Assessing Survivability Risk Due to Significant Events in Fossil Generation Facilities

2014 TECHNICAL REPORT

Assessing Survivability Risk Due to Significant Events in Fossil Generation Facilities

EPRI Project Manager
N. Espinoza

ELECTRIC POWER RESEARCH INSTITUTE

3420 Hillview Avenue
Palo Alto, CA 94304-1338
USA

PO Box 10412
Palo Alto, CA 94303-0813
USA

800.313.3774
650.855.2121

askepri@epri.com

www.epri.com

3002003205
Final Report, December 2014

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THIS DOCUMENT WAS PREPARED BY THE ORGANIZATIONS NAMED BELOW AS AN ACCOUNT OF WORK SPONSORED OR COSPONSORED BY THE ELECTRIC POWER RESEARCH INSTITUTE, INC. (EPRI). NEITHER EPRI, ANY MEMBER OF EPRI, ANY COSPONSOR, THE ORGANIZATIONS BELOW, NOR ANY PERSON ACTING ON BEHALF OF ANY OF THEM:

(A) MAKES ANY WARRANTY OR REPRESENTATION WHATSOEVER, EXPRESS OR IMPLIED, (I) WITH RESPECT TO THE USE OF ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT, INCLUDING MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR (II) THAT SUCH USE DOES NOT INFRINGE ON OR INTERFERE WITH PRIVATELY OWNED RIGHTS, INCLUDING ANY PARTY'S INTELLECTUAL PROPERTY, OR (III) THAT THIS DOCUMENT IS SUITABLE TO ANY PARTICULAR USER'S CIRCUMSTANCE; OR

(B) ASSUMES RESPONSIBILITY FOR ANY DAMAGES OR OTHER LIABILITY WHATSOEVER (INCLUDING ANY CONSEQUENTIAL DAMAGES, EVEN IF EPRI OR ANY EPRI REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) RESULTING FROM YOUR SELECTION OR USE OF THIS DOCUMENT OR ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT.

REFERENCE HEREIN TO ANY SPECIFIC COMMERCIAL PRODUCT, PROCESS, OR SERVICE BY ITS TRADE NAME, TRADEMARK, MANUFACTURER, OR OTHERWISE, DOES NOT NECESSARILY CONSTITUTE OR IMPLY ITS ENDORSEMENT, RECOMMENDATION, OR FAVORING BY EPRI.

THE FOLLOWING ORGANIZATIONS, UNDER CONTRACT TO EPRI, PREPARED THIS REPORT:

Southern Engineering Services, Inc.

Baker Engineering and Risk Consultants, Inc.

NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

Electric Power Research Institute, EPRI, and TOGETHER…SHAPING THE FUTURE OF ELECTRICITY are registered service marks of the Electric Power Research Institute, Inc.

Copyright © 2014 Electric Power Research Institute, Inc. All rights reserved.

Acknowledgments

The following organizations, under contract to the Electric Power Research Institute (EPRI), prepared this report:

Southern Engineering Services, Inc.
331 Allendale Drive
Canton, GA 30115

Principal Investigators
Bradley Geddes
Bruce Geddes

Baker Engineering and Risk Consultants, Inc.
3330 Oakwell Court, Suite 100
San Antonio, TX 87218

Principal Investigator
Philip Parsons

This report describes research sponsored by EPRI.

The EPRI project team acknowledges the following individuals who were particularly helpful in providing input on the project:

Wayne Crawford	Accuro
Ray Chambers	Accuro
Tom Rawe	Accuro
Tom Guthrie	Accuro
Tony Wanat	CH2M Hill
Bob Hall	Duke Energy (Retired)
Ray Weidler	Duke Energy (Retired)
Joseph Flick	New York Power Authority
Bohdan Dackow	New York Power Authority
Lindsey McCloy	New York Power Authority

Michael Leonard	New York Power Authority
Steve Logan	Southern Company
Ron Raines	Southern Company
John Sorge	Southern Company
Matt Wallace	Ameren
Joe Bradley	Ameren
Mark Little	EPRI

This publication is a corporate document that should be cited in the literature in the following manner:

Assessing Survivability Risk Due to Significant Events in Fossil Generation Facilities.
EPRI, Palo Alto, CA: 2014.
3002003205.

Product Description

This report describes the results of research on survivability of significant events in fossil generation facilities. It briefly describes some of the hazards that may be found in a fossil generation facility, how they can lead to a significant event, and the potential consequences of significant events. This report includes summary lists of some of the design features and administrative controls that could be used to prevent or reduce the likelihood of certain types of significant events or mitigate their consequences.

Background

Potential hazards exist in fossil generation facilities, events do happen, and events have consequences that can challenge survivability. The good news is that, in many cases, existing or proposed design features and/or administrative controls can prevent or reduce the likelihood of a hazard leading to an event, as well as design features and/or administrative controls that can help mitigate the consequences of an event. Thus, means are available for both preventing and mitigating events, and if they are applied and maintained effectively, survivability can be reasonably ensured. Furthermore, proven risk assessment methods can be used to help identify and select the appropriate means for improving survivability, if necessary.

Objectives

The research project that produced this report started out with the objective of main control room (MCR) hardening and survivability, with the idea that significant events do occur, they can affect MCR personnel, and MCR personnel should be protected. However, as the research unfolded, Electric Power Research Institute (EPRI) members reported that they were just as concerned about protecting people in other inhabited spaces. In addition, experts on the topics of hazard analysis and risk assessment reported that it is helpful to consider means for *preventing* significant events, as well as means for *mitigating* their consequences.

Ultimately, this research centered on the objective of characterizing and assessing survivability risk due to significant events in fossil generation facilities.

Approach

This report describes the results of interviews with EPRI members, a literature search, and input by domain experts in the fossil generation, petroleum refining, and chemical industries.

Four specific events—hydrogen explosions, steam turbine wrecks, coal dust explosions, and toxic releases of anhydrous ammonia—were selected (based on input from project participants) for describing hazard characteristics, event characteristics, event consequences, the types of measures that can be applied to prevent or mitigate events, and industry references that provide detailed guidance.

Results

During the development of this report, it was determined that, in general, design criteria for hardening structures in the fossil generation industry are lacking. Accordingly, this report presents a methodology that may be used to systematically approach the concepts of hazards, events, and consequences with an emphasis on typical design features and administrative controls for preventing these events or mitigating their consequences. Although four specific events were selected to illustrate these concepts, this approach can be extended to other types of events as well.

Some additional information was provided by experts in the petroleum refining and chemical industries who are concerned about some of the same hazards, events, and survivability risks faced by owner/operators of fossil generation facilities. This cross-sector input includes a description of qualitative and quantitative risk assessment methods and how they can be extended to the fossil generation industry. Additional research is proposed for identifying and ranking hazards, performing a demonstration project at an operating facility, or adding additional types of events to this report.

Applications, Value, and Use

The intended audience for this report is owner/operators of fossil generation facilities. Its value is in providing a model for characterizing significant events where survivability is a question. This report can be used to systematically consider potential hazards, potential events, and potential consequences within a specific facility, and some of the means for preventing or mitigating significant events.

Keywords

Administrative controls
Design features
Hazards
Risk assessment
Significant events
Survivability

Table of Contents

List of Figures

List of Tables

Section 1: Introduction

1.1 Background

As the fossil power industry has evolved from hard switches and panel boards, to digital control systems and computer interfaces, the need to evaluate the layout, functionality and safety of the typical fossil power plant control room has surfaced. Many times our operating personnel are located within the power block, directing plan operations from a centralized control center or other inhabited spaces. However, with extreme weather events, neighboring industrial facility accidents and the potential for internal equipment malfunctions, further considerations can be given to future designs as well as retrofitting existing designs to ensure the functionality of the inhabited spaces and the safety of the operating personnel.

1.2 Objectives

The original intent of this study was to look at considerations that should be given to control room hardening and survivability for fossil power stations. This project sought to evaluate the following topics for control room design and hardening: location, size, physical security, human factor engineering, ergonomics, regulatory requirements, safety requirements and survivability during internal and/or external events.

However, as the research unfolded, EPRI members reported that they were just as concerned about protecting people in other inhabited spaces. In addition, experts on the topics of hazard analysis and risk assessment reported that it is helpful to consider means for *preventing* significant events as well as means for *mitigating* their consequences.

Ultimately, this research centered on the objective of characterizing and assessing survivability risk due to significant events in fossil generation facilities.

1.3 Project Scope

1.3.1 Investigate Current Design and Regulatory Requirements

Investigate current design requirements and regulatory requirements for control room design and hardening based on most likely hazards and consequences. This includes discussions with EPRI members concerning any current design and regulatory requirements that they are implementing for control room survivability and hardening, including what hazards are being considered in the design criteria.

1.3.2 Benchmark Similar and Relevant Industries

Benchmark similar and relevant industries to determine what lessons learned can be applied to the fossil power industry. While this review will focus on fossil power plant control room matters, experience will be drawn from control rooms across the board in fossil, renewables, non-power control rooms (for example, chemical, oil refining, mining, and manufacturing), and nuclear facilities to understand issues and lessons learned. This will include consideration of the experiences of other off-site facilities.

1.4 Hazard Analysis as a Basis for Survivability

This EPRI report summarizes the results from an investigation into industry requirements and best practices for control room hardening and survivability. Research results showed that the fossil generation industry does not have any guidance, standards, or best practices specific to control room hardening and survivability design. Nor are there any studies on evaluating potential hazards and consequences versus risk that affect control room design. There is some existing guidance and standards that are related to control room ergonomics, human factors, fire mitigation, and safety.

The investigation evolved from control room hardening design requirements to understanding hazards, events, and consequences that can impact survivability of inhabited spaces in general. Hazards exist that can result in an event. The likelihood and potential consequences of an event should be analyzed based on local design and conditions at a specific plant.

The likelihood of an event can be determined through several possible methods. Consequences can be evaluated qualitatively or quantitatively via event modeling. Consequence modeling results can then be used to determine what impact, if any, on habitable spaces might result from an event. The overall survivability risk of an event is a function of the likelihood of a hazard leading to the event, and the consequences of the event. Understanding the survivability risk allows an owner/operator to make decisions regarding whether and how to prevent and/or mitigate an event.

An important result of the research is that all occupied habitable spaces should be considered and analyzed in addition to the control room. Offices, break rooms, meeting rooms, and so on, are sometimes in the same building as the control room, or are in other buildings within the plant. In order to develop hardening and design requirements, the vulnerability to all onsite personnel of a hazardous event need to be determined.

A list of hazards and related events was identified that can impact survivability (see Table 3-1). The list is based on input from the interviews and literature, is not all inclusive, and is not based on industry data and analysis. A sub set of four hazardous events were selected for high level evaluation, in no particular order, using the "Bow Tie" method to illustrate a method for characterizing hazards and potential events. The four events are:

1. Hydrogen Explosions
2. Steam Turbine Wrecks
3. Coal Dust Explosions
4. Toxic Releases of Anhydrous Ammonia

This report uses the Bow Tie method to summarize the hazardous event and explore possible approaches for prevention and mitigation.

Baker Engineering and Risk Consultants, Inc. (BakerRisk) were approached to provide relevant input, in particular from the refining and petrochemical industries on related subject matter. BakerRisk is an internationally recognized firm dedicated to help predict, prevent, and mitigate hazards from explosions, fires, and toxic releases. BakerRisk specializes in process safety and risk management services to companies in the petroleum and chemical industries, as well as engineering and testing services for government agencies and private companies involved with hazardous materials.

The research into the petroleum refining and chemical industries shows that they systematically analyze consequences and likelihood of hazardous events for habitable space design, including retrofits of existing habitable spaces. Some of the guidance, standards, approaches, and methods used in the petroleum refining and chemical industries are described in Section 5. In addition, a proposed approach for how these methods could be applied to the fossil generation industry is included in Appendix B.

Note: The scope of the project did not allow for detailed research on potential hazards, hazard analysis, and consequence/likelihood analysis versus cost that would affect control room design. Nor does the scope address specific control room design details. There are existing approaches and models to perform these type of detailed analysis that EPRI may consider applying in future projects.

