSB stated in both its BP Texas City Final Investigation Report (issued in March 2007) and its draft Chevron Regulatory Report (Appendix F) the importance of having a well-resourced, competent regulator consisting of individuals with the necessary training, education, and experience to conduct comprehensive and robust inspections of facilities with the goal of preventing catastrophic accidents. As noted above, currently DOSH employs only four Process Safety Specialists to cover approximately 270 PSM facilities within the state of Washington, and only one of those has significant refinery experience. None have metallurgical experience and only one has an engineering background. Despite the fact that DOSH performed a detailed NEP inspection at the Tesoro refinery, the team did not have the technical expertise to inspect for and identify possible damage mechanisms present in the NHT unit such as HTHA. Individuals within L&I have expressed to the CSB that there is currently no funding in the state of Washington to form a multi-disciplinary process safety group to conduct more thorough facility inspections. This was also the case in California at the time of the Chevron incident in August 2012. Despite the fact that Cal/OSHA had formed a dedicated PSM unit, it did not have the staffing, funding, or experience to oversee the state's 15 petroleum refineries. Following the Chevron incident, the California State Legislature approved a 2013-2014 state budget bill (AP 110) that allows the California Department of Industrial Relations to charge state petroleum refineries a "fee" by March 31, 2014, to help pay for at least 15 new positions in Cal/OSHA's Process Safety Unit, which enforces the California PSM standard throughout the state.[231]

The safety case regulatory regime will require a full commitment and extensive effort by the Washington legislature, regulators, and Washington petroleum refineries. The CSB believes that this effort is necessary to ensure that Washington, like other regions around the world, is effectively managing process safety and risk, and in the process, preventing major accidents such as the April 2, 2010, Tesoro incident.

7.7 Similar Deficiencies in the Anacortes and Richmond Refinery Incidents

The CSB identified a number of similar causal findings for both the April 2010 Tesoro Anacortes Refinery incident and the August 2012 Chevron Richmond Refinery incident. These findings included ineffective PHAs, lack of effective safeguards to prevent damage mechanism hazards, no requirements to use the hierarchy of controls or to implement inherently safer design to the greatest extent possible, weak and permissive industry standards that lack minimum requirements to control damage mechanism hazards, and regulators that lack sufficiently qualified personnel to provide effective oversight.

7.7.1 Reliance on Inspection Instead of Inherently Safer Design in Mechanical Integrity Programs at Tesoro and Chevron Refineries

The August 6, 2012, Richmond, California, Chevron refinery incident occurred when a severely thinned, low-silicon carbon steel pipe component ruptured, releasing hot hydrocarbons that autoignited and

[231] *See*: http://www.caltax.org/homepage/062113_Legislature_Approves.html (accessed July 9, 2013).

endangered the lives of 19 employees.[232] Like HTHA, low-silicon areas that result in rapid corrosion are very difficult to identify by inspection. Identification of this hazard requires the inspection of every single component in a carbon steel piping circuit to identify the quickly corroding pieces. Despite this difficulty and despite Chevron's notable expertise on sulfidation corrosion,[233] the refinery still operated the high-risk piping circuit with a carbon steel material of construction, the steel that is most susceptible to rapid rates of sulfidation corrosion in low-silicon components. The refinery then relied on its inspection program to identify any quickly corroding pieces, a very low-ranking method on the hierarchy of controls, to prevent process safety incidents. Ultimately, the inspection program failed to detect the low-silicon component in the piping circuit. Had Chevron designed the piping circuit by using an inherently safer material of construction, such as high-chromium steel, the corrosion rates in the piping circuit would have been much slower and much more uniform, and the incident would not have occurred.

The Anacortes refinery also in effect relied on its mechanical integrity program to identify damage mechanisms such as HTHA in its NHT heat exchangers instead of incorporating design elements that would eliminate the risk of HTHA. Although Tesoro was not actively looking for HTHA in the B and E heat exchangers, this is the only mechanical integrity component that could identify the damage in the heat exchangers. As described previously, inspection for HTHA is very difficult and not sufficiently reliable. The use of inherently safer materials of construction, such as high-chromium steels, significantly lowers the risk of HTHA in this type of service.

Both Tesoro and Chevron had the expertise and capability needed to design the damage mechanisms out of the equipment by incorporating inherently safer design. However, both companies continued to rely on mechanical integrity programs, such as inspection, to identify the damage after it had already occurred in the system. Although inspection programs are needed they are very low on the hierarchy of controls, and in both cases the inspection strategies failed to prevent a major process safety incident. Since the incidents, both Chevron and Tesoro redesigned the equipment that failed, incorporating inherently safer design practices. Now, sulfidation corrosion in Chevron's new piping circuit will be significantly reduced and without risk of variable corrosion rates. Tesoro installed new NHT heat exchangers, using materials of construction that are highly resistant to HTHA.

7.7.2 Ineffective PHAs at Tesoro and Chevron

PHAs are a crucial opportunity to identify hazards in a refinery process unit. However, neither Tesoro nor Chevron PHAs identified the significant hazards that led to the April 2010 and August 2012 incidents, respectively. The CSB found similar deficiencies in the PHA of both companies. Instead of performing a rigorous analysis of damage mechanisms present in the refinery during the PHA process, both companies simply cited non-specific, judgment-based qualitative safeguards to reduce the risk of damage mechanisms. The effectiveness of these safeguards was neither evaluated nor documented; instead, the

[232] The CSB is releasing three different reports on the Chevron incident. All reports can be found at http://www.csb.gov/chevron-refinery-fire/ (accessed January 6, 2014).

[233] Chevron employees were leaders in the development of the industry standard on sulfidation corrosion, API RP 939-C.

PHAs merely listed general safeguards. If the adequacy of these safeguards to control and prevent damage mechanisms had been verified, recommendations could have been made to improve safeguards intended to protect against the failure of the highly susceptible carbon steel equipment.

7.7.3 Applicable API Standards Lack Minimum Requirements to Control Hazards

The Anacortes and Richmond refineries relied on API standards to assist in the selection of materials of construction for both Tesoro NHT heat exchangers and the Chevron piping circuit: specifically, API RP 941, *Steels for Hydrogen Service at Elevated Temperatures and Pressures in Petroleum Refineries and Petrochemical Plants,* and API RP 939-C, *Guidelines for Avoiding Sulfidation (Sulfidic) Corrosion Failures in Oil Refineries*. Both documents provide guidance on how to avoid HTHA and sulfidation corrosion failures, respectively, but neither document imposes minimum requirements on the user to adequately control hazards. In fact, the CSB found in its Chevron investigation that API RP 939-C was specifically written to ***not*** require any action by the user (emphasis added). Thus, API's current consensus, standard creating process is not effective in ensuring that companies perform essential safety practices that can prevent fatal process safety incidents.

7.7.4 Weak Regulations and Ineffective Regulators

The CSB found significant gaps in the regulations and the competency of the regulators in both Washington and California. Refineries in both states are required to comply with requirements in the state OSHA PSM and EPA RMP regulations. However, neither state's regulations were successful in preventing major process safety incidents.

Under the existing regulatory systems in both Washington and California, there is no requirement to conduct DMHRs or to reduce risk to ALARP. Both Tesoro and Chevron were required to "control" hazards, but there was no requirement to evaluate the effectiveness of the controls or to ensure the use of the hierarchy of controls. In addition, there is no requirement to submit PHAs to the regulator, and the regulator is not responsible for assessing the quality of the PHA or the proposed safeguards. Furthermore, neither Washington nor California requires the use of inherently safer design to the greatest extent feasible. A safety case regulatory regime in both states would help to ensure that all of the refineries in these states rigorously apply process safety concepts that focus more effectively on prevention. The new regulatory framework would also emphasize the implementation of inherently safer designs and the hierarchy of controls to prevent major process safety incidents.

Both states also have significant weaknesses in their staffing of PSM inspectors. Washington L&I (the Washington PSM regulator) and Cal/OSHA (the California PSM regulator) lack sufficient technically experienced and qualified staff members to verify that PSM requirements are being implemented adequately. Cal/OSHA has only seven inspectors, and only one with a technical background, for 1,700 PSM-covered facilities, and Washington L&I has only four inspectors, and only one with a technical background, for more than 270 PSM-covered facilities.

As described in the CSB Chevron Regulatory Report and in Section 7.0 of this report, it is essential that regulators of high-hazard facilities are independent, well funded, well staffed, and technically qualified. These regulators must be able to communicate effectively with refinery personnel and to monitor the adequacy of refinery process safety practices.

7.8 Environmental Protection Agency and Chemical Accident Release Programs

The CSB determined that a key causal factor of the April 2010 incident was Tesoro's failure to implement more effective safeguards to prevent the heat exchanger failure, such as the use of inherently safer materials that are resistant to HTHA. In a number of recent CSB investigations, such as the Chevron Richmond Refinery incident, the CSB found that the implementation by the company of the hierarchy of controls and inherent safety could have helped to prevent the incident. A number of these incidents had significant offsite consequences or had the potential to do so. The CSB has determined that Tesoro policies and relevant API standards do not require the application of inherently safer systems analysis or use of the hierarchy of controls to more effectively prevent chemical accidents. In this section of the report the CSB will examine the requirements of the use of inherent safety under the Clean Air Act and EPA's Risk Management Program.

Both the Chevron and Tesoro incidents could have been prevented if inherently safer equipment construction materials had been used.

7.8.1 Background

Under the authority of the Clean Air Act (CAA) section 112(r),[234] the EPA adopted the Risk Management Program regulations at 40 CFR Part 68, which went into effect in 1999. The CAA provides that the regulations and appropriate guidance developed "provide to the greatest extent practicable, for the prevention and detection of accidental releases of regulated substances and for response to such releases by the owners or operators of the sources of such releases."[235] The EPA's Risk Management Program requires facilities that contain more than the threshold quantity of any of the 77 listed toxic chemicals or

[234] 42 U.S.C. §7412(r)(7)(B)(ii) requires the Administrator to promulgate regulations that "shall require the owner or operator of stationary sources at which a regulated substance is present in more than a threshold quantity to prepare and implement a risk management plan to detect and prevent or minimize accidental releases of such substances from the stationary source, and to provide a prompt emergency response to any such releases in order to protect human health and the environment." (1999).

[235] 42 U.S.C. §7412(r)(7)(B)(i) (1990).

63 flammable substances[236] to prepare and submit to the regulating agency emergency contact information, descriptions of processes and hazardous chemicals onsite, an accident history, and worst-case release scenarios.[237] The regulation defines three different Program levels (Program 1, 2, or 3) based on a process unit's potential for impact to the public and the requirements to prevent accidents.[238] Program 3 processes are subject to additional, more stringent requirements to prevent accidents similar to those of the OSHA PSM standard. Program 3 facilities must implement elements of a prevention program, including: process safety information (PSI), PHA, standard operating procedures (SOPs), training, mechanical integrity, compliance audits, incident investigations, MOC, pre-startup reviews, employee participation, and hot work permits. These prevention program elements are based primarily on the OSHA PSM standard, and much of the language contained in each element is identical to the PSM standard.

Each covered facility is required to submit a risk management plan (RMP) to EPA for all covered processes[239] and update and resubmit these plans at least once every five years, or whenever a major accident occurs or the emergency contact information changes. Completing and submitting the RMP satisfies the regulatory requirement; again, the effectiveness of the RMP in risk reduction is not assessed by the EPA, rendering this another activity-based requirement for a covered facility. There is no approval of the RMP by the EPA, and there is no additional duty on the facility to implement what it says it is doing in the RMP, unlike the safety case regulatory regime.

Any facility with one or more covered processes must include in its RMP an executive summary; the registration for the facility; the certification statement; a worst-case scenario for each process involving flammables or toxics; the five-year accident history for each process; information concerning emergency response at the facility; at least one alternative release scenario analysis for each regulated toxic substance or flammable; a summary of the prevention program for each Program 2 process; and a summary of the prevention program for each Program 3 process.[240]

The Tesoro Anacortes Refinery is a covered facility under the RMP program, and its CR/NHT unit is considered to be a Program 3 process, as it contains more than the threshold quantity of a flammable mixture including butane, ethane, hydrogen, methane, and propane.[241] The refinery last submitted an updated RMP to EPA on March 28, 2011. The RMP contained a five-year accident history that listed the April 2, 2010, NHT catastrophic heat exchanger failure as well as a section on worst-case scenarios,

[236] According to 40 CFR §68.10(a), "[a]n owner or operator of a stationary source that has more than a threshold quantity of a regulated substance in a process, as determined under §68.115, shall comply with the requirements of this part no later than the latest of the following dates…"

[237] *See* 40 CFR §68.12. General Requirements.

[238] *See* 40 CFR §68.10. Applicability.

[239] 40 CFR §68.150 (1999).

[240] EPA Office of Solid Waste and Emergency Response. *General Guidance on Risk Management Programs for Chemical Accident Prevention (40 CFR Part 68);* March 2009; pp 9-1 and 9-2. *See* http://www.epa.gov/osweroe1/docs/chem/Toc_final.pdf (accessed May 14, 2013).

[241] *See* http://data.rtknet.org/rmp/rmp.php?database=rmp&detail=3&datype=t&facility_id=100000028034 (accessed January 23, 2014).

which stated that the worst-case scenario associated with a release of flammable substances at Tesoro would be a vapor cloud explosion involving the full inventory of the largest storage tank containing an RMP regulated flammable mixture.[242]

7.8.2 Enforcement of Inherent Safety in the United States

Although industry good practice guidance provides[243] that inherently safer technology (IST) is the preferable and often the most effective safety precaution in the hierarchy of controls to prevent major accidents it is not enforced by the EPA through its RMP program or through its General Duty Clause or other provisions of the Clean Air Act.

7.8.3 The EPA RMP Program

As discussed in Section 4.1.3, the hierarchy of controls is a well-recognized safety tool to rank the effectiveness of techniques to control hazards, with inherent safety being the most effective choice. The CCPS defines inherently safer design as the process of identifying and implementing inherent safety in a specific context that is permanent and inseparable.[244] The CCPS also notes that "inherently safer design solutions eliminate or mitigate the hazard by using materials and process conditions that are less hazardous."[245] Regulatory regimes around the world have recognized the importance of inherent safety; for example, the HSE requires major hazard facilities in the UK to implement inherently safer systems analysis including at the design stage in order to satisfy the risk reduction requirement of as low as reasonably practicable, or ALARP.[246]

The RMP program regulations under 40 CFR Part 68 do not require the use or implementation of inherently safer design or the hierarchy of controls. This is reflected in both the regulatory language, which does not mention either concept, as well as citations issued by the EPA to companies following an incident. As of January 2014, the EPA had issued no civil enforcement penalties to Tesoro as a result of its April 2010 incident that resulted in seven fatalities. The EPA did conduct "post-incident" inspections of the Tesoro Anacortes Refinery in January and October of 2011. However, no violations were issued related to the implementation of inherently safer systems analysis or the hierarchy of controls. In December 2013 the EPA also issued a Finding of Violations relating to the Chevron Richmond Refinery incident of August 2012. Again, no violations related to either accident prevention approach.

---

242 *Ibid.*

243 CRC Press, *Process Plants: A Handbook for Inherently Safer Design Second Edition*; Kletz, Trevor and Amyotte, Paul; 2010; pp 15-16.

244 Center for Chemical Process Safety (CCPS). *Inherently Safer Chemical Processes – A Life Cycle Approach.* 2nd ed., Section 2.2, 2009.

245 *Ibid* at Section 5.1.1.

246 According to the HSE, essential considerations for determining whether a duty holder has reduced risks to ALARP include "the adoption of inherently safer designs…." HSE. *The Safety Report Assessment Manual, Sections 8 to 15.* p 30. http://www.hse.gov.uk/comah/sram/s8-15.pdf (accessed October 30, 2013). The HSE also notes that the guidance to COMAH Regulation 4 (General Duty) "describes the application of all measures necessary to reduce risk of a major accident to ALARP based on a hierarchical approach (inherent safety, prevention, control, mitigation)." *Ibid* at 8.

The CSB found in both its Chevron and Tesoro investigations that the incidents could have been prevented if inherently safer materials of construction had been used. In the years leading up to the Chevron incident, Chevron employees repeatedly recommended implementing inherently safer designs through the management of change (MOC) process, incident investigations, technical reports, and recommendations from employees in the past. However, despite the fact that Chevron's training programs on inherently safer systems stated that "the greatest opportunity to eliminate or minimize hazards [is] during the development phase of new projects or major revamps of existing facilities," the CSB did not identify any documented, thorough analysis of these proposed inherently safer solutions. Instead, Chevron repeatedly failed to implement proposed inherently safer recommendations to upgrade crude unit piping from carbon steel to metallurgy that was less susceptible to sulfidation corrosion. This led to extremely thinned piping which ultimately ruptured on August 6, 2012.

At Tesoro, the CSB found that the carbon steel E heat exchanger ruptured because it was in a highly weakened state because of HTHA. As discussed in Section 7.4 the Tesoro PHA goals encourage PHA teams to seek inherently safer safeguards to reduce risk. However, these approaches were never implemented until after the April 2010 incident. As discussed in Section 4.1.3, the CSB determined that implementing inherently safer design by using materials that are HTHA-resistant, such as stainless steel, is higher on the hierarchy of controls than post-weld heat treating or reliance upon inspections, and is therefore a better approach to prevent HTHA damage.

7.8.4 The General Duty Clause

Section 112(r)(1) of the Clean Air Act, known as the General Duty Clause, states the following:

> It is the objective of the regulations and programs authorized under this subsection to prevent the accidental release and to minimize the consequences of any such release of any substance listed pursuant to paragraph (3) or any other extremely hazardous substance. Owners and operators of stationary sources producing, processing, handling, or storing such stances under paragraph (3) have a general duty to identify hazards which may result from accidental releases using appropriate hazard assessment techniques, to design and maintain a safe facility taking such steps as are necessary to prevent releases, and to minimize the consequences of accidental releases which do occur.[247]

The General Duty Clause has been in effect since November 15, 1990, when Congress adopted the Clean Air Act Amendments of 1990. According to EPA guidance on the General Duty Clause, "EPA believes that owners and operators who have [] [extremely hazardous] substances must adhere, at a minimum, to recognized industry standards and practices (as well as any government regulations) in order to be in

[247] 42 U.S.C. §7412(r)(1) (1990).

compliance with the general duty clause."[248] The EPA notes that to comply with the General Duty Clause, "many industries have developed standards and generally recognized safe practices to manage the risks associated with extremely hazardous substances."[249]

The application of IST is considered by many to be good industry practice. Yet inherent safety concepts are not enforced by the EPA through the General Duty Clause. According to process safety expert Dr. Paul Amyotte in a presentation at the CSB's April 2013 Chevron Interim Report Public Meeting in Richmond, California, there are numerous resources available on the topic of inherent safety, most of which are written by "industrial practitioners." The call for widespread use of inherently safer design principles in industry is being made mainly by people in industry.[250] For example, as discussed in Section 4.1.4, API RP 571 *Damage Mechanisms Affecting Fixed Equipment in the Refining Industry* implicitly supports the concept of inherently safer design by describing material selection to avoid HTHA failures, noting "300 Series SS, as well as 5Cr, 9Cr and 12Cr alloys, are not susceptible to HTHA at conditions normally seen in refinery units."[251] In addition, the CCPS has stated in its 2009 book *Inherently Safer Chemical Processes A Life Cycle Approach*, which was written by 18 committee members, 16 of which were listed as having affiliation with industrial companies, that the modern approach to chemical process safety "is to apply risk management systems theory…[which] includes recognition of the hazards posted by the process, and a continual effort to analyze the risks, and to reduce or control them to the lowest levels practical…."[252]

> **Although inherently safer technology (IST) is the most effective major accident prevention approach in the hierarchy of controls, it is not enforced by the EPA through the General Duty Clause under the Clean Air Act.**

7.8.5 The EPA's Authority to Enforce Inherent Safety

The EPA has acknowledged that it has the authority to require the application of IST through the General Duty Clause. In an August 2013 letter responding to a Congressional inquiry that specifically asked, among other things, whether the EPA believes it "has the authority to mandate the use and/or

---

248 EPA. *Guidance for Implementation of the General Duty Clause Clean Air Act Section 112(r)(1).* May 2000; p 2. http://www.epa.gov/oem/docs/chem/gdcregionalguidance.pdf (accessed January 23, 2014).

249 *Ibid.*

250 Dr. Paul Amyotte. Presentation to the U.S. Chemical Safety and Hazard Investigation Board Public Meeting to Release Interim Report and Safety Recommendations Resulting from Chevron Refinery Investigation. Richmond, CA April 19, 2013; p 2.

251 API RP 571. *Damage Mechanisms Affecting Fixed Equipment in the Refining Industry.* 2003; page '5-83'.

252 CCPS. *Inherently Safer Chemical Processes – A Life Cycle Approach.* 2nd ed.; 2009; p 9.

consideration of Inherently Safer Technologies under Section 112(r) of the Clean Air Act[,]" EPA Assistant Administrator Mathy Stanislaus stated that the EPA has "broad authority to promulgate regulations for chemical accident prevention…" and can "consider factors such as facility design, equipment, and quantity of substances handled (and other factors)." He also stated that the EPA was currently evaluating various methods of improving increased chemical plant safety including safer management, increased preparedness management, and facility design and operations, and would also be examining best practices being utilized by industry leaders.

> **The EPA has the authority to require the application of IST through the General Duty Clause.**

Others have argued that the EPA has additional authority under Clean Air Act section 112(r)(7)(A) to promulgate a new rule requiring industries to implement IST. This section authorizes the EPA Administrator to "promulgate release prevention, detection, and correction requirements which may include monitoring, record-keeping, reporting, training…and other design, equipment, work practice, and operational requirements."[253] Section 112(r) further requires that the risk management plan include "safety precautions and maintenance, monitoring and employee training measures" to prevent accidental releases.[254] As described in Section 4.1.3, inherent safety and the hierarchy of controls are long established, widely recognized methods for achieving more effective safety precautions to prevent chemical accidents. Incorporating requirements for the implementation of inherent safety and the hierarchy of controls is not only consistent with the 112(r) proscribed features of the risk management plan but in fact serves to make the safety precautions more effective in preventing accidental releases.

Despite its acknowledged authority to do so, to date the EPA has not required industries to implement IST through either the creation of a new rule or the enforcement of the Clean Air Act General Duty Clause. In the wake of Bhopal and more recently the 9/11 tragedy, many groups have urged the EPA to create a new regulation requiring the implementation of IST or at a minimum, use its authority under the General Duty Clause to require industries to implement IST. On March 14, 2012, the National Environmental Justice Advisory Council[255] (NEJAC) sent a letter to the EPA urging the agency to promulgate new rules or guidance to "utilize its authority under the 'General Duty Clause' of the 1990 Clean Air Act section 112(r) (also known as the Bhopal clause) to require covered chemical facilities to prevent, where feasible, catastrophic chemical releases."[256] The NEJAC noted that flaws in the chemical security law

[253] 42 U.S.C. §7412(r)(7)(A) (1990).

[254] 42 U.S.C. §7412(r)(7)(B)(ii)(II) (1990).

[255] NEJAC is a federal advisory committee to EPA that was established on September 30, 1993. It provides advice and recommendations about issues related to environmental justice. For more information *see* http://www.epa.gov/Compliance/ej/nejac/index.html (accessed January 24, 2014).

[256] *See* https://www.documentcloud.org/documents/332041-nejac-letter.html (accessed January 22, 2014).

administered by the U.S. Department of Homeland Security (DHS) prohibited the agency from requiring the use of safer chemical processes at facilities. The group also reiterated that the EPA had made a proposal in 2002 to implement the General Duty Clause to make chemical plants safer. According to the proposal, chemical plants would be made "inherently safer by reducing quantities of hazardous chemicals handled or stored, substituting less hazardous chemicals for extremely hazardous ones, or otherwise modifying the design of processes to reduce or eliminate chemical hazards."[257] The NEJAC also stated that in 2003, the Government Accountability Office (GAO) concluded that the EPA could "'interpret the Clean Air Act's general duty clause to address chemical facility security… According to EPA, it would not have to make any regulatory changes as it currently implements the general duty clause through guidance...' to address the specific threat of disastrous risks to vulnerable communities."[258] The NEJAC concluded by recommending that "EPA use its authority under the 1990 Clean Air Act, Section 112(r), to reduce or eliminate these catastrophic risks, where feasible, by issuing new rules and guidance to fully implement the General Duty Clause. This action would reduce the danger and imminent threat that chemical plants, chemical manufacturing, and the transport and storage of hazardous chemicals pose to environmental justice and communities."[259]

On July 25, 2012, the Coalition to Prevent Chemical Disasters[260] ("the Coalition") petitioned the EPA to "commence a rulemaking [pursuant to the Administrative Procedure Act (AP), 5 U.S.C. §553(e), and section 112(r)(7)(A)[261] of the Clean Air Act (CAA), 42 U.S.C. §7412(r)(7)(A)] to require the use of inherently safer technologies, where feasible, by facilities that use or store hazardous chemicals." The petition also requested that, pending completion of the rulemaking, EPA revise its guidance concerning the enforcement of the CAA's general duty clause, section 112(r)(1), 42 U.S.C. §7412(r)(1), to "make clear that the duty to prevent releases of extremely hazardous substances includes the use, where feasible, of safer technologies to minimize the presence and possible release of hazardous chemicals."[262]

In the wake of the April 2013 explosion and fire that occurred at a facility in West, Texas, and resulted in fifteen fatalities and hundreds of injuries, President Obama issued Executive Order 13650 on August 1, 2013. It established the Chemical Facility Safety and Security Working Group, which includes OSHA

---

[257] *Ibid.*

[258] *Ibid.*

[259] *Ibid.*

[260] The Coalition consists of over 100 organizations formed to prevent chemical disasters and protect workers. For more information *see* http://preventchemicaldisasters.org/ (accessed January 24, 2014).