1.5 Existing Design Features and Administrative Controls

Owners, consultants, vendors, EPC contractors, industry organizations, and regulators have identified similar hazards that are listed in this report, across a range of industries, and address them in varying ways and depth in existing facility design features and administrative programs and procedures. To date, prevention and mitigation of identified hazards have been focused on administrative procedures and equipment/system mitigation including equipment/system design and the addition of equipment/systems for safety purposes, and do not typically address design requirements for inhabited spaces.

Existing plant design and administrative programs and procedures address many of the potential hazards. When analyzing a hazard it is important to consider, and take credit for, existing plant design and administrative programs and procedures.

The number of standards and guidelines that are relevant are too numerous to list. Section 4 provides four examples of a high level application of the bow tie model. These examples list some applicable standards and guidelines for the particular hazard.

Section 2: Definitions and Acronyms

2.1 Definitions

Blast Wave: A pressure pulse following a shock wave. It is due to velocity imparted by the shock wave to the medium particles [21].

Deflagration: A flame moving through a flammable mixture in the form of a subsonic wave (with respect to the unburned mixture [21].

Detonation: An exothermic chemical reaction coupled to a shock wave that propagates through a detonable mixture. The velocity of the shock wave is supersonic with respect to the unburned gases. After initiation, the thermal energy of the reaction sustains the shock wave, and the shock wave compresses the unreacted material to sustain the reaction [21].

Hazard: A system state or set of conditions that, together with a particular set of worst-case environment conditions, will lead to an accident (loss) [17].

Overpressure: The pressure in a blast wave above atmospheric pressure [21].

Safety: Freedom from accidents (loss events) [17].

2.2 Acronyms

API	American Petroleum Institute
DCS	Distributed Control System
EPC	Engineering, Procurement, and Construction
IDLH	Immediately Dangerous to Life and Health
IEMI	Intentional Electromagnetic Interference
HEMP	High Altitude Electromagnetic Pulse
NFPA	National Fire Protection Association
NOx	Nitrogen Oxides

OE	Operating Experience
OSHA	Occupational Safety and Health Administration
PHA	Process Hazard Analysis
ppmv	parts per million by volume
PSM	Process Safety Management
RMP	EPA Risk Management Program
SCBA	Self Contained Breathing Apparatus
SCR	Selective Catalytic Reduction
SNCR	Selective Non-Catalytic Reduction
SOV	Solenoid Operated Valve

Section 3: Research Results

This report is based on interviews and research of literature and available guidance and standards.

A series of informal interviews were conducted with plant personnel, engineering firms, and consultants from the fossil generation industry and petro-chemical industry. The questions were designed to discover any 1) relevant guidance, standards, and best practices, 2) operating experience, and 3) EPRI member objectives for the report. The interview questions and summary of answers are included in Appendix A.

3.1 Owner/Operator Objectives

Owner/Operators and their proxies, such as Engineering, Procurement, and Construction (EPC) firms and consultants, identified the following objectives:

- Event-free operations and maintenance
- Industrial and personnel safety
- Habitability (for everyone, not just control room operators), including egress to habitable areas in the event of a hazard or accident
- Low initial cost of construction
- Compliance with NERC-CIP, OSHA, NFPA and Local Building Codes
- Well Designed Main Control Room (for example, Human Factors Engineering)

Owners agreed that the primary objective for this report was habitability and personnel safety. The remaining objectives were to be considered as part of the research.

3.2 Overview of Hazards, Events and Consequences

The term "hazard" per Reference [17] is *"a system state or set of conditions that, together with a particular set of worst case environment conditions, will lead to an accident (loss)."* Note that it is easy to confuse system states, conditions, and events when identifying hazards. Reference [17] further explains (emphasis added):

"This definition [of hazard] requires some explanation. First, hazards may be defined in terms of conditions, as here, or in terms of events as long as one of these choices is used consistently. While there have been arguments about whether hazards are events or conditions, the distinction is irrelevant and either can be used."

The hazard convention used in this guideline is the same convention used in the definition of hazard provided in Reference [17] (that is, hazards are system states or conditions, not events). For example, this guideline considers a toxic chemical as a potential hazard, and a toxic release would be an event with potential consequences (that is, injury or death).

3.2.1 The Bowtie Model

This guideline uses the "Bowtie Model," illustrated in Figure 3-1, to make the following key points:

- Hazards can be managed via facility design features and/or administrative controls so that events can be prevented, or their likelihood can be significantly reduced. Identify hazards, then identify methods for assessing their likelihood, and then identify measures that can be taken to preventing them. Hazards are differentiated from events.
- The consequences of an event, should one occur, can be mitigated via facility design features and/or administrative controls. If a hazard is not prevented or eliminated, or its likelihood exceeds an acceptable threshold, then measures can be taken to mitigate the consequences of the hazard to prevent harm, such as hardening structures where people work (for example, the control room).

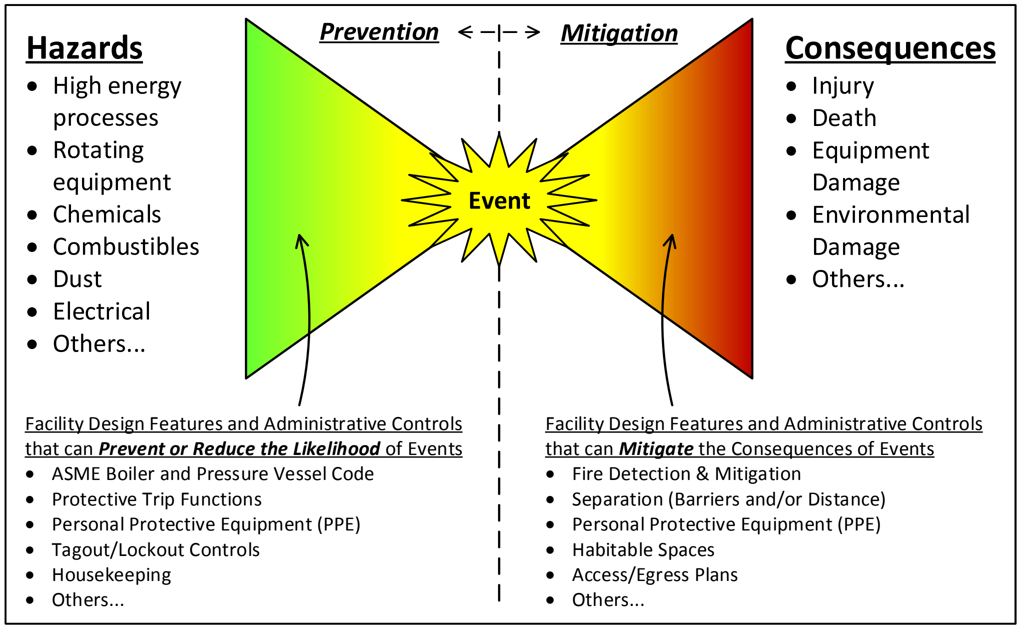

Figure 3-1
The Bowtie Model

There are a number of potential hazards within a fossil generation plant. A complete listing of all possible hazards and any ranking of those hazards is not available. However, based on interviews with owner/operators and some limited but publicly available event information (see Section 3.3), a partial list of hazards is provided on the left side of Figure 3-1, and is repeated in Table 3-1 alongside the events they can cause:

Table 3-1
Partial List of Potential Hazards and Related Events

Potential Hazards	Related Events
Lubricating oil	Fire
High energy line (for example, steam, liquid, gas)	▪ Leak ▪ Break
Hydrogen	▪ Harmful Release ▪ Fire ▪ Explosion
Natural gas	▪ Harmful Release ▪ Fire ▪ Explosion
Coal dust	▪ Harmful Release ▪ Explosion

Table 3-1 (continued)
Partial List of Potential Hazards and Related Events

Potential Hazards	Related Events
Rotating equipment	▪ Missile ▪ Misoperation (for example, during maintenance)
Chemicals (for example, anhydrous ammonia)	Toxic Release
Electrical equipment	▪ Short (phase-to-phase or ground) ▪ Arc Flash ▪ Misoperation
Malicious attacker	▪ Cyber penetration ▪ Physical penetration ▪ IEMI or HEMP
External (that is, chemical, wind, water, and so on)	▪ Toxic release from neighboring facility ▪ Dam break ▪ Tornado, Hurricane, Tsunami

3.3 Operating Experience

Some industries (for example, nuclear, refining co-ops) have created mechanisms for formally sharing lessons learned from events and shared analysis of solutions. Fossil generation industry experts share experiences informally through a variety of peer-to-peer relationships, and industry conferences and trade publications; however the fossil generation industry does not have a formal mechanism for capturing and sharing operating experience. EPRI 1012783, *Guidelines for Obtaining and Using Operating Experience at Fossil Power Plants*, EPRI, Palo Alto, CA; February 2007 [69] provides guidance for owner to create a program to capture and utilize operating experience from events within the owner's facilities.

During the interview process the project team attempted to capture information about control room design and design criteria as affected by past events and lessons learned, hazard characterization, and available guidelines and standards. The only available information was through one individual's personal experience and knowledge and some limited, publically available event information provided by OSHA.

3.3.1 Benefits of Shared Operating Experience

Some owner/operators may be reluctant to share event information for a variety of reasons, including:

- A belief that there is an increased risk of liability for legal action if information about an event is made public
- A belief that negative public relations could result if information about an event is made public
- Concern about individual job security

However, owner/operators can benefit by sharing operating experience with each other, in the interest of applying lessons-learned and preventing the same event at different facilities.

Unfortunately, in some cases, it requires the result of a catastrophic industrial event to initiate changes to the way an industry approaches hazard mitigation. For example, in the refining industry, a combination of operator error and poor siting of contractor domiciles resulted in 15 fatalities and 170 injuries when an explosion occurred at the BP Texas City in 2005. Fatalities and injuries occurred in and around work trailers that were placed too near to the process unit and were not evacuated prior to the startup. Alarms and gauges that should have warned of overfilling equipment failed to operate properly on the day of the accident. All who perished were contractors located in light wood trailers within 200ft of the explosion. Changes from this event resulted in greater scrutiny of operating procedures, maintenance and inspection protocols along with development of specific siting criteria for light wood trailers. OSHA imposed an $87 million fine on the company for failing to correct safety hazards, the largest fine issued in OSHA's history.

3.4 Event Prevention

At a glance, one might conclude from Figure 3-1and Table 3-1 that the only sensible way to avoid an event is to prevent it altogether by eliminating any hazards that can lead to events. However, upon closer examination, some hazards are related to components and materials that perform a useful function, and are within the control of the owner/operator, as described in Example 2-1. Some events can be prevented, or their likelihood significantly reduced, by taking credit for existing or proposed facility design features and/or administrative controls that can *prevent or reduce the likelihood of hazards that can lead to events*. Thus, event prevention (that is, the left-hand side of the bowtie model shown Figure 3-1) is a viable option for many potential hazards.

Example 2-1: Preventing a Hazard that is ***Within*** the Control of an Owner/Operator

A main generator is cooled by hydrogen gas, and hydrogen is not flammable when the fuel/air ratio is less than 4% by volume, or greater than 75% by volume. In the band of 4% to 75% fuel/air ratio, hydrogen is a significant hazard because it is easily ignited [18].

Design Features

The facility has the following design features to significantly reduce the likelihood of events due to a hydrogen hazard (that is, a flammable mixture of hydrogen and air):

- Overpressure relief devices are provided on hydrogen lines, and are located outdoors or in well ventilated areas
- Hydrogen monitors detect concentrations in certain spaces and provide a control room alarm when the concentration exceeds 2% by volume (preferably interlocked to shut down the hydrogen feed)
- Pressure sensors are mounted on the hydrogen supply, connected to the DCS for remote monitoring and archiving
- An odorant is added to the hydrogen so that leaks are detected by smell (similar to natural gas odorants)
- Ignition suppression is provided in areas that store or transport hydrogen

Administrative Controls

The owner/operator has also instituted the following administrative controls to significantly reduce the likelihood of events due to a hydrogen hazard:

- Gate guards are required to notify the control room when a hydrogen delivery truck arrives
- An equipment operator is dispatched to oversee hydrogen unloading operations, using a checklist
- The control room monitors hydrogen pressures during delivery operations and notifies the equipment monitor to take appropriate actions (up to and including evacuation to a safe area) if limits are exceeded

3.5 Event Mitigation

On the other hand, some hazards are not within the control of the owner/operator, and therefore it is not practical to focus on event prevention. Instead, owner/operators may be able ***mitigate the consequences of an event*** by taking advantage of existing or proposed facility design features and/or administrative controls (that is, the right-hand side of the bowtie model in Figure 3-1). Of course, even if some hazards and events are outside the control of the owner/operator, their likelihood is still an important concern when considering the application of design features and/or administrative controls. Example 2-2 describes the methods used by an owner/operator to mitigate the consequences of an event due to a hazard beyond its control.