[261] 42 U.S.C. §7412(r)(7)(A) states: "In order to prevent accidental releases of regulated substances, the Administrator is authorized to promulgate release prevention, detection, and correction requirements which may include monitoring, record-keeping, reporting, training, vapor recovery, secondary containment, and other design, equipment, work practice, and operational requirements. Regulations promulgated under this paragraph may make distinctions between various types, classes, and kinds of facilities, devices and systems taking into consideration factors including, but not limited to, the size, location, process, process controls, quantity of substances handled, potency of substances, and response capabilities present at any stationary source. Regulations promulgated pursuant to this subparagraph shall have an effective date, as determined by the Administrator, assuring compliance as expeditiously as practicable."

[262] https://www.documentcloud.org/documents/404584-petition-to-epa-to-prevent-chem-disasters-filed.html (accessed January 22, 2014).

and the EPA, and tasked the group with, among other things, developing options for enhancing and modernizing policies, regulations, and standards to improve the safety and security of chemical facilities.[263] A senior EPA official overseeing implementation of the Executive Order has stated the EPA is examining the successes of a New Jersey program that requires facilities to consider IST, such as safer chemicals, as a possible model for a federal IST policy.[264] New Jersey's 2008 IST rule has led facility owners and operators to take a "hard look at opportunities to reduce risk" at industrial plants.[265]

New Jersey is the only state with some IST requirements.[266] The Toxic Catastrophe Prevention Act (TCPA) implements IST requirements in New Jersey, and covers approximately 90 facilities in the state.[267] An owner or operator of a covered facility must complete an IST review report and must submit it to the New Jersey Department of Environmental Protection (DEP). The report "…shall identify available inherently safer technology alternatives or combinations of alternatives that minimize or eliminate the potential for an EHS [extraordinarily hazardous substance] release."[268]

IST alternatives that are identified must be determined as "feasible" in order for implementation to be required. Feasible means "capable of being accomplished in a successful manner, taking into account environmental, public health and safety, legal, technological, and economic factors."[269] If IST is not implemented, they must provide a written justification using a qualitative and quantitative evaluation of environmental, public health and safety, legal, technological, and economic factors. If they decide to implement the IST, they must provide a schedule of when they will do it.[270]

An update is required every five years for all covered processes and at the same time as the updates of applicable hazard reviews or process hazard analysis. An update of the IST review is also required when there is a major change. While New Jersey's IST rule contains positive features, it is primarily focused on the activity of the production of the IST report and lacks rigorous goal setting elements such as requiring facilities to reduce risks to as low as reasonably practicable, or ALARP or requiring that the use of IST prevent accidental chemical releases.

---

263 *Improving Chemical Facility Safety and Security.* Exec. Order No. 13650, 78 Fed. Reg. 48029 (August 1, 2013). http://www.whitehouse.gov/the-press-office/2013/08/01/executive-order-improving-chemical-facility-safety-and-security (accessed January 24, 2014).

264 http://insideepa.com/Risk-Policy-Report/Risk-Policy-Report-12/03/2013/epa-looks-to-new-jersey-program-as-possible-model-for-ist-requirements/menu-id-1098.html (accessed January 22, 2014).

265 *Ibid.*

266 Contra Costa County, California has a guidance document entitled "Attachment C: Inherently Safer Systems Checklist" which is provided as a tool for facilities to utilize during the PHA process. The actual use of the checklist is not required. *See* http://cchealth.org/hazmat/pdf/iso/attachment_c.pdf (accessed April 17, 2013).

267 Under Title 7 of the New Jersey Administrative Code. *See* N.J.A.C. Section 7:31-4.12 (2010). Available at http://www.nj.gov/dep/rpp/brp/tcpa/downloads/conrulerev9_no%20fonts.pdf (accessed January 23, 2014).

268 N.J.A.C. Section 7:31-4.12 (d) (2010).

269 N.J.A.C. Section 7:31-1.5 (2010).

270 N.J.A.C. Section 7:31-4.12 (e) and (f) (2010).

7.8.6 The Role of Inherent Safety in Major Accident Prevention

In 2011, Dr. Paul Amyotte released an article analyzing 63 CSB reports, studies, and bulletins resulting from CSB incident investigations to identify examples related to inherent safety and risk reduction measures. The article identified over 200 examples of the hierarchy of controls, with 36 percent of those being inherent safety.[271] He concluded that the CSB products contained numerous examples where the use of the hierarchy of controls, including inherent safety, would be helpful in reducing risk in the process industries.[272] The four main principles of inherent safety (minimization, substitution, moderation, and simplification) all play a role in the prevention and mitigation of process incidents.

Simply put, the CSB has investigated numerous major process safety incidents over the years, including the Chevron and Tesoro incidents, where the implementation of inherently safer design and materials of construction could have prevented the incident. The EPA should work with industry and stakeholders to develop and implement a new regulation requiring companies to use inherently safer systems analysis and the hierarchy of controls in establishing safeguards for identified process hazards to help prevent these major process safety incidents from occurring in the future. While the new regulation is being adopted, the EPA should use its existing authorities under the CAA General Duty Clause to implement inherently safer systems and the hierarchy of controls to the greatest extent feasible for chemical accident prevention.

[271] Amyotte, Paul; MacDonald, Dustin K.; and Khan, Faisal I. *An Analysis of CSB Investigation Reports Concerning the Hierarchy of Controls.* 2011; p 1.

[272] *Ibid.*

8.0 Recommendations

Pursuant to its authority under 42 U.S.C. §7412(r)(6)(C)(i) and (ii), and in the interest of promoting safer operations at petroleum refineries and protecting workers and communities from future accidents both in the state of Washington and nationally, the CSB makes the following safety recommendations:

8.1 The U.S. Environmental Protection Agency

2010-08-I-WA-R1

Revise the Chemical Accident Prevention Provisions under 40 CFR Part 68 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. The goal shall be to reduce the risk of major accidents to the greatest extent practicable, to be interpreted as equivalent to as low as reasonably practicable (ALARP). Include requirements for inherently safer systems analysis to be automatically triggered for all management of change, incident investigation, and process hazard analysis reviews and recommendations, prior to the construction of a new process, process unit rebuilds, significant process repairs, and in the development of corrective actions.

2010-08-I-WA-R2

Until Recommendation 2010-08-I-WA-R1 is in effect, enforce the use of inherently safer systems analysis and the hierarchy of controls to the greatest extent feasible in establishing safeguards for identified process hazards through the Clean Air Act's General Duty Clause, section 112(r)(1), 42 U.S.C. §7412(r)(1).

2010-08-I-WA-R3

Develop guidance for the required use of inherently safer systems analysis and the hierarchy of controls for enforcement under 40 CFR Part 68 and the Clean Air Act's General Duty Clause, section 112(r)(1), 42 U.S.C. §7412(r)(1).

8.2 Washington State Legislature, Governor of Washington

2010-08-I-WA-R4

Develop and implement a step-by-step plan to supplement the existing process safety management regulatory framework for petroleum refineries in the state of Washington with a more rigorous safety management regulatory framework based on the principles of the "safety case" type regulatory regime in use in countries such as the United Kingdom, Australia, and Norway, and as described in this report, with the following minimum components:

a. A case for safety written by the duty holder that includes a systematic analysis and documentation of all major hazards and effective control methods implemented to reduce those risks as low as reasonably practicable (ALARP);

b. A thorough review of the safety case report by technically competent regulatory personnel that requires modifications and improvements to the document as necessary prior to acceptance;

c. Audits and preventative inspections by the regulator to verify effective implementation of safety case elements;

d. A risk management approach that requires analysis and effective implementation of safeguards, using the hierarchy of controls, to protect people and the environment from major accident hazards. The effectiveness of the safeguards will be demonstrated through the use of leading and lagging process safety indicators. Include indicators that measure safety culture, such as incident reporting and action item implementation culture;

e. Ability to adapt and implement safety requirements in response to newly identified hazards, advances in technology, lessons learned from major accidents, and improved safety codes without the need for new rule-making;

f. Determines when new or improved industry standards and practices are needed and initiates programs and other activities such as forums to prompt the timely development and implementation of such standards and practices;

g. Uses a tripartite model where the regulator, the company, and workers and their representatives play an equal and essential role in the direction of preventing major accidents;

h. A regulatory model and accompanying guidance based on the UK's The Safety Representatives and Safety Committees Regulations 1977 and the Health and Safety (Consultation with Employees) Regulations 1996, which set out the legal framework for the rights and responsibilities of workers and their representatives on health and safety-related matters, and the election of safety representatives and establishment of safety committees to serve health and safety-related functions. The elected representatives should have a legally recognized role that goes beyond consultation in activities such as process hazard analysis, management of change, incident investigation, audits, and identification and effective control of hazards. The representatives should also have the authority to stop work that is perceived to be unsafe or that presents a serious hazard until the regulator intervenes to address the safety concern. Workforce participation practices should be documented by the duty holder and submitted to the regulator;

i. Requires reporting of information to the public such as a summary of the safety case report, a list of safeguards implemented and standards used to reduce risk, and process safety indicators that demonstrate the effectiveness of the safeguards and management systems;

j. An independent, well-funded, well-staffed, technically competent regulator; and

k. A compensation system to assure the safety case regulator has the ability to attract and retain a sufficient number of employees with the necessary skills and experience to ensure regulator technical competency. Periodically conduct a market analysis and benchmarking review to ensure the compensation system remains competitive with equivalent positions in the Washington petroleum refineries.

2010-08-I-WA-R5

Work with the regulator, the petroleum refining industry, labor, and other relevant stakeholders in the state of Washington to develop and implement a system that collects, tracks, and analyzes process safety leading and lagging indicators from operators and contractors to promote continuous safety improvements. At a minimum, this program shall:

a. Require the use of leading and lagging process safety indicators to actively monitor the effectiveness of process safety management systems and safeguards for major accident prevention. Include leading and lagging indicators that are measureable, actionable, and standardized. Require that the reported data be used for continuous process safety improvement and accident prevention;

b. Analyze data to identify trends and poor performers and publish annual reports with the data at facility and corporate levels;

c. Require companies to publicly report required indicators annually at facility and corporate levels;

d. Use process safety indicators (1) to drive continuous improvement for major accident prevention by using the data to identify industry and facility safety trends and deficiencies and (2) to determine appropriate allocation of regulator resources and inspections; and

e. Be periodically updated to incorporate new learning from world-wide industry improvements in order to drive continuous major accident safety improvements in Washington.

2010-08-I-WA-R6

Revise the Washington Administrative Code (WAC) Title 296, Section 67 (Process Safety Management), to require improvements to mechanical integrity and process hazard analysis programs for all Washington oil refineries. These improvements shall include engaging a diverse team of qualified personnel to perform a documented damage mechanism hazard review. This review shall be an integral part of the Process Hazard Analysis cycle and shall be conducted on all PSM-covered process piping circuits and process equipment. The damage mechanism hazard review shall identify potential process damage mechanisms and consequences of failure, and shall ensure effective safeguards are in place to control hazards presented by those damage mechanisms. Require the analysis and incorporation of applicable industry best practices and inherently safety systems to the greatest extent feasible into this review.

2010-08-I-WA-R7

Revise the Washington Process Safety Management regulations to require that all safety codes, standards, employer internal procedures and recognized and generally accepted good engineering practices (RAGAGEP) used in the implementation of the regulations contain adequate minimum requirements (“shall” language) to ensure the prevention of potentially catastrophic chemical releases and incidents.

8.3 Department of Safety and Health – Labor and Industries (L&I)

2010-08-I-WA-R8

Perform a verification audit at all Washington petroleum refineries to ensure:

a. Prevention of HTHA equipment failure and safe operation of the equipment. Audit HTHA prevention and process condition monitoring techniques used at all Washington petroleum refineries. Verify that all affected equipment in use meets the requirements contained in Recommendation 2010-08-I-WA-R10.

b. For nonroutine work, a written hazard evaluation is performed by a multidisciplinary team and, where feasible, conducted during the job planning process prior to the day of the job execution. Verify that each facility has an effective written decision-making protocol used to determine when it is necessary to shut a process down to safely perform work or conduct repairs. Ensure the program reflects the guidance in the CCPS *Risk Based Process Safety* book related to hazardous nonroutine work.

c. Effective programs are in place to control of the number of essential personnel present during all hazardous nonroutine work.

2010-08-I-WA-R9

Oversee the performance of the periodic process safety culture surveys performed at the Tesoro Anacortes refinery, per the requirements listed in Recommendation 2010-I-WA-R15. Incorporate the expertise of process safety culture experts in the development and interpretation of the safety culture surveys. Ensure the effective participation of the workforce and their representatives in the development of the surveys and the implementation of corrective actions.

8.4 American Petroleum Institute

2010-08-I-WA-R10

Revise American Petroleum Institute API RP 941*: Steels for Hydrogen Service at Elevated Temperatures and Pressures in Petroleum Refineries and Petrochemical Plants* to:

a. Clearly establish the minimum necessary “shall” requirements to prevent HTHA equipment failures using a format such as that used in *ANSI/AIHA Z10-2012, Occupational Health and Safety Management Systems;*

b. Require the use of inherently safer materials to the greatest extent feasible;

c. Require verification of actual operating conditions to confirm that material of construction selection prevents HTHA equipment failure; and

d. Prohibit the use of carbon steel above 400 ºF in applications where HTHA could occur.

2010-08-I-WA-R11

Revise American Petroleum Institute API RP 581: *Risk-Based Inspection Technology* to:

a. Clearly establish the minimum necessary “shall” requirements to prevent HTHA equipment failures using a format such as that used in *ANSI/AIHA Z10-2012, Occupational Health and Safety Management Systems;*

b. Prohibit the use of carbon steel above 400 ºF in applications where HTHA could occur.

c. Require verification of actual operating conditions to determine potential equipment damage mechanisms.

8.5 Tesoro Refining & Marketing Company LLC

2010-08-I-WA-R12

Actively participate with API in the completion of recommendation 2010-08-I-WA-R10. Document this participation.

2010-08-I-WA-R13

Once recommendation 2010-08-I-WA-R10 is in effect, develop and implement a plan to meet the requirements established through the acceptable completion of recommendation 2010-08-I-WA-R10. Document the implementation of the plan and the corrective actions taken.

2010-08-I-WA-R14

Revise and improve the Process Hazard Analysis (PHA), the Integrity Operating Window (IOW), and the damage mechanism hazard review (DMHR) programs and cross-linking among these three programs such that all identified hazards are effectively managed in each program. For all Tesoro refineries require:

a. the IOW to review the most recent PHA damage mechanism hazards and safeguards identified to control these hazards;

b. the IOW review or revalidation to be conducted at least every five years;

c. the IOW to analyze and incorporate applicable industry best practice, the hierarchy of controls, and inherently safer design to the greatest extent feasible;

d. the DMHR report to be developed by the DMHR team and not just the "corrosion expert;"

e. the DMHR team to review the operating data to verify an accurate understanding of how the data was obtained, what it represents, and that it appropriately addresses both routine and nonroutine operations;

f. the DMHR and/or IOW review to identify and review gaps between current industry best practices and existing Tesoro practices with regard to material selection and process controls and make recommendations that reduce risks from damage mechanism hazards;

g. the DMHR and IOW review to review applicable Tesoro and industry-wide damage mechanism incidents as part of the respective DMHR or IOW review;

h. the DMHR to review relevant MOCs to fully evaluate the impact of the MOC on damage mechanism hazards;

i. the identification of minimum qualifications for the "corrosion expert" and ensure that the DMHR team has the necessary skills to meet these requirements;

j. for sites that have a corrosion/materials engineer, the corrosion/materials engineer shall be a required participant in the DMHR;

k. the PHA to review the most recent DMHR and IOW reviews in order to contain a complete record of all identified damage mechanism hazards, evaluate existing safeguards, and propose new safeguards to control the identified hazards;

l. the PHA to review the consequence of damage mechanism hazards identified in the risk-based inspection (RBI) program and IOW reviews to ensure effective safeguards are present to control the damage mechanism hazard; and

m. the PHA to use the hierarchy of controls and implement opportunities for inherently safer design to the greatest extent feasible.

8.6 Tesoro Anacortes Refinery

2010-08-I-WA-R15

Implement a process safety culture program including a written procedure for periodic process safety culture surveys across the work force at the Tesoro Anacortes Refinery that are administered by a third party approved by the refinery health and safety committee and the regulator. Include a focus on items that measure, at a minimum, willingness to report incidents, normalization of hazardous conditions, and burden of proof of safety in plant process safety programs and practices. Develop and implement corrective actions to address identified process safety culture issues. The third party firm shall issue a report on the survey results and the report shall be made available to the plant workforce. The refinery health and safety committee shall develop corrective actions and monitor progress to ensure effective implementation of these corrective actions. The minimum frequency of process safety culture surveys shall be at least once every three years.

Appendix A AcciMap Causal Analysis

The CSB team has developed an accident map (AcciMap) as a visual depiction of the casual factors of the April 2, 2010 Tesoro Anacortes Refinery explosion and fire (Figure 37).[273] An AcciMap is a multi-layered causal diagram that provides visualization of higher level causes at the company, industry and governmental levels. This diagram is especially useful for developing broadly applicable recommendations for accident prevention,[274] and includes five levels:

- *Outcome:* Consequences of the incident
- *Physical Events and Conditions:* The immediate causes of the incident.[275]
- *Tesoro:* Latent causes of the incident associated with company rules and policies.
- *Industry Codes and Standards:* Latent causes of the incident associated with industry recommended practices, codes, and standards.
- *Government:* Latent causes associated with government laws and legislation developed to manage highly hazardous industries.

[273] A full-size, high resolution version of the Tesoro AcciMap is located on the CSB website.

[274] The AcciMap tool was developed by Jens Rasmussen and popularized by Andrew Hopkins. Rasmussen, J., &. A. Hopkins. *Risk Management in a Dynamic Society: A Modeling Problem*. Safety Science, 27 (2.3), 1997; pp 183-213

[275] Immediate causal factors are the actions and conditions that directly lead to the consequence. However, while understanding immediate causal factors is vital, they are typically symptoms of systemic, or latent, causal factors. Latent causal factors are the pre-actions and pre-conditions that enabled the immediate causal factors to occur. It is these latent causal factors that must be alleviated in order to provide broad corrective change and prevent recurrence of similar incidents.

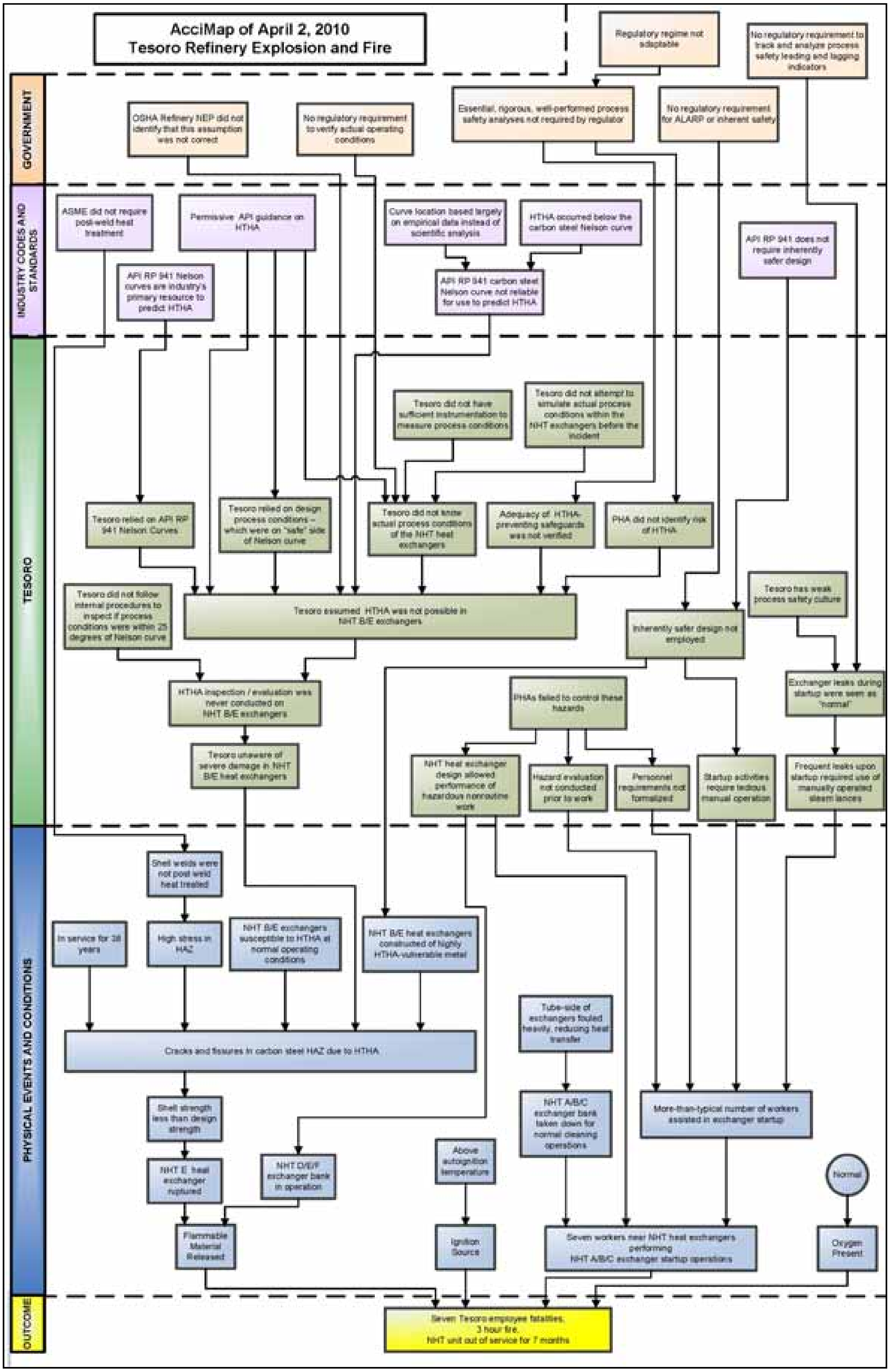


Figure 37. AcciMap of April 2, 2010 Tesoro Anacortes Refinery Explosion and Fire

A.1 AcciMap Outcomes

Seven Tesoro operations personnel were fatally injured following the sudden catastrophic failure of the in-service E heat exchanger that resulted in an explosion and fire. The fire burned for more than three hours and resulted in a seven month shutdown.

A.2 Physical Events and Conditions

The explosion and fire resulted from the sudden catastrophic rupture of the E heat exchanger, releasing flammable material that ignited likely because it was above its autoignition temperature.

The seven fatally-injured employees, a more-than-typical number of workers for this job, were in the process of putting a bank of three heat exchangers (A/B/C) back in service. These heat exchangers were taken out of service several days before the incident for a maintenance cleaning operation to remove fouling, a deposit that greatly reduced heat transfer efficiency of the heat exchangers. While the A/B/C bank of heat exchangers was being cleaned, the NHT Unit continued to operate on the other bank, a matching series of three heat exchangers (D/E/F).

When returning the three clean heat exchangers back to service, the middle heat exchanger of the D/E/F heat exchanger bank (the E heat exchanger) catastrophically ruptured. Post-incident metallurgical analysis determined that the E heat exchanger ruptured because of an advanced stage of HTHA. The HTHA occurred in both the B and E heat exchangers in the high stress, non post-weld heat-treated welds. The heat exchangers were in service for 38 years and were constructed of carbon steel, a material that is highly vulnerable to HTHA damage.

A.3 Tesoro

The intention of the established Tesoro procedures for startup of a bank of these heat exchangers was to require only one operator to be in the unit for the startup activity that was proceeding at the time of the incident. However, the more common practice was for additional operators to assist with this physical, labor-intensive startup activity. On the night of the incident, the operations supervisor requested five additional personnel to assist with the startup. All seven were present at the time of the incident and were working near the site of the explosion and fire.

During startups of these heat exchangers, Tesoro routinely relied on the addition of ad hoc operations staff from other nearby operating units. This use of such additional personnel was explained as a result of both a collaborative culture and a need driven by task requirements. The startup of the heat exchangers required coordinated manual labor. In addition, a history of leaks was seen by the company as “normal” because of the high frequency of such leaks. The mitigation of these leaks required personnel standing by with steam lances, which some of the additional workers were likely doing on the night of the incident.

The startup of the NHT heat exchangers was hazardous nonroutine work. Leaks routinely developed that posed hazards to workers conducting the startup activities. Shell Oil and Tesoro PHAs at the refinery repeatedly failed to ensure that these hazards were controlled and that the number of workers exposed to these hazards was minimized.

Tesoro was not aware of the severe HTHA damage in the B and E heat exchangers because it never performed any type of HTHA examination of the heat exchangers. Tesoro took this approach because corrosion experts had concluded HTHA was not probable in these heat exchangers. This conclusion was based on a combination of reliance on the carbon steel Nelson curve (which the CSB has found to be unreliable) and a lack of knowledge of the actual operating conditions of the NHT heat exchangers. Instead of monitoring or modeling process conditions for use in PHAs and damage mechanism reviews, corrosion experts relied on process design data that suggested a lower HTHA susceptibility than indicated by the CSB modeling estimates. Therefore, these opportunities to identify the risks of HTHA were unsuccessful in preventing the April 2010 incident.