Example 2-2: Mitigating Events Due to a Hazard that is ***Not Within*** the Control of an Owner/Operator

A fossil generation facility is located near a neighboring chemical plant that processes anhydrous ammonia. The chemical plant is owned and operated by another company, and it is not possible for the fossil generation owner/operator to directly prevent or reduce the likelihood of a hazardous release of ammonia. Instead, the owner/operator has elected to evaluate potential design features and administrative controls within their own facility that can be used to ***mitigate the consequences*** of a toxic ammonia release event caused by the neighboring facility:

Design Features

- A set of two ammonia sensors are mounted on the fence at the boundary of the fossil generation facility, directly in line with the neighboring chemical facility
- The sensors are equipped with transmitters that are connected to the DCS for indication, alarm and archiving
- The main control room ventilation system is set up to provide positive pressure
- Main control room HVAC dampers can be manually closed by the control room operator or automatically via the DCS if necessary

Administrative Controls

- The ammonia sensors are periodically calibrated using a source and procedure provided by the sensor manufacturer
- Ammonia sensor alarm setpoints are established according to OSHA requirements
- If an ammonia alarm is received, the main control room operator will alert other people to leave the area, or don personal protective equipment suitable for an ammonia plume
- Personal protective equipment suitable for egress through an ammonia plume is staged within the control room, maintenance shop, and office areas

3.6 Hazards and Events

Risk is a function of 1) the likelihood of a hazard leading to an event and 2) the consequences of the event, as shown in Figure 3-2. First, evaluate the likelihood of a hazard leading to an event on a low-medium-high basis (or any other suitable scale), then evaluate the consequences of that event on an equivalent scale. It is evident from Figure 3-2 that low likelihood + low consequences yields low risk and high likelihood + high consequences yields high risk, and everything in between is graded according to various combinations.

In most cases, owner/operators can manage risk by managing a potential hazard that can lead to an event, managing the consequences of an event, or managing both. In some cases the decision to prevent hazards or mitigate consequences, via facility design features and/or administrative controls, is a regulatory mandate (for example, NERC-CIP), while in other cases it is simply a business decision.

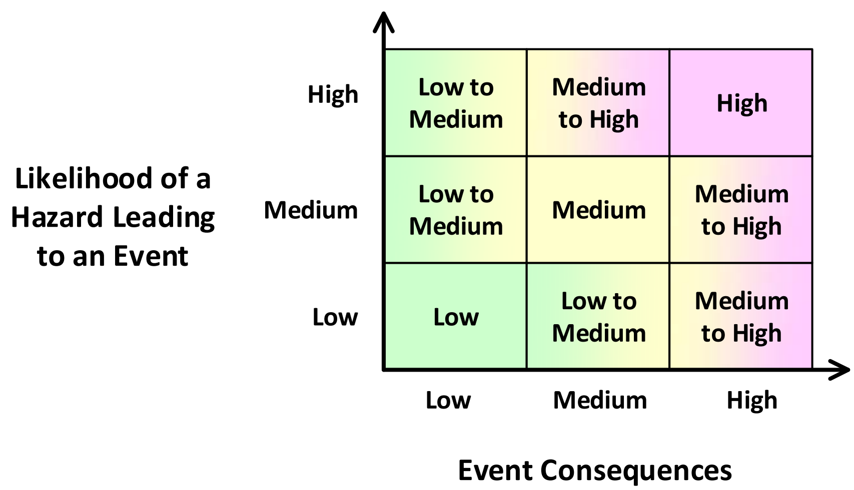

Figure 3-2
Risk as a Function of Event Likelihood vs. Event Consequences

The risk model in Figure 3-2 is analogous to the bowtie model in Figure 3-1 because both models are concerned about events, and both models communicate the idea that hazards can lead to events, which in turn, can have consequences. The difference between these models is that the bowtie model presents a deterministic view while the risk model presents a qualitative view or quantitative view (if probabilities are assigned).

Owner/operators should establish decision making and design criteria for managing risks based on:

- Identifying potential hazards
- Assessing the likelihood that an identified hazard will lead to an event
- Assessing the potential consequences of an event

3.7 Inhabited Space Hardening and Survivability

3.7.1 Interview Results

Interviews revealed that events that would dictate control room survivability and hardening were generally not considered in the original plant design. In many cases the main control room is a sheet metal structure that conforms to local building codes, with no consideration for survivability beyond 1) fire protection and 2) normal environmental conditions.

A number of interviewees considered some control room designs as unable to withstand significant events, such as explosions, because they were designed with windows overlooking the turbine, standard doors, and standard structures. These interviewees indicated that no guidelines or standards were known or used for control room hardening except in some instances for fire doors and for positive ventilation pressure. One interviewee stated that some upgrades to control room doors and HVAC systems for positive pressure were performed as part of larger projects. Some newer plant designs recognize the safety benefit of locating the control room and administrative spaces away from the power block. These newer plants take advantage of modern Distributed Control Systems (DCS) that reduce the cost of remote control (for example, using trunk line for communicating local I/O data back to remote controllers and servers).

The interview questions and summary of results are included in Appendix A.

3.7.2 Design Criteria Based on Hazard Analysis

Whether or not to harden an inhabited space or to modify existing equipment, and to what degree, are the key questions. Before expensive modifications are considered the design and decision making criteria need to be developed. Should all habitable enclosed spaces be considered? And how should any design criteria be developed? What if the likelihood of an event is extremely low?

Hazards should be identified and analyzed to determine their likelihood and the potential consequences of events. Some hazard analysis methods (for example, event trees, fault trees, quantitative risk assessment (QRA), and so on) are able to determine the probability of an event due to faults and failures of systems and equipment that could lead to hazardous conditions. In addition, there are modeling methods that are able to determine the consequences of a hazardous event. For example, it is possible to model a coal dust explosion within a particular facility to yield temperature, fire, and blast effects, such as a pressure wave, over distance and time.

Owner/operators can use hazard analysis results to help decide whether and how to harden habitable spaces. Engineering can establish design criteria for structures, such as "*all continuously occupied buildings shall be blast resistant to a 6.5 psi event*" and determine if any structural modifications are recommended. Only with that information can the owner determine whether the habitable spaces are in danger and whether to retro-fit the existing control room or to implement additional preventative measures.

An example of a graphical representation of a blast pressure wave from an explosion is shown in Figure 3-3. The blast wave shape provided is typical for any energetic overpressure event, be it a bursting pressure vessel, high explosive and so on. The rise time (shown in Figure 3-3 to be quasi-instantaneous) is more typical for a very energetic event, such as a detonation of high explosive. A finite rise time will occur for less energetic events, nevertheless, wave shapes are assumed to be of this character as it provides a conservative design basis.

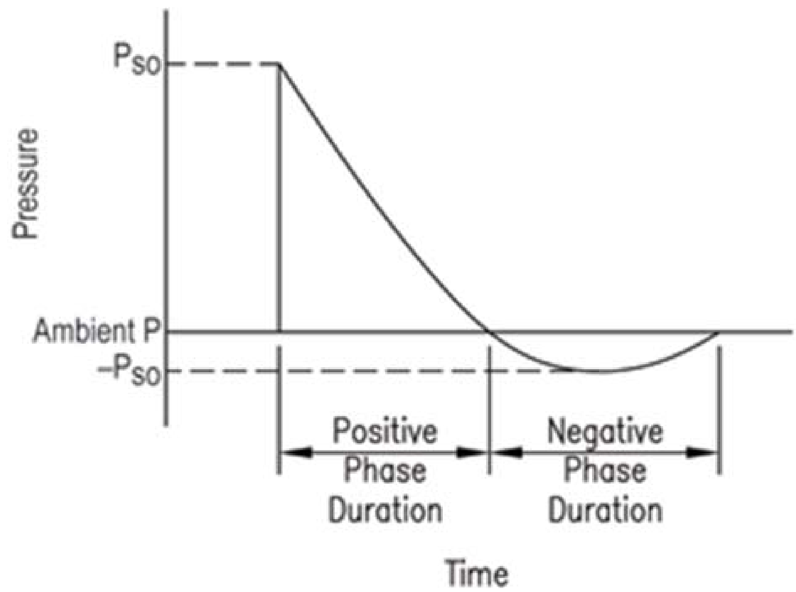

Figure 3-3
Typical Blast Wave History

The research was unable to find any standards, guidelines or efforts to model hazards for control room hardening within the fossil generation industry. However, existing standards, guidance, and models in the petroleum refining and chemical industry can identify some of the potential hazards, likelihood of event occurrence, and their potential consequences. The models are based on a thorough review of each plant design as well as current operations and maintenance practices, and they yield specific results.

The refining and chemical industry is models credible events as design input for habitable space hardening modifications, as well as operations and maintenance practices that can reduce the likelihood of events. See Section 14 for a description of hazard and event modeling within the petroleum refining and chemical industries. A proposed approach to use existing petroleum and chemical hazard analysis models for fossil generation is included in Appendix B.

Example 2-3: Coal Dust Explosion: Prevent, Mitigate, or Both?

A fossil generation facility burns pulverized coal. Coal dust is a potential hazard that, if it becomes airborne at the right fuel/air ratio in a contained enclosure, ignites and generates a significant blast wave, could be harmful to humans, structures and equipment.

A deterministic analysis (that is, with no consideration of likelihood) of a potential coal dust explosion shows that the control room is subject to a blast overpressure greater than 6.5 psi. The owner/operator considers the following options:

Design Features

Design a structural modification of the control room to withstand the blast load so that inhabitants can survive and safely evacuate. Particular attention should be made to doors and windows which are often the weakest components and can generate projectile hazards. Further, door integrity is essential for effective evacuation post-event.

Administrative Controls

Take credit for an existing coal dust housekeeping program that is designed to prevent coal dust from becoming a hazard

The owner/operator then assesses the risk of coal dust explosions by assessing the *likelihood* of a coal dust hazard leading to a detonation event. Even though the *consequences* of a coal dust explosion event are high, the likelihood is low, such that the risk is judged to be moderate using the risk matrix illustrated in Figure 3-2. To reduce risk, the owner/operator reduces the likelihood of a coal dust explosion by strengthening the existing administrative controls via:

- Expanded training and awareness of the coal dust housekeeping program to all employees located at the facility
- Periodic self-assessments of the coal dust housekeeping program, and taking corrective actions as needed
- More specific criteria for managing ignition sources in areas where coal dust accumulations could become hazardous

Control rooms often have other unctional spaces within the same structure, such as administrative offices, break rooms, meeting rooms, and personnel inhabit other enclosed spaces inside the plant such as a maintenance shop or tool room. Some spaces are continuously inhabited versus occasionally inhabited, and should be accounted for in the analysis.

Another consideration is egress paths. In the event of a catastrophic event, personnel typically are expected to evacuate to a safe area and stay there until further notice. If the control room is designed to withstand an event, but there is not a safe evacuation route, then the design may not meet the objective of personnel safety.

When developing the design criteria for hardening, all inhabitable spaces and egress should be considered.

Section 4: Events That Can Impact Inhabited Spaces

The following four events are described at a high level for the purpose of identifying some specific potential hazards that could, under certain conditions, lead to events that could adversely impact the main control room and other inhabited spaces. The hazards, events and consequences described in this section are only generalized and are not meant to be definitive or complete. Their only purpose here is to describe how facility design features and/or administrative controls can be used to 1) prevent or significantly reduce the likelihood of these events, or 2) reduce their consequences. Any guidance, criteria or recommendations summarized herein are not necessarily comprehensive or complete, and are meant only to show that hazards can be identified, the likelihood of events can be reduced, and if an event occurs, options for how its consequences can may be mitigated.

Owner/operators should consider the hazards within their own facilities and assess the available or proposed design features and/or administrative controls (using the appropriate codes, standards and guidelines), that can be used to 1) prevent or significantly reduce the likelihood of events that can result from those hazards, and/or 2) mitigate the consequences.

4.1 Hydrogen Explosions

Hydrogen explosions do occur in fossil generation facilities and should be a concern of any owner/operator that uses hydrogen within their facility. This section focuses on hydrogen explosions because of the interest in such operating experience. However, other hydrogen-related events due to liquid and gaseous hydrogen hazards can occur, such as releases that can lead to frostbite or asphyxiation. See Reference [21] for guidance on other hydrogen-related hazards and events.

4.1.1 Operating Experience

In 2013 a coal fired plant in Georgia experienced a generator hydrogen explosion that injured three people, resulting in significant damage and $119K in proposed fines. The explosion resulted from a mixture of generator hydrogen and air that was ignited during maintenance activities.

In 2007 a coal fired plant in Ohio experienced a hydrogen explosion during a delivery by a local supplier. The explosion, which resulted from a leak past a faulty rupture disk device, killed the delivery truck driver and injured nine plant employees [19].

4.1.2 Hydrogen Hazards and Hydrogen Explosion Event Characterization

If hydrogen is used in a fossil generation facility, it most likely involves a main generator cooling application. It is usually collected by manufacturers via cryogenic methods, stored in a liquid form under pressure, and delivered by local suppliers via tank trucks where it is transferred to one or more tanks located within or adjacent to the generation facility. Pipes and valves are used in a hydrogen supply system that transports stored hydrogen, at the appropriate pressure, to its end use application. Local pressure indicators and pressure regulators are typically used by delivery truck operators or equipment operators to manage the hydrogen supply system, and overpressure relief devices such as rupture discs or relief valves are used to limit overpressure transients.

Hydrogen, being the lightest element in the periodic table, has a higher propensity for leakage than other gases. Leaks usually occur via inadequate seals or gaskets, valve misalignment, or failures of flanges or equipment [21]. Hydrogen is flammable in a wide range of fuel/air ratios (4% to 75%), and is easily ignited via energy sources as low as 0.02 millijoules at atmospheric pressure. It is odorless and tasteless. It is lighter than air and will therefore rise and collect under roofs and overhangs where it can form an explosion hazard. [18].

When hydrogen is mixed with air at a ratio between 4% and 75%, and it is ignited, the result is usually a ***deflagration***, which is defined as "*a flame moving through a flammable mixture in the form of a subsonic wave (with respect to the unburned mixture)*" [21]. In some cases, particularly at optimal combustion concentration and turbulent conditions, a deflagration can evolve into a ***detonation***, which is defined as an "*Exothermic chemical reaction coupled to a shock wave that propagates through a detonable mixture. The velocity of the shock wave is supersonic with respect to the unburned gases. After initiation, the thermal energy of the reaction sustains the shock wave, and the shock wave compresses the unreacted material to sustain the reaction*" [21].

It is worth noting that a ***blast wave*** is a result of a shock wave, and is defined as a *"pressure pulse following a shock wave. It is due to velocity imparted by the shock wave to the medium particles"* [21]. Blast waves result in ***overpressure***, which is defined as "t*he pressure in a blast wave above atmospheric pressure* [21]. The physics of hydrogen deflagrations, detonations, shock waves and blast waves are complex and beyond the scope of this guideline. However, Reference [21] provides the following general characteristics of burning hydrogen:

- The flame temperature of burning hydrogen in air, at 19.6% by volume, is 3,718°F.
- Under turbulent conditions, a deflagration flame front can approach hundreds of meters per second.
- If turbulent conditions are sufficient, the flame speed may transition to supersonic, resulting in a detonation, and the resulting reaction zone is a shock wave and the accompanying blast wave has a much greater potential for causing personnel injury or equipment damage.
- Overpressure due to a hydrogen blast wave varies widely and its magnitude is dependent on a variety of factors that are described in Annex C of Reference [21], including the fuel/air ratio, ignition source, and whether or not the explosion is initiated in a confined space (such as in a main generator exciter enclosure).
- Overpressures for a hydrogen explosion can be as high as 30 psig for a moderate deflagration and > 300 psig for a detonation.
- Section 2.10.3.11 of Reference [21] describes the physiological consequences of overpressure due to blast waves ranging from ***eardrum ruptures*** in the 3.4 to 74.4 psi range, ***lung damage*** in the 15 psi (100ms duration) to 174 psi (0.5ms duration) range, and ***lethal lung rupture*** in the 50 psi (79ms duration) to 126 psi (17ms duration) range.

4.1.3 Preventing and Mitigating Hydrogen Explosions

The bowtie model illustrated in Figure 4-1 lists some of the potential explosive hazards presented by hydrogen on the left-hand side, and the potential consequences of a hydrogen explosion on the right-hand side. Note that other consequences such as frostbite and asphyxiation due to local releases of liquid or gaseous hydrogen are not discussed here because the scope of this guideline is limited to main control room hardening and survivability.

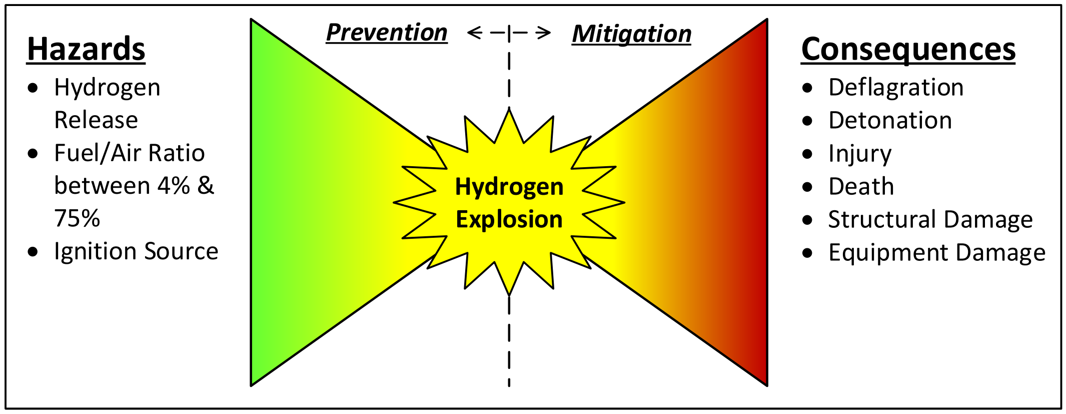

Figure 4-1
Hydrogen Explosion Bowtie Model

4.1.3.1 Reducing the Likelihood of Hydrogen Explosions

Design Features

Reference [21] describes design features that can be used to ***prevent or reduce the likelihood of a hydrogen hazard*** leading to a hydrogen explosion (note that this list is not all inclusive; consult Reference [21] for detailed guidance):

- Selection of compatible materials for hydrogen supply system service, such as aluminum, copper, and authentic stainless steels, using the general guidance of Tables A5.1 and A5.2 in Reference [21], and forbidding the use of gray, ductile or cast iron materials in hydrogen systems per 29 CFR 1910.103 and NFPA 50A.
- Reducing the effects of hydrogen embrittlement and stress corrosion cracking by loss prevention measures such as coatings, elimination of stress concentrations, increased material thickness, surface finish, and so on.
- Eliminating ignition sources via lightning protection, dissipating static charge in vent stacks via discharge rods, bonding and grounding metallic structures, and so on.
- Ventilating structures with normal air exchange of about 1ft^3 per square foot of solid floor in the space, establishing a ventilation rate that can dilute gaseous hydrogen leaks to about 1% by volume, and locating ventilation outlet at the high point of a room in an exterior wall or the roof.
- Hydrogen containing vessels, piping and equipment failures caused by overpressure results in a leak before it ruptures.
- For hydrogen containers in buildings, vent their safety relief devices, without obstruction, to the outdoors at the minimum elevation to assure safety; and locate safety relief vents at least 50 feet from air intakes.

- Hydrogen systems meet the design criteria and guidance in the following Sections of Reference [21]:
  - Section 5.2: fixed and mobile hydrogen storage vessels
  - Section 5.3: piping systems
  - Section 5.4: components
  - Section 5.5: overpressure protection
  - Section 5.6: venting and flaring
  - Section 5.7: contamination
- Locate and install hydrogen storage facilities per 29 CFR 1910.103 and NFPA 50A.
- Instrument hydrogen systems for monitoring and controlling operations, logging performance data, provide warning and alarms for out-of-limit conditions, and indicate hazardous conditions; and ensure hydrogen detectors meet Class I, Division I or II, or Group B requirements of NFPA 70 as appropriate.

Administrative Controls

Reference [21] also describes administrative controls that can be used to ***prevent or reduce the likelihood of a hydrogen hazard*** leading to a hydrogen explosion (note that this list is not all inclusive; consult Reference [21] for detailed guidance):

- Setting up exclusion areas in which personnel access is limited, equipment meets requirements for elimination or control of ignition sources, and operations are consistent with safety requirements
- Areas within 15 feet of gaseous hydrogen or 25 feet of liquid hydrogen kept free of weeds, dry vegetation and combustible materials
- Personnel accessing an exclusion zone provided with PPE and detection devices
- Exclusion areas have placarding, posting and labelling warns that hydrogen is present, is a flammable gas, and smoking and open flames are prohibited
- Avoid spraying water or using water in a fire suppression system in or around hydrogen vent openings
- Document, tag and label hydrogen storage vessels, piping and components
- Provide portable hydrogen detection equipment for personnel entering an area where hydrogen is leaking or may have leaked
- Hydrogen storage piping and installation are examined, inspected and certified in accordance with the ASME Boiler and Pressure Vessel code, AMSE B31.1, or ASME B31.3, as appropriate
- Hydrogen systems are operated and maintained within limits

- Hydrogen detectors are maintained and periodically calibrated
- Offloading of hydrogen deliveries includes notification of appropriate personnel such as a safety representative
- Liquid hydrogen vessels are purged before loading to ensure removal of any condensable gas or air

4.1.3.2 Mitigating the Consequences of Hydrogen Explosions

Design Features

Reference [21] describes design features that can be used to ***mitigate the consequences of a hydrogen explosion*** (note that this list is not all inclusive; consult Reference [21] for detailed guidance):

- Designing buildings with explosion venting in exterior walls or the roof, with a minimum venting area of 0.033 ft^2 per cubic foot of room volume (this is a minimum requirement but typically not sufficient to provide effective mitigation for most instances, in that, an evaluation must be performed to determine actual vent area requirements [for instance, if the deflagration transitions to detonation, then venting provides zero mitigation benefit])
- Design control rooms to protect occupants from the most severe credible hazard
- Consider control room windows a hazard; windows should be eliminated or made as small as practical and should be designed to withstand the predicted blast load
- Provide appropriate fire detection and suppression systems for hydrogen systems containing significant hazards

Administrative Controls

Reference [21] also describes administrative controls that can be used to ***mitigate the consequences of a hydrogen explosion*** (note that this list is not all inclusive; consult Reference [21] for detailed guidance):

- Personnel are notified immediately upon detection of hydrogen leaks or fires.
- Apply fire suppression methods to control a remaining fire until the release of fuel is terminated or the fuel supply is exhausted.
- Emergency procedures address escape, escape routes, personnel accountability, reporting, fire suppression response, appropriate medical response, and summoning outside assistance.

4.1.4 Codes, Standards and Guidelines Related to Hydrogen Safety

The following codes, standards and guidelines can be used to inform an assessment of facility design features and administrative controls that can be used to 1) identify hydrogen related hazards, 2) prevent or reduce the likelihood of hydrogen hazards leading to explosions, and 3) if a hydrogen explosion occurs, characterize and mitigate its effects:

1. AIAA G-095-2004, "Guide to Safety of Hydrogen and Hydrogen Systems," American Institute of Aeronautics and Astronautics (AIAA), 1801 Alexander Bell Drive, Reston, VA 20191 (ISBN: 1-56347-675-4).
2. 29 CFR 1910.103, "Hydrogen".
3. NFPA 50A, "Standard for Gaseous Hydrogen Systems at Consumer Sites," National Fire Protection Association, 1999.
4. NFPA 50B, "Standard for Liquefied Hydrogen Systems at Consumer Sites," National Fire Protection Association, 1999.
5. NFPA 70, "National Electric Code," 2014 Edition.
6. EPRI 1025330, *Turbine-Generator Auxiliary Systems, Volume 3: Generator Hydrogen System Maintenance Guide*, EPRI, Palo Alto, CA; December 2012.