A.4 Industry Codes and Standards

API RP 941 is the industry standard for preventing equipment failure from HTHA by establishing equipment operating limits. This standard contains empirical industry HTHA experience based on temperature and hydrogen partial pressure. It notes operating boundaries at locations where various materials of construction have failed because of HTHA and where they apparently have not failed. Over the years, the boundaries have become more conservative in response to industry failures that occurred outside of the previously experienced operating limits.

API RP 941 is written with permissive language. It is presented as a guideline that "is often used when selecting materials in hydrogen service." It is also described as "an aide for materials selection." API RP 941 does not establish minimum requirements to prevent HTHA failures:

- There are no minimum requirements for performing HTHA susceptibility evaluations.
- There are no minimum requirements for selection of materials of construction to ensure that inherently safer design is employed.

Analysis of the metal recovered from the B and E heat exchanger shell walls revealed a significant occurrence of HTHA well within the "safe" operating limits established by API RP 941, indicating that the current location of the carbon steel Nelson curve cannot be trusted to prevent equipment failure and cannot be relied on to predict the occurrence of HTHA. Damage from HTHA was occurring in portions of the B and E heat exchangers that CSB process modeling determined were operating as much as 120 °F degrees below the carbon steel Nelson curve.

Other industry standards, such as API RP 581, offer guidance on how to predict, mitigate, and control the occurrence of HTHA. However, such standards share similar weaknesses with API RP 941. API 581 does not require verification of actual operating conditions when identifying applicable damage mechanisms. API RP 581 calculations to determine susceptibility of equipment to HTHA confirmed that the B and E heat exchangers were not susceptible to HTHA.

A.5 Government

The existing federal and state of Washington regulations for PSM of highly hazardous chemicals were not sufficient to prevent this incident as they were primarily activity based and did not focus on specific risk reduction (such as ALARP), inherently safer design, require leading and lagging process safety indicators, or require continuous improvement. For example, the unit PHA ineffectively identified and managed hazards, but its completion still satisfied the state of Washington's PSM standard. In addition, despite its ability to do so, the EPA does not require facilities to analyze opportunities to implement inherently safer design.

The state of Washington's L&I completed a formal inspection of the CR and NHT process units as part of the OSHA Refinery NEP in March 2009, just more than one year before the incident. However, the NEP inspection lacked the level of detail required to detect the technical deficiencies in the Tesoro refinery's mechanical integrity program. No HTHA issues were identified, and no citations relating to the E heat exchanger were issued. The state of Washington did not have sufficient personnel resources with the required technical knowledge and experience to seek out and oversee the highly technical area of failure mechanisms. The state of Washington has only four PSM specialists in its compliance section to regulate nearly 270 PSM-covered facilities, including five petroleum refineries.

Appendix B NHT A/B/C Heat Exchanger Startup Trend Data

Trends of tube-side outlet temperatures are shown in Figure 39 through Figure 42 for the night of the incident and for the three previous startups for the A/B/C heat exchangers. The locations of the two temperature measurements are shown in Figure 38.

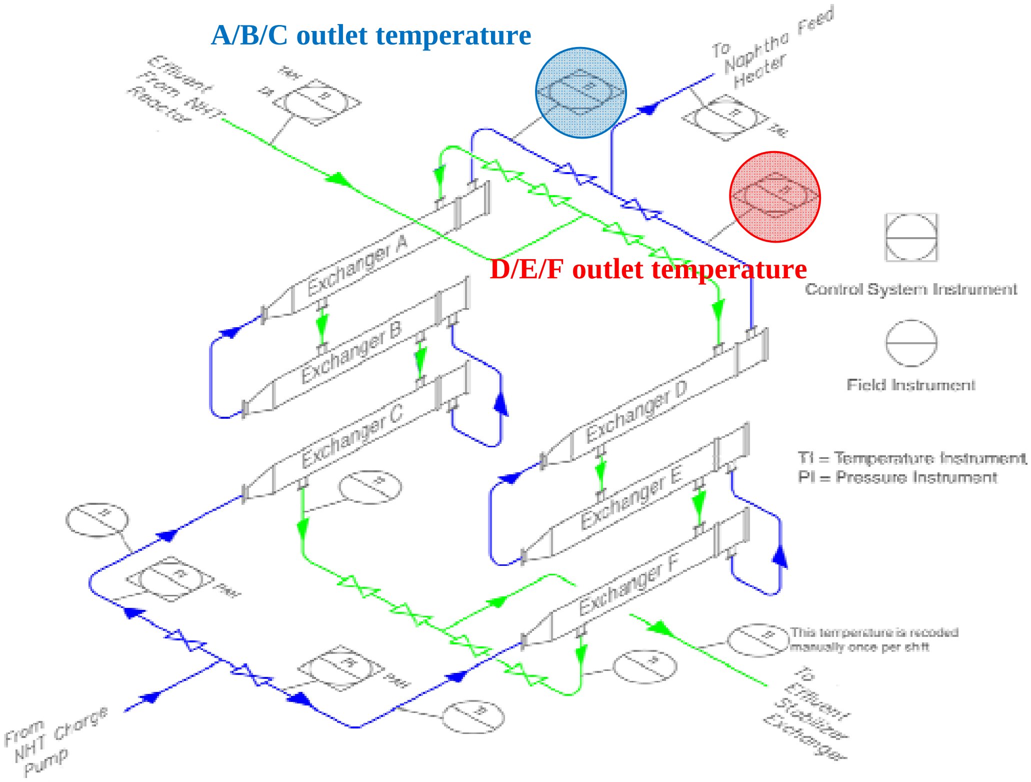


Figure 38. Location of the Two Outlet Temperature Measurements

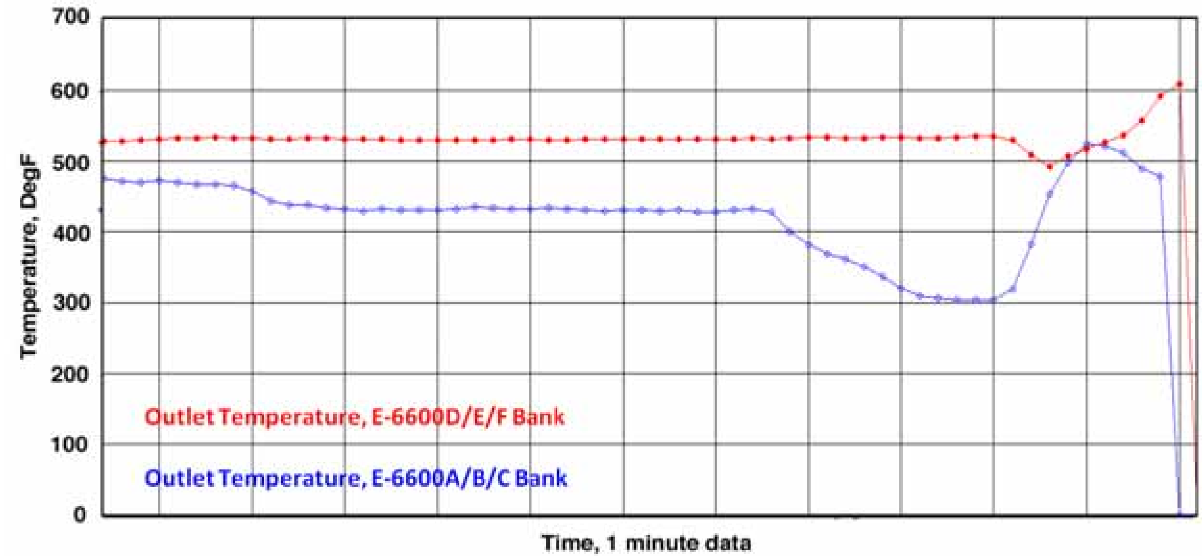


Figure 39. Temperature Data During NHT A/B/C Heat Exchanger Bank Startup on Night of the Incident

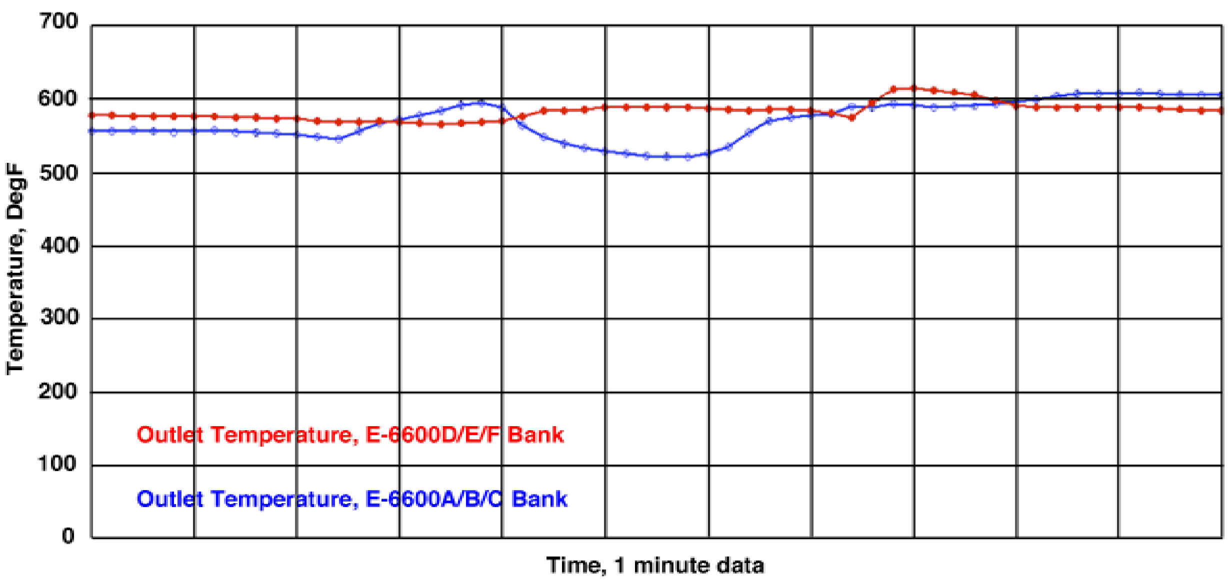


Figure 40. Temperature Data During NHT A/B/C Heat Exchanger Bank Startup on August 29, 2009

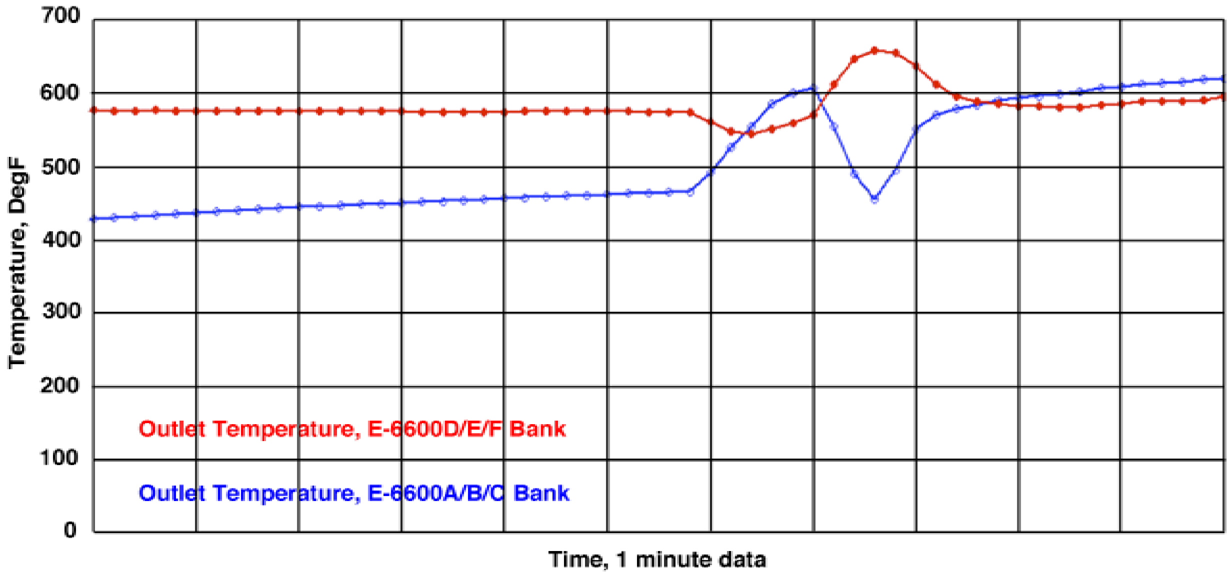


Figure 41. Temperature Data During NHT A/B/C Heat Exchanger Bank Startup on April 2, 2009

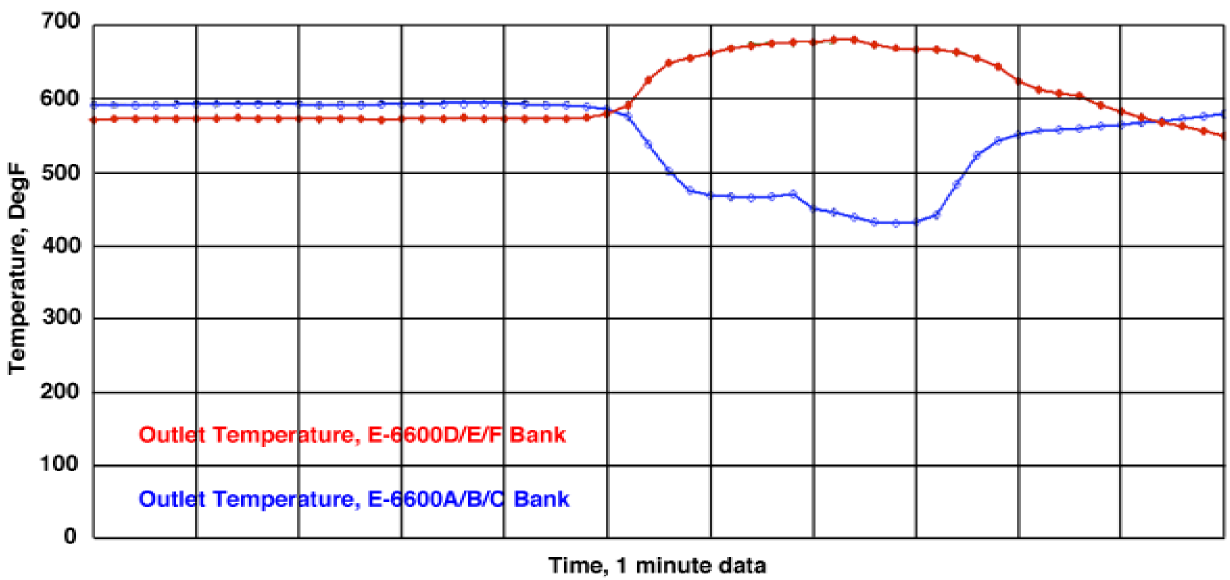


Figure 42. Temperature Data During NHT A/B/C Heat Exchanger Bank Startup on February 3, 2008

Appendix C CSB Simulation of the NHT Heat Exchangers

C.1 Background

Process conditions (temperature, pressure, flow, and composition data) were available for the NHT feed streams entering and exiting the two banks of the NHT heat exchangers (Figure 43). However, the system lacked instrumentation between the individual heat exchangers. Therefore, the actual process conditions of the fluid entering and exiting the B and E heat exchangers were not available. The CSB used the *Aspen HYSYS*® and *Aspen Exchanger Design and Rating* process simulation computer software to model the A/B/C and D/E/F heat exchanger banks for estimating process conditions in the B and E heat exchangers where HTHA occurred.

Of particular importance was the capability to model the qualitative fouling observations documented by Shell Oil workers.[276] These observations indicate that the heat exchangers primarily fouled within the tubes. The observations also indicate that fouling in the A and D tubes was "Heavy", fouling in the B and E tubes was "Moderate", and fouling in the C and F tubes was "Light."[277] The documented observations show that the shell-side of the NHT heat exchangers experienced the formation of a light scale.

[276] These observations were made when Shell Oil owned the refinery.

[277] Other qualitative descriptions were also noted. However, these conditions were most frequently reported.

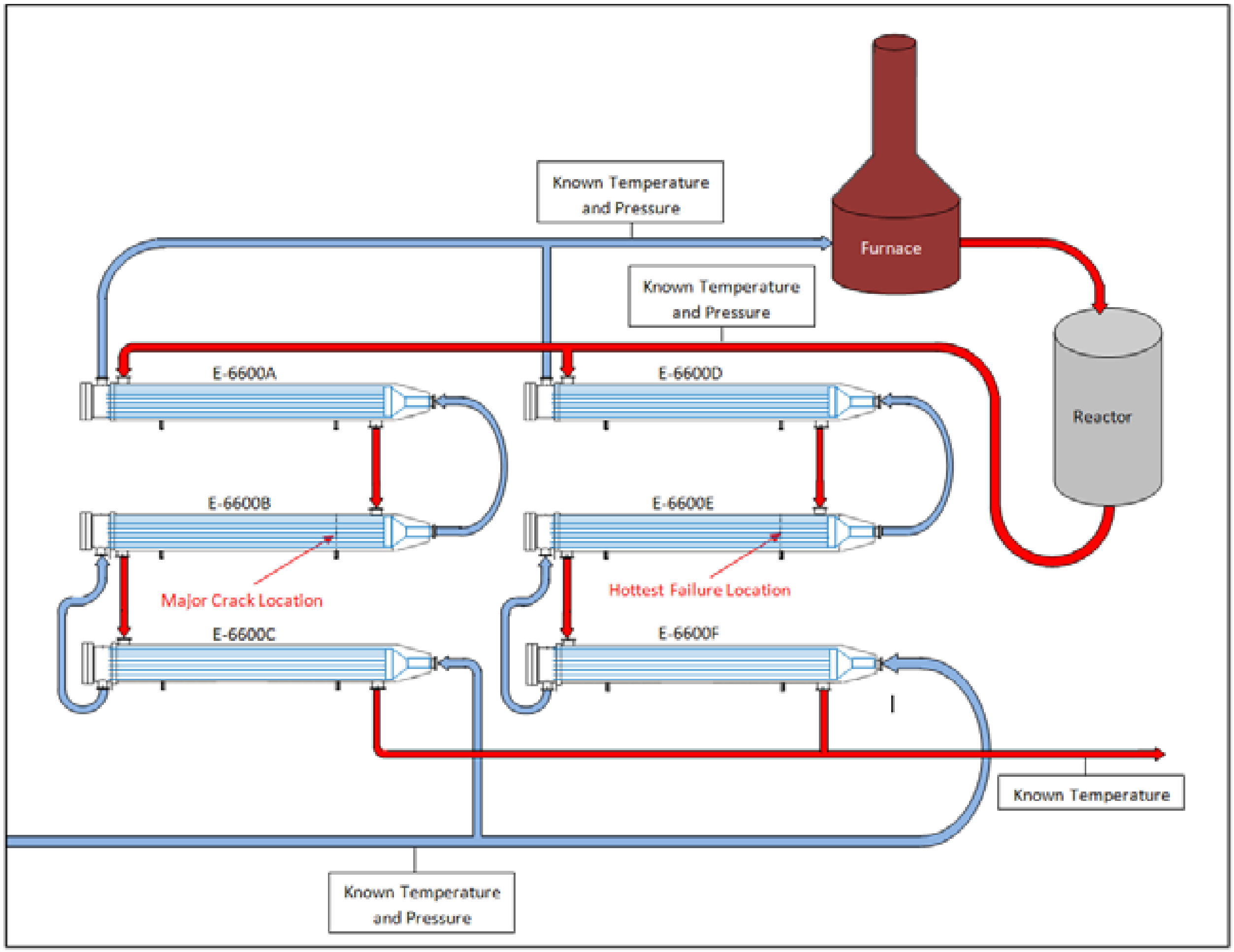


Figure 43. NHT Heat Exchanger Configuration with Known Process Conditions Indicated

C.2 Modeling Approach

The computer program *Aspen Exchanger Design and Rating* is a tool that allows the development of a rigorous mechanical model of a heat exchanger based on the actual mechanical details. The heat exchanger design data entered into the program included specific construction details such as the heat exchanger type; the shell dimensions; the number, diameter, and length of tubes; the baffle configuration; and the material of construction.

The model developed using *Aspen Exchanger Design and Rating* was then used as an input to another Aspen computer program, *Aspen HYSYS*®. This software provides the capability to combine the heat exchanger mechanical model into a process model of an entire section of a refinery process, such as the NHT heat exchangers. Model inputs include data from the process, such as flow rates, temperature, pressures, process compositions and process physical properties. The CSB used the *Aspen HYSYS*®

model to simulate past performance of the NHT feed/effluent heat exchangers. Historical DCS data and composition data were input into the model to reflect actual operating conditions.

C.3 Fouling Distribution

A key focus of the CSB modeling effort was to estimate operating conditions of the heat exchangers when they were fouled. Fouling results in higher shell-side temperatures, and the potential for HTHA would have been most severe during higher-temperature periods. The model includes input parameters, called *fouling resistance*, for estimating heat exchanger fouling. The CSB calibrated these fouling parameters by matching actual operating data under fouled conditions. Next, the CSB apportioned the level of fouling among the various heat exchangers. In both the model results and the data for actual heat exchangers in the unit, distribution of fouling among the A/D, B/E, and C/F heat exchanger tubes greatly affects the process conditions within the B and E heat exchangers.

Because actual fouling distribution throughout the heat exchangers was not known, the CSB performed a sensitivity analysis of possible fouling distributions on the tube-side of the heat exchangers to approximate conditions that existed based on the available qualitative visual observations. For example, these observations described a uniformly light scale on the shell-side of each heat exchanger. As a result, a constant, light fouling resistance was incorporated in the model to represent this light scale. Qualitative observations also described fouling inside the tubes, with the extent of observed fouling increasing from C/F to B/E and then to A/D. The tube-side fouling distributions analyzed for the sensitivity analysis are shown in Figure 44. Distribution 2 was selected for the model because it best matched the overall documented observations of heat exchanger fouling.

	Percent fouling resistance in A/D exchangers	Percent fouling resistance in B/E exchangers	Percent fouling resistance in C/F exchangers
Distribution 1	60%	30%	10%
Distribution 2	55%	32.5%	12.5%
Distribution 3	50%	35%	15%

Figure 44. NHT Heat Exchanger Fouling Distributions Analyzed

A schematic of how these distributions may appear visually is shown in Figure 45.

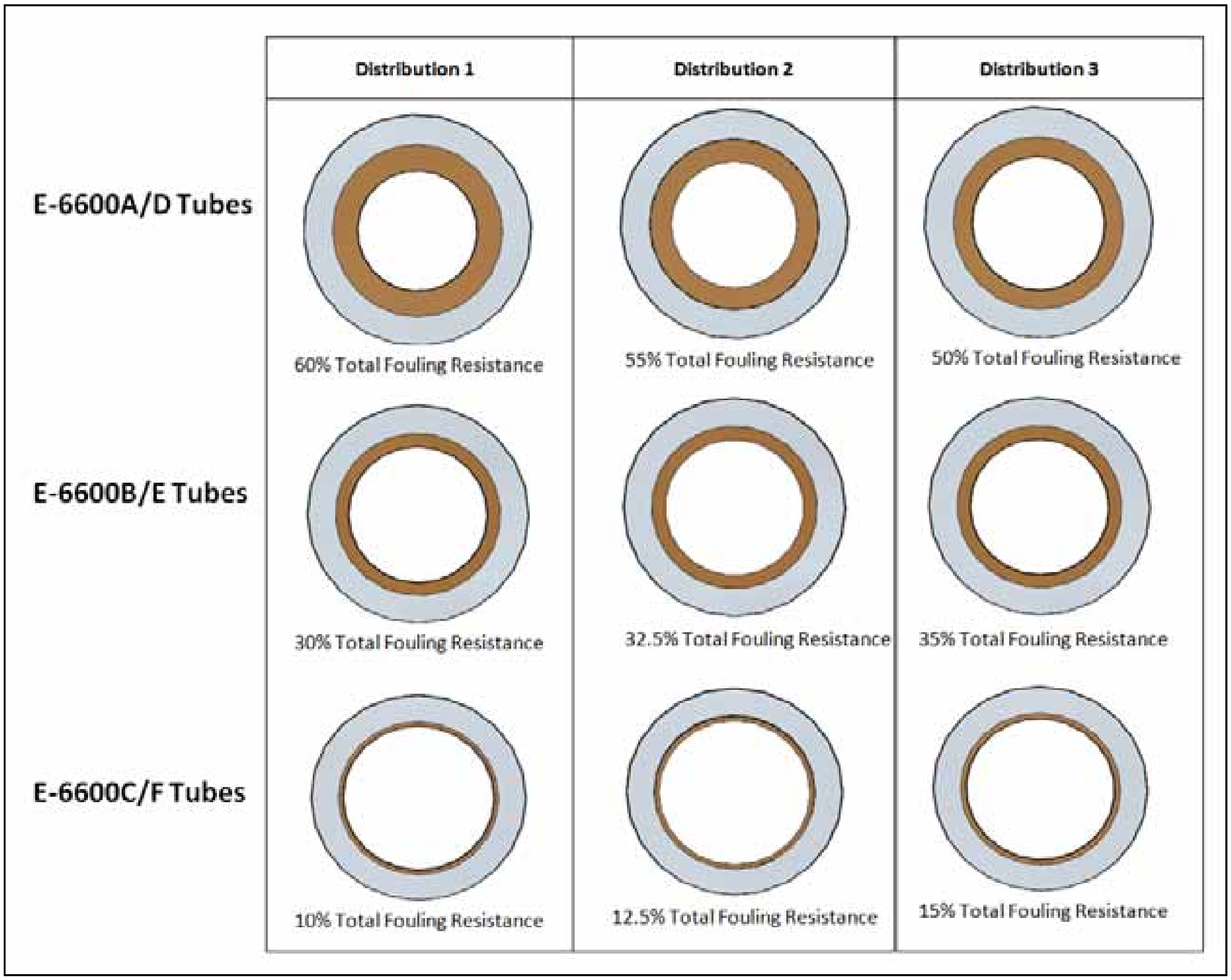


Figure 45. Visualization of Possible Tube-Side Fouling Distributions

C.4 DCS Data and Composition Data Availability

The necessary DCS and fluid composition data needed to model the heat exchangers were only available between 2007 and 2010.[278] As a result, all modeled values represent estimates of process conditions causing HTHA from 2007 through 2010. HTHA degradation of the B and E heat exchangers from HTHA during this time period is likely because the heat exchangers had experienced higher temperature and greater mechanical stress in the 2007 to 20010 time period than on the night of the incident.[279]

[278] The Tesoro Anacortes, Washington refinery first installed its DCS system in 2002. However, not all variables necessary for process simulation of the NHT heat exchangers were measured until 2007.