4.2 Steam Turbine Wrecks

As described below, turbine wrecks do occur in fossil generation facilities and should be a concern of any owner/operator.

4.2.1 Operating Experience

In 2011, a fossil generation facility in South Africa experienced a catastrophic main turbine wreck due to an overspeed condition during testing. Nobody was hurt, but *"…extensive damage was done to the plant by missiles created by thrown machine components*" [22].

Reference [23] summarizes twenty-one main turbine failures between 1950 and 1972, fourteen of which generated missiles that penetrated the turbine casing. Nine of the fourteen missile events were caused by "…*manufacturing defects or design deficiencies in the rotating parts, and occurred near or at normal operating speeds; however, due to improved turbine design and improved manufacturing techniques, these failures would be unlikely to recur*", and "…*the other five overspeed events that generated missiles were caused by common-mode failures – sticking of steam control and dump valves…* [due to] *small clearances around valve stems and the presence of foreign material.*" Reference [23] adds that "*most of the overspeed events occurred at non-nuclear facilities with high temperature steam (~1000°F). High-temperature steam promoted the buildup of "boiler salts" – that is, salts or oxides – on the steam admission valves.*"

In 1977, a fossil station equipped with an 1800 RPM cross-compound, eight stage double-flow turbine experienced a last stage low pressure turbine disc rupture (see details below) [28].

4.2.2 Steam Turbine Hazards and Steam Turbine Wreck Event Characterization

As used here, a steam turbine wreck is a significant dynamic event that involves catastrophic damage of the turbine, up to and including shaft breaks, rotor disc failures, casing ruptures, and missiles (that is, turbine blades, shaft pieces, and so on).

The dynamics of turbine wrecks and missiles are complex and beyond the scope of this report. The limiting case is likely to be a rupture of a low pressure rotor disc (or wheel) in an 1800 RPM machine with shrunk-on discs that crack at bore, keyway and rim attachment locations due to stress corrosion mechanisms [27] [30].

The likelihood of a rupture increases significantly as turbine speed approaches destructive overspeed conditions. Reference [31] describes two broad categories of turbine failures, referred to as "design overspeed" (up to 130% of the rated speed) and "destructive overspeed" (any speed above the design overspeed), and adds that "*Missiles resulting from design overspeed failures are the result of the brittle fracture of turbine blade wheels or portions of the turbine rotor itself. Failures of this type can occur during startup or normal operation. Missiles resulting from destructive overspeed failures would be generated if the overspeed protection system malfunctioned and if the turbine speed increased to a point at which the low-pressure wheels or rotor would undergo ductile failure*."

Reference [28] describes an event at a fossil station equipped with an 1800 RPM cross-compound, eight stage, double-flow turbine that experienced a last stage low pressure turbine disc rupture due to a stress corrosion crack in a blade attachment area, while operating at normal speed. One segment of the ruptured disc "…*exited the turbine casing with a trajectory sloping upwards at about 15 degrees. Exiting the building, the segment sheared through a 12 inch steel beam and perforated a 6 inch thick reinforced concrete wall. The segment then struck a 55,000 lb. transformer, whose end was displaced about 6 feet, deflecting the segment's trajectory slightly to one side. The segment then bounded off the side of an adjacent hill and impacted equipment in the switch yard on top of the hill. The segment came to rest 355 feet away from and 60 feet above the turbine axis*."

4.2.3 Preventing and Mitigating Steam Turbine Wrecks

The bowtie model illustrated in Figure 4-2 lists some of the potential hazards that can lead to a turbine wreck on the left-hand side, and the potential consequences of a turbine wreck on the right-hand side.

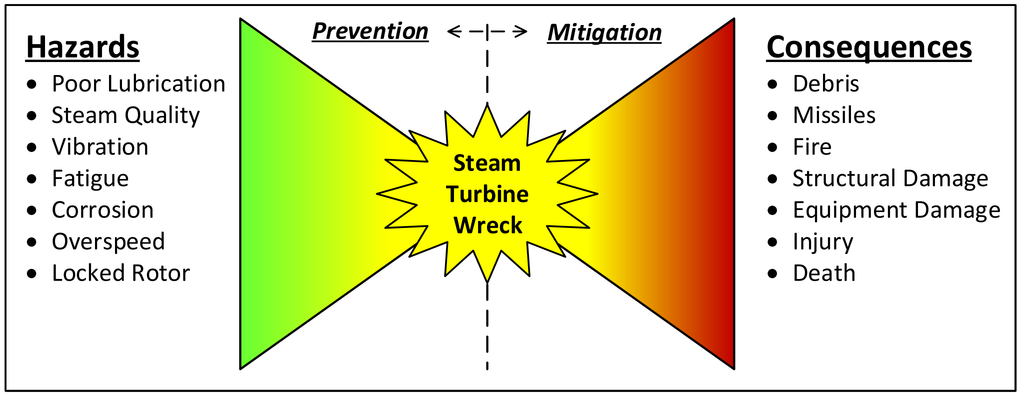

Figure 4-2
Steam Turbine Wreck Bowtie Model

The leading causes of steam turbine damage and related losses in the chemical, oil and gas industries, between 1980 and 1995, are characterized in [29] as follows (in order of relative size of average loss):

- Overspeed
- Fatigue, corrosion, stress
- Water induction
- Excessive vibration
- Loosening of parts

4.2.3.1 Reducing the Likelihood of Turbine Wrecks due to Overspeed Conditions

For brevity, the remainder of the discussion on turbine wrecks is limited to those due to overspeed conditions because they are more likely to result in the most significant consequences [29]. A turbine overspeed hazard leading to a rotor burst that destroys the turbine case generally depends on three conditions [29]:

- A sudden and large loss of load
- The governor valve fails to control the speed of the turbine
- The overspeed trip system fails to function properly

Reference [23] advises that the probability of unacceptable damage due to a turbine missile is the product of three probabilities (modified here for applicability to main control room hardening and survivability):

- P1: probability that a high energy turbine missile will penetrate its casing
- P2: probability that the high energy turbine missile will strike the main control room
- P3: probability that the high energy turbine missile will cause unacceptable damage to the main control room

Design Features

The following design features can be used to ***prevent or reduce the likelihood of an overspeed condition*** that can lead to a turbine wreck:

- ANSI/ISA 77.14.01-2010 [23] prescribes the following criteria for steam turbine overspeed trip systems in fossil fuel facilities:
  - "Two independent turbine overspeed trip systems shall be provided: The primary system shall be within the turbine control system; the backup system shall be either a mechanical overspeed trip device or an electronic overspeed trip system as defined by the American Petroleum Institute standard, API 670.
  - The backup overspeed trip system shall be capable of tripping the turbine without the involvement of the turbine control system.
  - Speed sensing devices (probes) used by the turbine control system shall be independent of those used by a backup electronic overspeed trip system.
  - The turbine control system and the electronic overspeed trip system, when utilized as the backup system for the overspeed trip function, shall perform the trip function through independent solenoids.
  - A multi-toothed surface for speed sensing shall be provided integral with or securely attached to the turbine shaft. Sharing this surface between the turbine control system, a backup electronic overspeed trip system, and a tachometer shall be permitted. Details of the speed sensing measurement shall follow API 670."
- API 670 [24] provides minimum electromechanical requirements for machinery protection systems, under the following categories:
  - General design specifications (temperature, humidity, shock, accuracy, chemical resistance, and so on).
  - Conventional hardware requirements (radial shaft vibration, axial position, speed, phase reference, accelerometer-based casing transducers, temperature, monitoring systems, wiring and grounding, and so on).
  - Transducer and sensor arrangement (location, orientation, mounting, identification, and so on).
  - Inspection, testing and shipment.
  - Vendor's data.
- EPRI 1013461 [25] provides guidance on modernizing turbine overspeed trip systems, covering the following design-related issues and topics:
  - Better protection by removal of hazards, improved reliability, improved safety, redundancy, better control, and avoiding obsolescence.
  - Applying FMEA to improve the design by identifying and resolving unacceptable failure modes and effects.
  - Providing design features for surveillance and overspeed test activities.

- Reference [29] provides the following design recommendations to prevent or reduce the likelihood (that is, P1 per the above discussion of probabilities) of large industrial steam turbine wrecks due to overspeed conditions:
  – Apply a liberal safety factor in the design of couplings.
  – Equip steam turbines and driven equipment with condition monitoring systems.
  – Provide axial vibration trips on excess vibration.
  – Provide bearing temperature trips on excess temperature or high rate of temperature increase.
  – Use electronic governors and electronic overspeed trip systems because they can:
    - Be tested online with a simulated or stimulated signal
    - Generally respond more quickly to changing conditions
    - Provide redundancy and eliminate single point vulnerabilities
    - Eliminate moving parts that are sources of mechanical problems (for example, links, levers, trip bolts, and so on)
  – Electronic overspeed trip systems should have at least two independent speed sensing systems, and the governor system should have its own speed sensing system. The overall protection system design should ensure that both the governor valve and trip/throttle valve close when overspeed is detected.
- Reference [23] describes the following design considerations that can help reduce the likelihood (P1) of overspeed events:
  – Turbine speed indication at the front standard.
  – A detent in the turbine trip lever at the front standard to assist an operator that is required to hold the lever in one position during overspeed testing.
  – Improved communication between front standard operator and the control room.
  – Backup trip solenoid operated valve (SOV) to enable protective turbine trip during testing.
  – System modifications to enable independent, full functional hydraulic operational testing of all turbine protection SOVs.
  – Avoid use of spool-type SOVs.
  – Use of a filter in the turbine oil header to reduce foreign material.
  – Prevent bypass of valid turbine trip signals during turbine trip testing.

- One option for owner/operators of steam turbines with shrunk-on discs that may be susceptible to cracking and rupture is to replace them with new wheels or mono-block rotors that are less susceptible to cracking and rupture mechanisms.
- Reference [33] describes a number of credible failure modes in couplings that can lead to turbomachinery damage, and coupling designs that can prevent or reduce the likelihood of failed couplings.

Administrative Controls

The following administrative controls can be used to ***prevent or reduce the likelihood of an overspeed condition*** that can lead to a turbine wreck:

- EPRI 1013461 [25] also provides guidance on overspeed trip system test methods and test frequency
- Reference [29] advises that "*the greatest probability of success in preventing a catastrophic steam turbine overspeed accident lies in proper coupling installation and condition monitoring to ensure excessive stress is not applied to the coupling while the turbine is in operation.*"
- Reference [29] also provides the following recommendations for preventing large industrial steam turbine wrecks due to overspeed conditions:
  - When a steam turbine is shut down for a scheduled outage after being in service for an extended period, or during an overspeed test, stop the turbine by tripping the trip/throttle valve and measure the closing time. If the closing time is excessive, determine and correct the cause.
  - Consult the manufacturer to determine the appropriate frequencies and procedures for proper testing, exercising, inspecting and maintaining trip/throttle valves.
  - Provide specific, detailed and written procedures for overspeed trip tests
  - When performing an uncoupled or low load overspeed trip test, turbine speed should be controlled with a hand operated block valve.
  - Provide every effort to ensure good quality steam because most overspeed accidents involved governor valve and/or trip/throttle valve sticking, and most of the sticking problems are caused by impure steam.
- Reference [30] suggests the following approach to detecting and correcting conditions that can lead to cracks and failures in rotors with shrunk-on wheels:
  - Determine material properties of each disc (yield strength, fracture toughness, hardness, and chemical composition) through sampling and testing.
  - Determine stress profile of each disc via finite element stress analysis.
  - Determine critical flaw sizes at various locations.

- Assess high potential crack locations with advanced ultrasonic inspection methods.
- Assess remaining life based on past, current and planned operating conditions.

- Reference [27] reports that discs that have been exposed *only* to dry steam have not cracked, and discs that have been exposed to wet steam have cracked *only* when evidence of higher-than-normal oxygen levels are present
- Reference [23] describes the value of clear, written procedures and operator training to assure that the steam supply to the main turbine is isolated before the generator output breakers are opened; or avoiding premature relatching that can reopen the steam admission valves.
- Reference [33] describes a number of administrative controls, such as maintenance activities, that can prevent or reduce the likelihood of failed couplings.