[279] On February 23, 2008, the D/E/F heat exchanger tube outlet temperature increased by 100 °F over a 10 minute period before being brought down for a cleaning operation, reaching a maximum temperature of 681 °F. On August 22, 2009, during a startup of the D/E/F heat exchanger bank following a cleaning operation, the D/E/F exchanger bank tube outlet temperature increased by 100 °F over a four minute period, reaching a maximum temperature of approximately 641 °F during the startup. Other high-stress events during exchanger

The CSB modeled 10 days of operation during this 2007 to 2010 time period. Two of the periods modeled were characterized by clean heat exchanger conditions; during three of the periods modeled, middle-of-run operation conditions existed; and five of the periods modeled were characterized by fouled heat exchanger conditions near the end of a run.

C.5 Calibration of Model with Actual Process Data

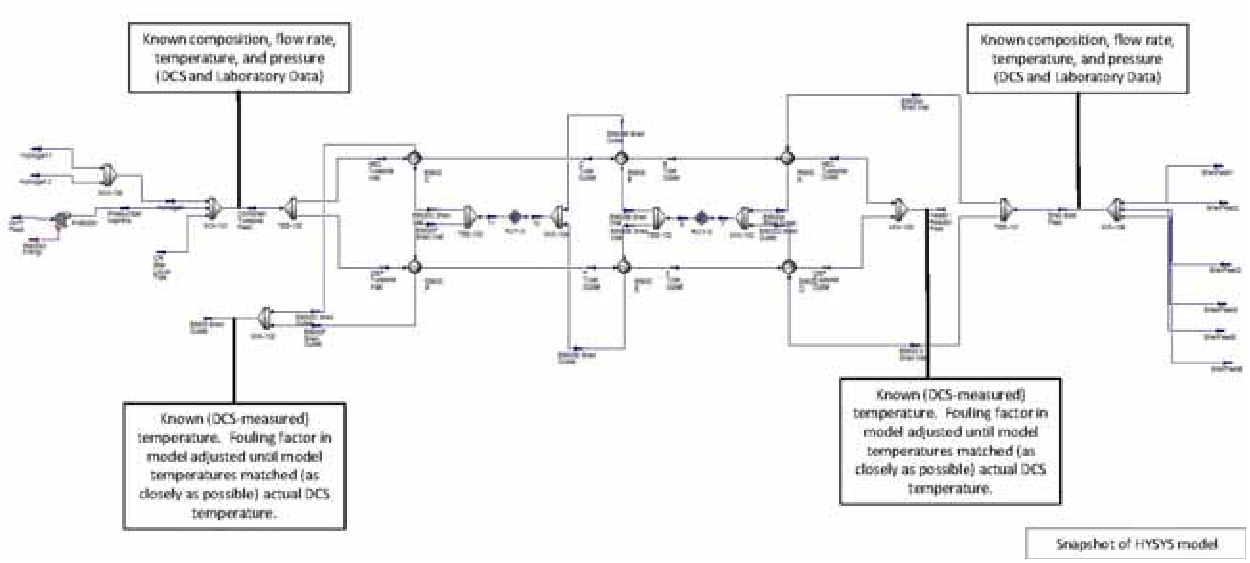


Figure 46. Calibration of HYSYS Model with Actual Process Data. The fouling resistances (fouling factors), maintaining the 55%, 32.5%, 12.5% split, were adjusted until the tube-side and shell-side outlet model temperature results closely matched actual DCS-measured temperatures.

Shown in Figure 46, actual composition data, flow rates, temperatures, and pressures were available for the process fluid entering both the tube-side and shell-side of the heat exchanger banks. Measured temperature values were available for the fluid exiting both the tube-side and shell-side of the heat exchanger banks. The fouling resistances (fouling factors) were adjusted in the model, maintaining the 55%, 32.5%, and 12.5% split until the model's tube and shell outlet temperatures closely matched the actual, measured process temperatures. This method resulted in an average of 4% error between the model's outlet temperatures and the actual, measured tube and shell outlet temperatures. The temperature profile of the B and E heat exchangers was then analyzed to determine temperatures and hydrogen partial pressures along the length of the heat exchangers.

C.6 Modeling Results

startup are also shown in Appendix B. The E heat exchanger did not rupture as a result of the temperature and mechanical stresses of these startups.

The resulting plot of modeled operating conditions of the B and E heat exchangers is shown in Figure 47, which illustrates the full operating region of the B and E heat exchangers, the operating conditions at the rupture location, and the operating conditions at the CS2 seam (the coldest location where signs of HTHA were evident in the E heat exchanger). All graphed regions use the Distribution 2 fouling allocation.

The estimated operating regions for the stainless steel clad portion of the B and E heat exchangers extended above the carbon steel Nelson curve. At the rupture location, the estimated operating conditions are just below the carbon steel Nelson curve. Model results for the coldest area of the E heat exchanger where signs of HTHA were evident (the CS2 weld between Cans 1 and 2) indicate HTHA damage in equipment that operated between 70 °F to 120 °F below the carbon steel Nelson curve. All graphed regions use the Distribution 2 fouling allocation. The model results illustrate the imprecision of the carbon steel Nelson curve.

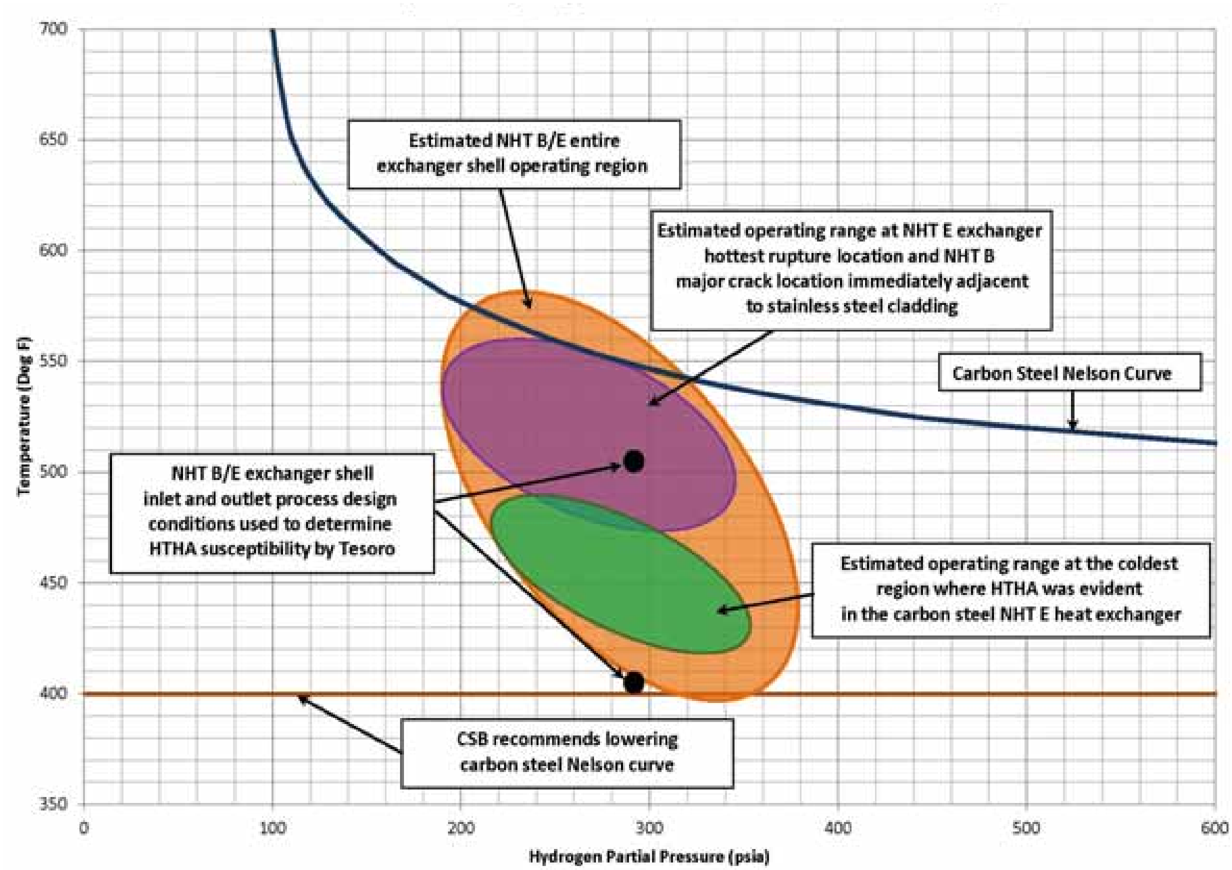


Figure 47. Estimated Operating Conditions of the B and E Heat Exchangers

Appendix D Evaluation of Current Tesoro Programs to Identify and Control Damage Mechanism Hazards

In developing a recommendation for Tesoro to address several of the findings in Section 1.2.2, the CSB evaluated current Tesoro standards for conducting DMHRs, PHAs, and Integrity Operating Window (IOW). In addition to the incident-specific analyses described in the report, this evaluation provides the necessary detail and support for recommendation 2010-08-I-WA-R14.

DMHRs evaluate a subset of hazards within the scope of a PHA.[280] Because of the specialized focus and expertise required to properly assess damage mechanism hazards, Tesoro has developed a program to evaluate these hazards outside of the PHA process, using external hired experts. The PHA team is then required to review this information and incorporate it into the applicable PHA.

The Tesoro PHA standard includes a requirement for the PHA team to review the most recent DMHR. This requirement establishes a link between the DMHR and the PHA, but it is not currently sufficient. To provide a better connection between the DMHR and the PHA, the DMHR team should be required to review the most recent PHA and validate the damage mechanism hazards and the safeguards identified to control these hazards. The PHA standard does not include a link between the IOW and the PHA. The PHA team should be required to review IOWs and validate the damage mechanism hazards and the safeguards identified to control these hazards.

IOWs are intended to address operating limits to prevent unexpected degradation of equipment. Like DMHRs, IOW reviews evaluate a subset of hazards within the scope of a PHA. The IOW standard addresses 51 degradation mechanisms that Tesoro has determined should be evaluated outside of the PHA process. The results of the IOW review must be integrated into the PHA; however, the PHA standard does not currently contain language to ensure that this requirement is completed. Although IOWs provide a mechanism to qualitatively rank degradation hazard risks, there is no provision to evaluate the effectiveness of safeguards, consider the hierarchy of controls, or evaluate opportunities for inherently safer design to the greatest extent feasible. The results of the DMHR are reviewed and incorporated into the development of IOWs. Although degradation hazards are evaluated in the IOW review process, IOWs are only revalidated every 10 years, twice the 5-year revalidation frequency allowed by the PSM regulations.[281] The IOW does evaluate incidents, but there is no provision to evaluate or consider industry-wide incidents. The IOW process does consider both routine and nonroutine operations.

The Tesoro PHA standard includes guidance to provide direction to the PHA team on its responsibilities. This guidance suggests that the PHA team is responsible only for a review of the completed critical

[280] The state of Washington PSM rule requires that the PHA shall address the hazards of the process. See: http://www.lni.wa.gov/wisha/rules/hazardouschemicals/#WAC296-67-017 (accessed December 29, 2013). These regulations do not specifically require a DMHR.