4.2.3.2 Mitigating the Consequences of Turbine Wrecks due to Overspeed Conditions

Design Features

The following design features that can be used to ***mitigate the consequences*** of a turbine wreck:

- Although Reference [31] takes a deterministic approach (that is, assume a turbine missile event occurs), it provides the following recommendations for safeguarding against turbine missiles (adapted here for protecting the main control room):
  - Orient the turbine (or the main control room) so that the main control room is less likely to be hit by a missile. Missiles are generally characterized as "low trajectory" (at or near horizontal) and "high trajectory" (that is, not low trajectory) for low pressure wheels in 1800 RPM machines. The hazard zone that is most susceptible to low trajectory missiles is depicted in Figure 4-3; if the main control room (or any other area that should be protected) is outside the gray zone in Figure 4-3 then the turbine is considered to be in a favorable orientation that significantly reduces the likelihood of a low trajectory missile hit.
  - On the other hand, protection against high-trajectory missiles involves reducing the likelihood of a turbine missile to begin with (per Section 4.2.3.1, above), or use barriers to block the missile from damaging the control room or any other areas that should be protected. When barriers are used to protect the control room, they are considered acceptable if no missile can compromise the final barrier that protects personnel and essential equipment. Steel barriers should be thick enough to prevent perforation, and concrete barriers should be thick enough to prevent backface scabbing.

- For unfavorably oriented turbines, barriers should protect the control room, and any other areas that should be protected, from both high-trajectory and low-trajectory missiles. For favorably oriented turbines, barriers should protect the control room, and any other areas that should be protected, from high-trajectory missiles.

- EPRI 1009665 [32] provides the following engineering judgments regarding structures that could be credited or designed as turbine missile barriers:
  - Equipment located within structures made of lightly reinforced concrete barriers on the order of (that is, at least as thick as) 12 to18 inches (30 to 40 cm) in thickness are less likely to be damaged by a missile than is unprotected equipment. Below 12-inch (30-cm) thickness, barrier effectiveness diminishes significantly.
  - Equipment located beyond two 12- to 18-inch (30- to 40-cm) barriers made of lightly reinforced concrete is not vulnerable to damage by a turbine missile unless the missile is of sufficient energy to penetrate the first barrier.
  - Equipment located beyond a barrier of more than 36 inches (91 cm) is not vulnerable to damage by a turbine missile.

- A hydrogen fire or explosion can also occur in conjunction with a turbine wreck. See Section 4.1.3.2 for guidance on facility design features that can mitigate the consequences of a hydrogen explosion.

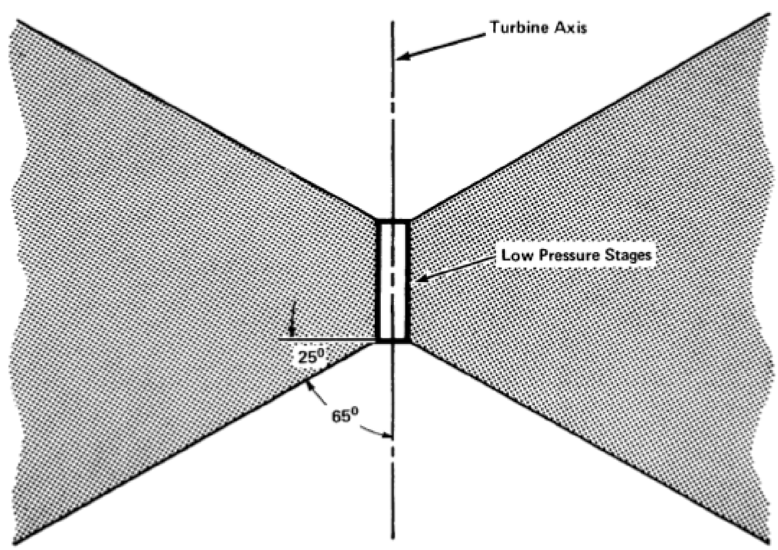

Figure 4-3
More Likely Missile Strike Zone (from RG 1.115)

Administrative Controls

The literature search performed for this report did not reveal any administrative controls that can be used to ***mitigate the consequences*** of a turbine wreck once it happens, probably because it is a very dynamic and catastrophic event that can only be effectively mitigated via facility design features. However, turbine wrecks can also result in secondary effects such as lube oil fires or hydrogen fires or explosions. See Section 4.1.3.2 for an overview of some administrative controls that can mitigate the consequences of a hydrogen explosion.

4.2.4 Codes, Standards and Guidelines Related to Steam Turbine Overspeed Safety

The following codes, standards and guidelines can be used to inform an assessment of facility design features and administrative controls that can be used to 1) identify hazards that could lead to overspeed-related turbine wrecks and prevent them or reduce their likelihood; and 2) if a turbine wreck occurs, characterize and mitigate its effects:

1. ANSI/ISA 77.14.01-2010, "Fossil Fuel Power Plant Steam Turbine Controls".
2. API 670, 4th Edition, "Machinery Protection Systems," American Petroleum Institute, December, 2000.
3. EPRI 1009665, *Guidance for Performing a Simplified Risk-Informed Turbine Missile Analysis*, EPRI, Palo Alto, CA; March 2005.
4. EPRI 1013461, *Turbine Overspeed Trip Modernization – Requirements and Implementation Guidance*, Final Report; EPRI, Palo Alto, CA; November 2006.
5. "Rotating Equipment Loss Prevention – An Insurer's Viewpoint," Clark, Proceedings of the Twenty-Fifth Turbomachinery Symposium, 1997; Texas A&M University.
6. "Coupling Credible Failure Modes and Owner Options to Intervene," by Locke, et al; Proceedings of the Forty-Second Turbomachinery Symposium, 2013; Texas A&M University.

4.3 Coal Dust Explosions

Dust explosions are credible in fossil generation facilities, for example, due to the presence of coal dust at coal fired power plants. This section focuses specifically on coal dust explosions because of the interest in such operating experience. Other hazards associated with coal include coal pile fires and coal dust flash fires, the latter being a concern to the operator where the former may also impact the integrity of occupied buildings.

4.3.1 Operating Experience

In 1999 a natural gas and coal fired power plant explosion in Michigan resulted in 6 fatalities and 14 serious injuries. The primary explosion resulted from an unintentional natural gas buildup in the furnace of an idle power boiler and was followed by a secondary explosion of disturbed coal dust. For more information see OSHA Technical Information Bulletin TIB 00-11-06 [48].

An explosion at a San Antonio power plant occurred after coal dust in a silo caught fire, doing damage to the cascade building atop. Coal was being fed into silos before being pulverized and moved into the plant itself. Two employees suffered minor injuries from falling debris [49].

4.3.2 Coal Dust Hazards and Coal Dust Explosion Event Characterization

Coal is typically prepared for use by crushing rough coal into small pieces. The crushing process generates significant fine particulates. The coal is then transported from the storage yard to in-plant storage silos. In plants that burn pulverized coal, silos feed coal pulverizers that further grind the coal to the consistency of talcum powder. The coal is sorted then blended with primary combustion air which transports the coal to the boiler furnace. In plants that do not burn pulverized coal, the larger coal pieces may be directly fed into the silos which then feed either mechanical distributors that drop the coal on a traveling grate or to cyclone burners which can efficiently burn larger pieces of fuel.

For a dust explosion to occur, there are five elements required to occur simultaneously: fuel, thermal energy, oxygen, suspension, and confinement. These form the five sides of the dust explosion pentagon. Like the fire triangle, removing any one of these requirements would prevent a dust explosion from propagating, although lack of confinement may still produce a flash fire. Similarly, lack of particulate suspension may result in a fire. The five components are discussed in greater detail in the following sections.

4.3.2.1 Fuel and Particle Size

Fuel particle size is an important factor, in that, too large a particle is difficult to suspend and also has significant thermal inertia required to initiate and propagate combustion. Experiments have shown that bituminous coal particles passing through a U.S. standard 20-mesh sieve (841 μm) can participate in a coal dust explosion [50]. For complete combustion, an industrial suspension boiler using bituminous coal requires an average particle size of 45μm and 80 to 85% of particles to be less than 200-mesh (74 μm) [50]. Per NFPA 654 [51], these coal dust particles are classified as combustible since "combustible particulate solids with a minimum dimension more than 500 micron generally have a surface-to-volume ratio that is too small to pose a deflagration hazard." In general, the smaller the particle size, the easier it is for the cloud to become suspended and ignited, and the intensity of the potential explosion is typically more severe.

4.3.2.2 Thermal Energy

Thermal energy is required to initiate the combustion reaction process. There are generally two forms of energy which ignite coal dust in industry; static discharge or heated surfaces.

The *minimum ignition energy* (MIE) required to ignite a cloud of coal dust can be as low as 30 mJ. For the most part, low energy electrostatic discharges are not an issue (for example, brush discharge associated with an insulating material such as a plastic container that has accumulated electrostatic charges resulting from the flow of material). People, however, on the upper end can generate sufficient electrostatic charge of this magnitude. Ungrounded/bonded equipment and inappropriately rated electrical enclosures and equipment can have more than sufficient energy to ignite a cloud of coal dust.

The *minimum ignition temperature* (MIT) of a dust cloud is the thermal energy imparted by a heated surface which may ignite a cloud or pile of coal dust. The ignition temperature of a coal dust cloud or pile decreases as the volatile content increases, and may be as low as 440°C (824°F) for a dust cloud and 160°C (320°F) for a dust pile. As the particle size decreases, the coal dust cloud also becomes easier to ignite. With dust layers on hot surfaces, the minimum ignition temperature decreases as the thickness of the deposit is increased. This is due to the insulating properties of layered material.

4.3.2.3 Dust Concentration in Suspension

The *minimum explosive concentration* (MEC) is an important parameter required to generate a dust explosion. This is the minimum quantity of dust in suspension that will propagate combustion in a cloud of coal dust. The MEC for bituminous coal is approximately 100 grams per cubic meter [50]. This means an average layer of 1-mm thick across the footprint of a building with height of 15-ft would be sufficient to generate the MEC if suspended. In other words, if coal dust layers are visible on the floor or elevated surfaces of a plant, then there is sufficient coal dust, if suspended, to propagate an explosion.

4.3.2.4 Oxygen

Typically oxygen is present under normal operating conditions. Reducing oxygen concentration to a level which will not promote combustion is one method used in industry to reduce the likelihood of an explosion occurring. It is recognized, however, that this is not often the most practical of solutions.

4.3.2.5 Confinement

Confinement is required to generate an explosion as the confinement (for example, plant building) prevents expansion of the burning coal cloud which results in production of overpressure. The maximum pressure developed is a function of the dust chemical characteristics (~7 barge for coal dust) and the strength of the enclosure. If the enclosure is weaker than the potential maximum pressure the dust can generate then the enclosure will catastrophically fail releasing all the developed pressure as a blast wave, along with hot products of combustion by way of a fireball. The consequence of such an event can be catastrophic.

4.3.3 Preventing and Mitigating Coal Dust Explosions

As noted earlier, coal dust when subdivided to the required size, can present an explosion and/or fire hazard. General handling procedures generate all requirements to satisfy the dust explosion pentagon. Ignition control is perhaps the most practical preventative technique for reducing the likelihood of a coal dust explosion during normal handling operations, since all other parameters are difficult to eliminate. Poor housekeeping can generate situations where a coal dust hazard exists without being readily apparent. Accumulations of dust outside of dust handling equipment can be sufficient the cause significant consequence if disturbed and ignited when in suspension. Examples of this could be fugitive coal dust generated during the pulverizing process which settles out on surfaces (for example, floors, rafters, elevated surfaces, and so on). Referring back to the 1999 incident in Michigan, coal dust participated as a secondary event, which became disturbed due to a primary event (that is, natural gas explosion), which contributed significantly to the resulting explosion magnitude. This type of secondary effect due to combustible dust has occurred and resulted in significant consequence across many industries (for example, Imperial Sugar 2008, Rouse Polymerics 2002) and should be recognized as a serious potential hazard.

The bowtie model illustrated in Figure 4-4 lists some of the potential hazards that can lead to a coal dust explosion on the left-hand side, and the potential consequences of a coal dust explosion on the right-hand side.

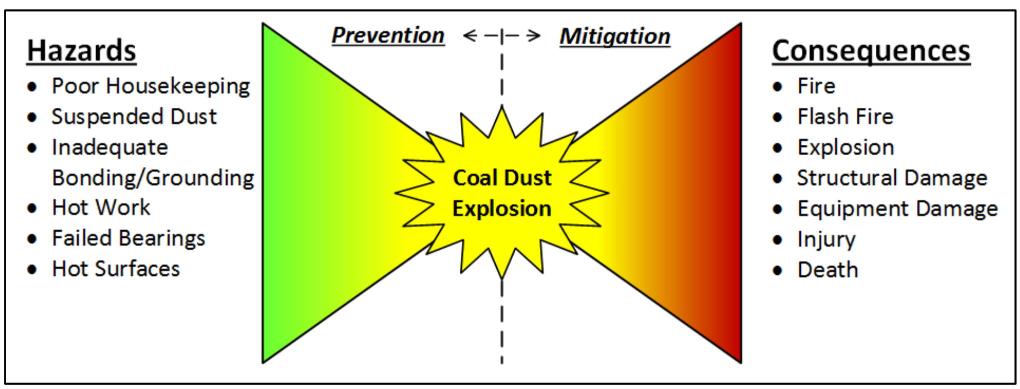

Figure 4-4
Coal Dust Explosion Bowtie Model

4.3.3.1 Reducing the Likelihood of Coal Dust Explosions

Design Features

The facility design features can be used to ***prevent or reduce the likelihood of coal dust hazards*** that can lead to a coal dust explosion:

- Engineer equipment (for example, crushers, transfer conveyors) to prevent fugitive dust emissions.
- Locate, to the extent possible, any dust accumulations in non-enclosed areas (that is, removing the confinement portion of the explosion pentagon).
- Where possible, operate in oxygen reduced atmosphere (that is, removing the oxidant portion of the explosion pentagon).
- Employing appropriate ignition control, such as electrical classification of equipment, temperature detection of bearings processing coal dust (that is, removing the ignition portion of the explosion pentagon).

Administrative Controls

The following administrative controls can be used to ***prevent or reduce the likelihood of coal dust hazards*** that can lead to a coal dust explosion:

- Implement a housekeeping plan to maintain dust accumulations in the facility below the minimum thresholds prescribed in relevant standards (for example, NFPA 654 [51]).
- Implement a preventative maintenance inspection program on all rotating and moving components that handle combustible material to identify possible friction surfaces (that is, prevent ignition).

4.3.3.2 Mitigating the Consequences of Coal Dust Explosions

Design Features

The following design features that can be used to ***mitigate the consequences*** of a coal dust explosion:

- Design occupied buildings to protect personnel from explosion (that is, to adequately withstand blast loads generated by an explosion). This includes consideration of door and window vulnerability from an explosion.
- Locate occupied buildings as far away from the hazard as practicable.
- Provide explosion venting on the process enclosure to limit the generated blast pressures and vent the products of the explosion in a controlled manner away from areas of concern. Consideration should be taken ensure the strength of overall structure can withstand the develop blast loads during venting, per NFPA 68 [52].

Administrative Controls

The following administrative controls can be used to ***mitigate the consequences*** of a coal dust explosion:

- Use of Flame retardant Clothing (FRC) for personnel working in areas with coal dust.
- Implement hot work controls within 30-ft of dust accumulations (NFPA 654 [51]).
- Implement appropriate cleaning procedures for areas with poor housekeeping (for example, not using compressed air as it creates suspended dust cloud).

4.3.4 Codes, Standards and Guidelines Related to Coal Dust Safety

The following codes, standards and guidelines can be used to inform an assessment of facility design features and administrative controls that can be used to 1) identify hazards that could lead to coal dust explosions and prevent them or reduce their likelihood, and 2) if a coal dust explosion occurs, characterize and mitigate its effects:

1. NFPA 499: "Recommended Practice For The Classification Of Combustible Dusts And Of Hazardous (Classified) Locations For Electrical Installations In Chemical Process Areas" 2013.
2. NFPA 68: "Standard On Explosion Protection By Deflagration Venting" 2013 [52].
3. EPRI 3002001229, *Dust Mitigation Methods for Coal Combustion Products*, EPRI, Palo Alto, CA; August 2013 [53].
4. OSHA Technical Information Bulletin TIB 00-11-06 "Potential for Natural Gas and Coal Dust Explosions in Electrical Power Generating Facilities" [48].
5. "Dust Explosion and Fire Prevention Handbook: A Guide to Good Industry Practices", Nicholas P. Cheremisinoff, 2014 [50].
6. NFPA 654: "Standard For The Prevention Of Fire And Dust Explosions From The Manufacturing, Processing, And Handling Of Combustible Particulate Solids" 2013 [51].
7. EPRI CS-5069, "Prevention, Detection, and Control of Coal Pulverizer Fires and Explosions EPRI, Palo Alto, CA; February 1987.
8. OSHA 29 CFR 1910.22, Housekeeping.
9. OSHA 29 CFR 1910.37, Maintenance, safeguards, and operational features for exit routes.
10. OSHA 29 CFR 1910.1200, Hazard Communication.
11. OSHA 29 CFR 1910.269, Electric Power Generation, Transmission, and Distribution (coal handling).

4.4 Toxic Releases of Anhydrous Ammonia

Most fossil generation plants have implemented some form of Selective Catalytic Reduction (SCR) and/or Selective Non-Catalytic Reduction (SNCR) technology to reduce Nitrogen Oxides (NOx) from post combustion gases. Both SCR and SNCR technologies utilize ammonia (NH3) as the reagent in the process to chemically react with NOx in the post combustion gases to reduce the nitrogen oxides to nitrogen and water. The ammonia is stored in one of three forms, 1) anhydrous ammonia, 2) aqueous ammonia, and 3) urea.

Anhydrous ammonia is widely used in SCRs. EPRI 1004148, "Reagent Storage and Handling for SCR and SNCR Systems" [35] is an excellent reference for the safe storage and handling of anhydrous ammonia. Reference [35] states that *"Anhydrous ammonia is essentially pure NH3. Commercial grade anhydrous ammonia is 99.5-99.7% pure, with a minimum water content of 0.3%. While not normally flammable, it can be combustible at concentrations of 15-28% with an ignition source 1200°F (649°C) or higher. When stored, the American National Standards Institute recommends a dilution capability of 100:1 in case of an ammonia leak."*

Anhydrous ammonia boiling point is minus 28 degrees Fahrenheit and is typically stored and transported as a liquid under pressure. Releases of anhydrous ammonia do occur in generation facilities and should be a concern of any owner/operator. This section focuses on anhydrous ammonia releases because of its highly toxic nature and widespread use.

4.4.1 Operating Experience (Multiple Industries)

In 2014, an employee was doing maintenance on a valve in an anhydrous ammonia system and there was a malfunction that resulted in a liquid ammonia release. The malfunction activated the suppression system, and the ammonia alarms were activated. Workers were able to quickly isolate the leak. One worker suffered a chemical burn to the hand. The leak occurred in the "Ammonia Farm" away from the main plant.

In 2008, an employee and coworkers were engaged in insulation work on a large anhydrous ammonia tank. The tank had been nearly emptied before work was allowed to begin. The employees were repositioning an adjustable scaffold for work the next day when a pressure relief cap was opened, releasing ammonia vapors. The employee was transported to the hospital for treatment of superficial eye and lung burns; he was released the next day. Two other coworkers were sent to the hospital for observation.

In 2007, an ammonia explosion occurred. The explosion was due to a failure of an anhydrous ammonia compressor. Two employees were injured in the explosion. Employee #1 was treated at an area hospital and released. Employee #2 was admitted to the hospital for treatment.

In 2003, an employee and a coworker filled an anhydrous ammonia nurse tank. After filling the nurse tank, the employee was hooking the tank to a pickup truck for transport when the tank ruptured along a weld seam on the bottom front side. Liquid ammonia was released through the approximate 40-in. split. The ammonia formed a cloud and a rapidly expanding, boiling-liquid blast enveloped the employee. The coworker assisted the employee to and into a water tank. The employee died 1.5 weeks later from chemical burns.

In 2003, an employee was filling a nurse tank from the bulk anhydrous ammonia tank at an ammonia plant. After the nurse tank was full, the employee disconnected the hoses from the nurse tank and was exposed to anhydrous ammonia. The exposure resulted in burn injuries to his face, neck, chest, and one eye, and injuries to his respiratory tract. The employee drove to a nearby facility a few blocks away and was taken immediately to a local hospital and transferred to a regional burn center. The employee died of complications due to chemical inhalation a few weeks later. The exposure appeared to have occurred either because the employee did not close the hose end valve before disconnecting the hose from the nurse tank, or because the safety catch did not engage when the valve was closed, and the valve handle was bumped, causing the valve to open. There was evidence that the employee applied snow to the injured areas. The required water supply had approximately one inch of ice on the surface.

Anhydrous ammonia release during transfer operations. The facility was receiving a truck load shipment of anhydrous ammonia. A transfer line ruptured while the material was being moved into a storage tank. Approximately 1,800 lbs. of anhydrous ammonia was released from the hose before the truck driver was able to get the discharge valve closed on the truck. As the liquid material exited the hose, the pressure reduction resulted in the conversion of the material from a liquid to a vapor cloud. The vapor cloud drifted off-site. A passing motorist was killed as the cloud drifted across a nearby highway. The motorist's car stalled when it entered the cloud, the motorist then left the car in an attempt escape, but was quickly overcome by the toxic fumes. An additional 14 people were treated for exposure to the fumes and seven of those were transported to a local hospital for additional treatment.

4.4.2 Anhydrous Ammonia Hazards and Toxic Release Event Characterization

Anhydrous ammonia is usually manufactured using a process which creates ammonia via the catalytic reaction of nitrogen and hydrogen under pressure and temperature. The ammonia is condensed from the reaction products and stored in a liquid form under pressure. Ammonia is delivered via tank trucks or rail cars using hoes, pipes and valves where it is transferred to one or more tanks located within or adjacent to the generation facility. Pumps, pipes and valves are used in a facility ammonia supply system that transports stored ammonia, at the appropriate pressure, to the SCR where is vaporized and injected into the post combustion gas stream (one high probability failure location is a failed gasket on the discharge side of a pump). Local pressure, temperature, flow, and level indicators, and pressure regulators are typically used by delivery operators or equipment operators to manage the ammonia supply system.

Anhydrous ammonia is stored on site in one or more tanks with amounts ranging from 10,000 gallons to over 100,000 gallons in multiple tanks depending on the unit size, required flow rates, and delivery capabilities.

The primary hazard is a vapor cloud that results from a liquid release. ANSI Standard K61.1-1999 [34] states: "At low concentration, ammonia gas is irritating to the eyes, skin and mucous membranes of the nose, throat and lungs. At higher concentrations, ammonia is corrosive to human tissue and possibly life threatening."

Reference [35] provides a further description of the hazardous effects of ammonia; "Ammonia gas and liquid can be irritating to the eyes, respiratory tract and skin due to the alkaline nature of ammonia. Breathing 1,700 to 2,500 ppm results in coughing, bronchospasm and chest pain, along with severe eye irritation and tearing. Inhaling 2,500 to 5,000 ppm ammonia causes shortness of breath, airway spasms, increased fluid in the lungs and severe chest pain. At levels above 5,000 ppm, ammonia causes chemical bronchitis, fluid accumulation in lungs, chemical burns of the skin and is potentially fatal. Permanent lung damage has not been associated with acute ammonia exposures unless the exposure concentrations are near lethal levels."

Reference [34] Table 2 lists the *"Human physiological response to various concentrations of ammonia in air"*. Power Engineering Volume 112, Issue 6, *"Safe Handling of Anhydrous Ammonia"* [38] includes a summary of the hazards to humans of ammonia exposure and is shown in Table 4-1 below.