[281] WAC 296-67-017(6), "Process hazard analysis," requires the PHA to be updated and revalidated at least every 5 years. See: http://www.lni.wa.gov/wisha/rules/hazardouschemicals/#WAC296-67-001 (accessed January 11, 2014).

process data sheet that the corrosion expert produces as part of the DMHR. A specific requirement is never explicitly made for the PHA team to identify damage mechanism hazards, evaluate existing safeguards, and propose new safeguards to control these hazards.

None of the Tesoro PHA, DMHR, or IOW standards ensure that effective safeguards are identified and evaluated to control damage mechanism hazards. Such a review is implied by the overarching requirements in the Tesoro PHA standard. However, the language used in the standard could functionally reduce the responsibility of the PHA team to a mere review of the critical process data sheet developed by the corrosion expert as part of the DMHR. No formal evaluation of safeguards is ever described as a requirement for damage mechanism hazards or for the establishment of IOWs.

To improve the DMHR, this team should conduct a review of the relevant PHA hazards that address damage mechanisms. For these hazards, the DMHR should validate consequence, frequency, and proposed safeguards to control damage mechanism hazards. The DMHR should also evaluate alternatives that consider the hierarchy of controls and opportunities for inherently safer design to the greatest extent feasible.

The final deliverable from a Tesoro DMHR is a written report that the corrosion expert prepares. Because the DMHR team does not review and approve this final report, it does not meet OSHA PSM requirements for a PHA. There is an OSHA interpretation letter from October 31, 1996, that essentially states that a "team"[282] must perform the hazard analysis. OSHA's intent appears to be that the analysis and recommendations developed remains a team product. As written, the Tesoro DMHR results in a team analysis but with a report developed by an individual.

Under the Tesoro DMHR standard, the corrosion expert is required to assemble a critical process data spreadsheet. This spreadsheet is submitted to someone who has process expertise to provide the required process operating data. However, there is no guidance on how these data should be obtained or assurance that the data are appropriate to properly evaluate a given damage mechanism. In light of the April 2010 incident at the Anacortes refinery, for each identified damage mechanism, there should be a clear understanding of what process data are required as well as a provision to ensure that design operating data are not used in lieu of obtaining actual measurements or performing a technical evaluation such as a process simulation to estimate needed process data. The DMHR team should review the operating data and collection techniques to verify an accurate understanding of how the data were obtained and what they represent, and it should appropriately consider routine and nonroutine operations as well as the full range of operating conditions.

Before the April 2010 incident, in 2003, API identified materials that are not susceptible or are highly resistant to HTHA damage.[283] Neither Shell Oil nor Tesoro damage mechanism reviews considered these materials as inherently safer controls for HTHA hazards. The Tesoro DMHR and IOW processes do not

[282] See: https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=INTERPRETATIONS&p_id=22289 (accessed December 29, 2013).

[283] API RP 571. "Damage Mechanisms Affecting Fixed Equipment in the Refining Industry." Pages 5–56, 2003.

ensure that gaps between current industry best practices and existing Tesoro practices are identified, evaluated, and considered when creating recommendations to reduce risk of damage mechanism hazards.

Tesoro should maintain an incident database on damage mechanism incidents, both for Tesoro and industry-wide. The DMHR and IOW teams should conduct a review of these incidents that should be included in the DMHR and IOW reports.[284]

As a result of separating the evaluation of damage mechanisms from the formal PHA process, potential gaps exist when the PHA team reviews MOCs and incident reports during the PHA process.[285] In addition to a review by the PHA team, MOCs relevant to potential damage mechanisms should be reviewed by the IOW team to fully evaluate the impact of proposed and planned changes within the refinery on relevant damage mechanism hazards. The IOW standard requires integration of IOWs into the MOC process, but the MOC standard currently has no provision to consider IOWs.

The Tesoro DMHR is one component of the Tesoro RBI program, which determines potential consequences for hazards such as equipment failure from damage mechanisms. Tesoro currently determines the consequences of damage mechanism hazards as a separate activity from the PHA, and there is no verification that the consequences determined by the DMHR are consistent with the PHA. To improve the Tesoro PHA process, PHA teams should review and validate the relevant consequence of hazards identified by the RBI program.[286]

Tesoro requires a corrosion expert to lead the DMHR process. However, the qualifications of the corrosion expert are not defined. Minimum qualifications should be clearly defined, and additional personnel should be added to the team if the identified corrosion expert does not meet all of the minimum qualifications.

The Tesoro requirement for DMHR meeting participants is confusing and should be clarified. The refinery corrosion and materials engineer is listed as a required participant, but then the DMHR document uses the language "if present." It is not clear why or under what conditions Tesoro would conduct a DMHR without the participation and expertise of the refinery corrosion and materials professional.

---

[284] The identification of any previous incident that had a likely potential for catastrophic consequences in the workplace is a requirement of the State of Washington PSM rule. See: http://www.lni.wa.gov/wisha/rules/hazardouschemicals/#WAC296-67-017 (accessed December 29, 2013).

[285] The Tesoro PHA standard requires PHA revalidations to address "Changes since the last PHA(s)—Management of Change (MOC)." The Tesoro PHA standard also requires the PHA to evaluate previous incidents. The standard requirements mirror the language of the State of Washington PSM rule, "The identification of any previous incident which had a likely potential for catastrophic consequences in the workplace."

[286] For these hazards, the PHA team should ensure that there are effective safeguards to control damage mechanism hazards. The PHA team should also evaluate alternatives that consider the hierarchy of controls and opportunities for inherently safer design to the greatest extent feasible.

Appendix E Inspection Techniques

The most basic nondestructive examination (NDE) technique is simply a visual examination that typically evaluates for physical damage such as dents or cracks, discoloration, or the presence of foreign material (such as process fouling or corrosion products similar to rust). However, significant damage is not always visible to the naked eye. Much like a doctor uses of X-rays or an MRI, or a CAT scan, the inspector uses more sophisticated tools and techniques to determine the condition of the refinery equipment. Typical NDE techniques include the following:

- **Ultrasonic Technique (UT)—**is the primary NDE technique for determining the extent of general corrosion attack. UT uses high frequency sound waves that are transmitted into a material and travel in a straight line and at a constant speed until they encounter a surface. The surface interface causes some of the wave energy to be reflected, and the rest of it is transmitted. The quantity of reflected versus transmitted energy is detected. Expert examination of the data provides information such as the presence of discontinuities and the thickness of the material or coating.[287]

- **Radiographic Technique (RT)—**also referred to as X-ray, is commonly performed using two different sources of radiation, X-ray and gamma ray. Advantages include a minimum surface preparation requirement and sensitivity to changes in thickness, corrosion, voids, cracks, and material density. The disadvantages are safety precautions required for the safe use of radiation, and access constraints in the field.[288]

- **Dye Penetrant Inspection (DPI)—**also called Liquid Penetrant Inspection (LPI) or Penetrant Technique (PT), is a widely applied and low-cost inspection method used to locate surface-breaking defects in all non-porous materials (such as metals, plastics, or ceramics). DPI is used to detect cracks, surface porosity, lack of penetration in welds and defects resulting from in-service conditions (for example fatigue cracks of components or welds) in castings, forgings, and welding surface defects.[289]

- **Magnetic Particle (MT)—**is used for finding surface and near surface defects in ferromagnetic material and is a versatile inspection method for field and shop applications. Magnetic particle testing works by magnetizing a ferromagnetic specimen using a magnet or special magnetizing equipment. If the specimen has discontinuity, the magnetic field flowing through the specimen is interrupted and leakage field occurs. Finely milled iron particles coated with a dye pigment are applied to the specimen. These are attracted to leakage fields and cluster to form an indication directly over the discontinuity. The indication is visually detected under proper lighting

[287] *See:* http://www.mistrasgroup.com/services/traditionalndt/ut.aspx (accessed August 1, 2013).

[288] *See:* http://www.mistrasgroup.com/services/traditionalndt/rt.aspx (accessed August 1, 2013).

[289] *See:* http://www.eceglobal.com/services/inspection-approvals/non-destructive-examination-nde/penetrant-testing-pt/, (accessed June 3, 2013).

conditions. Wet Fluorescent Magnetic Particles (WFMPT) is sometimes applied to increase sensitivity for locating very small defects.[290]

- **Ultrasonic Shear Wave—**also called Angled Beam Ultrasonic Technique, can be used to inspect pipe, critical welds in pressure vessels and plate weldments, and can be used to inspect cracks for depth, size, length and orientation. This is a common technique used for weld inspection, which provides a sensitive, fast and cost effective method to detect, locate, and validate a range of large to small defects and deterioration.[291]

- **Phased Array Ultrasonic Technology (PAUT)—**has the capability of creating multiple beam angles and focal points with the use of a multi-element ultrasonic transducer, and providing full volumetric sectorial scans (S-Scans), a feature unique to this technology. S-Scans are real-time side view images generated from a single inspection point; in essence, it depicts an internal view of the component being inspected. With this technology, weld flaw and crack detection and sizing can be achieved at a high rate of speed, many times faster than conventional shear wave inspection can achieve.[292]

- **Advanced Ultrasonic Backscatter Technique (AUBT)—**developed by Shell Oil in the early 1990s, is currently the best NDE method for detecting and quantifying damage from HTHA. The technique uses conventional UT probes and a digital oscilloscope to provide both an A-Scan display and frequency analysis.[293] AUBT is a sophisticated technique and requires a very high level of expertise.[294] There is no general certification of inspector competence in the application of HTHA detection techniques.

- **Velocity Ratio:** HTHA reduces the velocity of both shear and longitudinal waves. When a material is attacked by HTHA, the velocity reduction is slightly more with longitudinal than with shear waves. This in effect increases the ratio of shear wave to longitudinal wave velocities or the ratio of the transit times. This ratio of transit times can be used as an indicator of HTHA. Tests have shown that the velocity-ratio approach is only effective at high levels of HTHA and is limited to the base metal.[295]

---

[290] *See:* http://www.mistrasgroup.com/services/magnetic-particle-testing.aspx, (accessed June 3, 2013).

[291] *See:* http://techcorr.com/services/Inspection-and-Testing/Ultrasonic-Shear-Wave.cfm (accessed July 16, 2013).

[292] *See:* http://www.autsolutions.net/Phased_array.html (accessed July 16, 2013).

[293] *See:* http://www.spi-matrix.com/advanced-ultrasonic-backscatter.php (accessed July 16, 2013).

[294] See: http://www.nde.com/hydrogen.htm (accessed June 13, 2013).

[295] *See*: http://www.ndt-ed.org/EducationResources/CommunityCollege/Ultrasonics/Physics/modeconversion.htm (accessed January 13, 2013).

Appendix F Draft Chevron Regulatory Report

The draft Chevron Regulatory Report can be accessed at http://www.csb.gov/chevron-refinery-fire/.

Appendix G Spectrum Inspection Reports

The Spectrum Inspection Reports can be accessed at http://www.csb.gov/tesoro-refinery-fatal-explosion-and-fire/.

Appendix H Beta Laboratory Reports

The Beta Laboratory Reports can be found at http://www.csb.gov/tesoro-refinery-fatal-explosion-and-fire/.

Appendix I Metallurgical Review

The metallurgical report can be accessed at http://www.csb.gov/tesoro-refinery-fatal-explosion-and-fire/.

Appendix J Additional HTHA Evaluation Report

This report can be accessed at http://www.csb.gov/tesoro-refinery-fatal-explosion-and-fire/.

CSB Investigation Reports are formal, detailed reports on significant chemical accidents and include key findings, root causes, and safety recommendations. CSB Hazard Investigations are broader studies of significant chemical hazards. CSB Safety Bulletins are short, general-interest publications that provide new or noteworthy information on preventing chemical accidents. CSB Case Studies are short reports on specific accidents and include a discussion of relevant prevention practices. All reports may contain include safety recommendations when appropriate. CSB Investigation Digests are plain-language summaries of Investigation Reports.

The U.S. Chemical Safety and Hazard Investigation Board (CSB) is an independent Federal agency whose mission is to ensure the safety of workers, the public, and the environment by investigating and preventing chemical incidents. The CSB is a scientific investigative organization; it is not an enforcement or regulatory body. Established by the Clean Air Act Amendments of 1990, the CSB is responsible for determining the root and contributing causes of accidents, issuing safety recommendations, studying chemical safety issues, and evaluating the effectiveness of other government agencies involved in chemical safety.

No part of the conclusions, findings, or recommendations of the CSB relating to any chemical accident may be admitted as evidence or used in any action or suit for damages. See 42 U.S.C. § 7412(r)(6)(G). The CSB makes public its actions and decisions through investigation reports, summary reports, safety bulletins, safety recommendations, case studies, incident digests, special technical publications, and statistical reviews. More information about the CSB is available at www.csb.gov.

CSB publications can be downloaded at www.csb.gov or obtained by contacting:
U.S. Chemical Safety and Hazard Investigation Board
Office of Congressional, Public, and Board Affairs
2175 K Street NW, Suite 400
Washington, DC 20037-1848
(202) 261-7600