Table 4-1
Ammonia Exposure Effects

Ammonia Exposure Effects	
Readily detectable odor.	20-50 ppm
Severe irritation of eyes, nose and throat. No lasting effect with short-term exposure.	400-700 ppm
Dangerous, less than ½ hour exposure may be fatal.	2,000-3,000 ppm
Serious edema, strangulation, asphyxia, rapidly fatal.	5,000-10,000 ppm
Immediately fatal.	> 10,000 ppm

Regulatory Requirements

This report does not include a detailed discussion of the regulatory requirements for anhydrous ammonia. Reference [35], Section 3 provides a thorough review of the regulatory issues and requirements associated with anhydrous ammonia used in SCR and SNCR systems. The following summary of regulatory requirements are from reference [35].

Anhydrous Ammonia used in SCR and SNCR systems are subject to environmental, health, and safety regulations. "Ammonia, whether in anhydrous or aqueous form, presents a hazard to plant personnel and the potential for catastrophic releases that could impact offsite areas." The regulations include those administered by the U.S. Occupational Safety and Health Administration (OSHA), the U.S. Environmental Protection Agency (EPA), and the U.S. Department of Transportation (DOT).

"SCR and SNCR reagent systems are designed to standards specific to the chemical and the operating conditions of the storage, vaporization, and injection processes. OSHA's 29 CFR Part 1910.111, Storage and Handling of Anhydrous Ammonia [39], codifies a number of design requirements for vessels and piping systems for this particular reagent. The regulation puts forth design-related requirements for containers, pumps, fittings and appurtenances, pressure relief devices, electrical systems, and placarding/signage. The regulation references a number of industry standards including ANSI K61.1 [34] and Fertilizer Institute M-1, which are specific to anhydrous ammonia systems. Similarly, the regulation includes requirements for tank motor vehicles used for ammonia transportation. Motor vehicle requirements within this regulation include extensive references to DOT standards for tank truck and unloading design and operating features."

Figure 4-5
Anhydrous Ammonia Tank Labeling

Anhydrous ammonia is regulated under two federal programs that are intended to minimize accidental releases and their consequences. The two regulations are:

- 29 CFR 1910.119, the OSHA Process Safety Management (PSM) [40] standard (1992) which applies to processes containing anhydrous ammonia in amounts of 10,000 lbs. (4536 kg) and above
- 40 CFR Part 68, the EPA Risk Management Program (RMP) [41] regulation (1996) which applies to anhydrous ammonia in quantities of 10,000 lbs. (4536 kg) and above

The OSHA PSM standard requires a Process Hazards Analysis (PHA) be conducted on the system design. And the EPA RMP regulation requires modeling a worst case scenario off site release. The OSHA standard is designed to protect plant workers, and the EPA regulation is designed for off-site protection.

Facility Siting is one of the 14 elements of the PSM standard [40]. While a Facility Siting study is performed in terms of a PHA, which may take many forms, there are now many publications available which reference API standards (for example, 752, 753) as the appropriate methods for evaluating the hazards and their potential consequences, which is covered in more detail in Section 5.

Example prevention and mitigation, design and administrative controls from the regulations are included in the bow tie discussion below.

Modeling the Consequences of an Anhydrous Ammonia Release

The primary hazard from an anhydrous ammonia release is the resulting vapor cloud. The EPA RMP requires modeling a worst case release scenario. While the EPA regulation is primarily designed to protect against an offsite release, the modeling, prevention and mitigation guidance is relevant to habitable buildings on site.

"A worst-case ammonia scenario typically shows modeled impacts to a significant downwind distance. For ammonia, the RMP rule specifies a downwind plume concentration of 200 ppmv as the threshold for potential community harm. This is termed the "toxic endpoint concentration" per the RMP rule. The 200 ppmv value for ammonia is equivalent to the American Industrial Hygiene Associations Emergency Response Planning Guideline-2 (ERPG-2). The ERPG-2 concentration is defined as the maximum concentration below which individuals could be exposed for up to one hour without experiencing irreversible or other serious health effects or symptoms that could impair their abilities to take protective action.

EPA's worst-case definition for anhydrous ammonia is the complete airborne release of the contents of the largest storage vessel over a period of 10 minutes. As an example using EPA modeling guidance, the worst-case scenario for a 12,000 gallon (45,425 liter) outdoor anhydrous ammonia vessel results in a maximum downwind distance to the 200 ppmv toxic endpoint of 4.4 miles (7 km) in rural areas and 2.8 miles (4.5 km) in urban area" [35].

Since RMP is focused on offsite impacts, the consequences predicted to onsite targets are typically very conservative. Alternative methods (for example, Section 5) using more technical based models can predict more realistic consequences for onsite personnel – which may have beneficial cost implications as mitigation may not be as extreme if less conservative consequences are predicted.

The EPA has published *"Technical Background Document for Offsite Consequence Analysis for Anhydrous Ammonia, Chlorine, and Sulfur Dioxide"*, April 1999 [44]. This guidance concerns off site exposure and can be adapted to on site exposure. The EPA has also published a model, RMP*Comp that performs the calculations described in the background document. The Dutch National Institute of Public Health and the Environment (RIVM), Centre for External Safety, has published what is known as the "Purple Book"; "*Publication Series Dangerous Substances 3, Guidelines for Quantitative Risk Analysis (Purple Book)"*, Ministry of VROM, 2005 [45].

The methods and models described in references [44] and [45], as well as the techniques and models described in Section 5, can be used to model multiple release scenarios within the plant boundaries for inhabited spaces in order to determine both the probability and consequences of a release.

The UK Health and Safety Executive, *"Methods of approximation and determination of human vulnerability for offshore major accident hazard assessment"* [46] provides a good description of estimating the level of harm from a release using the methods described in the Purple Book.

"In order to estimate the level of harm from [ammonia] it is necessary to provide a means to quantify the exposure in terms of the intensity, duration of exposure and consequences of effect. This is usually achieved by an estimation of the received dose and a comparison of this against, statistically manipulated, experimental data to determine the probability of harm to an exposed population or individual. Vulnerability criteria can be established to determine dose levels that result in specific consequences. In this guidance the indicative criteria provides:

- *The threshold of harm above which, protection is required to prevent impairment of the functions an individual requires for escape or to avoid becoming a fatality (that is, survivability)*
- *A means for the estimation of fatality probability should dose levels exceed the harm threshold and adequate protection is not present*

There are two main approaches for the determination of the effects of received dose: the use of Probit Functions and the Determination of Harmful Dose (typically applied to toxic or thermal hazards).

Probits account for the variation in tolerance to harm for an exposed population. The fatality rate of personnel exposed to harmful agents over a given period of time can be calculated by use of probit functions."

Various release scenarios should be modeled including a tank complete release, tank partial release, truck or rail car release, and hose rupture or disconnect during transfer operations with assumptions regarding quantity of release, release height, duration, and atmospheric speed and stability. Each of the release scenarios should model the indoor air concentration over time with certain mixing and infiltration assumptions for the inhabited buildings. The owner can then make decisions about prevention and mitigation based on the likelihood and consequences of an anhydrous ammonia release.

4.4.3 Preventing and Mitigating Toxic Releases of Anhydrous Ammonia

The bowtie model illustrated in Figure 4-6 lists some of the potential hazards that can lead to a toxic release of anhydrous ammonia on the left-hand side, and the potential consequences of a toxic release of anhydrous ammonia on the right-hand side.

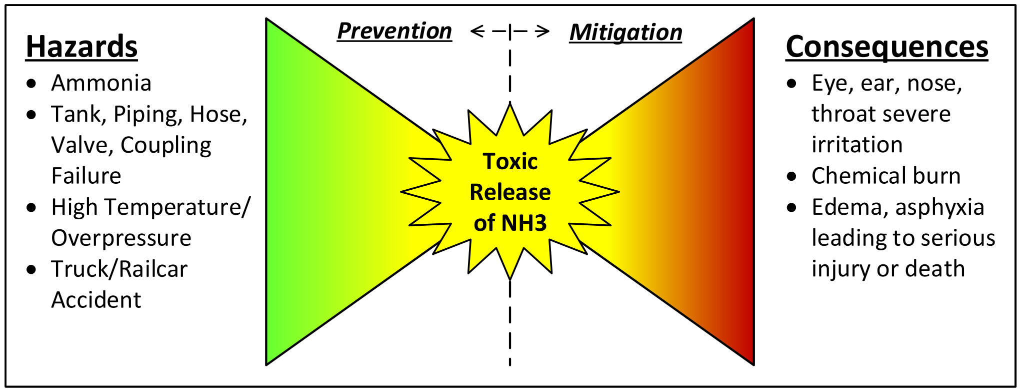

Figure 4-6
Toxic Release of Ammonia Bowtie Model

4.4.3.1 Reducing the Likelihood of Toxic Releases of Anhydrous Ammonia

Design Features

References [34], [35], [39], and [42] describe design features that are required or recommended to ***prevent or reduce the likelihood of anhydrous ammonia hazards*** that can lead to a toxic release. These references cover the design features for fixed containers, rail cars, trucks, and related piping, hoses, and other appurtenances. Examples of the types of design features to prevent or reduce the likelihood of anhydrous ammonia hazards that can lead to a toxic release are listed below (note that this list is not all inclusive; consult references [34], [35], [39], [42] for detailed standards and guidance).

- The use of mild steel ASME pressure rated vessels (ASME Boiler and Pressure Vessel Code, Section XIII) containers, piping, tubing and fittings.
- Minimum design pressure of 250 psig for containers and piping, and 350 psig for hoses with additional burst and test pressure requirements.
- The use of shut off valves, excess flow valves, and check valves in containers and transfer systems.
- The use of pressure relief valves with 2X capacity that are in direct communication with the container vapor space and meet the applicable requirements of ASME UG-125(c)(3); UL-132 *Standard on Safety Relief Valves for Anhydrous Ammonia and LP Gas*, and vented away from the container, upward, and unobstructed to the atmosphere unless connected to a control device.
- Filling density of tanks limited to prevent completely filling with liquid as measured by level, with internal liquid temperature measurement, to correct the amount of vapor and liquid corrected to 60°F.
- The use of liquid level gauges and fixed maximum level gauges.

- Emergency shutoff or backflow check valves in liquid and vapor fixed piping of transfer system. Installed so that a break due to pull-away will occur on hose or swivel type piping side (not fixed piping side).
- Emergency shutoff valve with manually and/or automatically activated shutoff from a remote location and at the installed location.
- Use of approved bulkheads and breakaways at truck unloading stations.

Administrative Controls

References [34] through [43] describe administrative controls that are required or recommended to ***prevent or reduce the likelihood of anhydrous ammonia hazards*** that can lead to a toxic release. Examples of the types of administrative controls to prevent or reduce the likelihood of anhydrous ammonia hazards that can lead to a toxic release are listed below (note that this list is not all inclusive; consult references [34] through [41] for detailed standards and guidance).

- Develop and implement the preventive measures from the 14 element OSHA Process Safety Management (PSM) program [40]:

  1. **Process safety information.** Written process safety information including information on the hazardous nature of ammonia, information on the technology of the process, and information on the equipment in the process.
  2. **Process Hazard Analysis (PHA)**. Conduct a PHA and identify, evaluate, and control the hazards associated with the entire system/process.
  3. **Operating Procedures**. Develop written operating procedures that include step-by-step procedures and operating limits for each operating phase (for example, initial startup, normal operations).
  4. **Employee Participation**. Develop a written plan of action to consult with employees and their representatives on the conduct and development of process hazard analyses and on the development of the other elements of process management.
  5. **Training**. Any person required to handle, transfer, transport, or otherwise work with ammonia shall be trained to understand the properties of ammonia, to become competent in safe operating practices, and to take appropriate action in the event of a leak or emergency.
  6. **Contractors**. Special provisions for contractors and their employees to emphasize the importance of everyone taking care that they do nothing to endanger those working nearby who may work for another employer.
  7. **Pre-Startup Safety Review**. Perform a pre-start-up safety review for new and modified facilities to assure that the design and construction is in accord with the design specifications.
  8. **Mechanical Integrity**. Develop written procedures for inspection and testing that must be performed on process equipment, using procedures that follow recognized and generally accepted good engineering practices.

9. **Hot Work Permit**. A permit must be issued for hot work operations conducted on or near an anhydrous ammonia process.
10. **Management of Change**. Develop written change management procedures for any change to the anhydrous ammonia system or process with considerations addressed prior to the change that include the technical basis for the proposed change, impact of the change on employee safety and health, modifications to operating procedures, necessary time period for the change, and authorization requirements for the proposed change.
11. **Incident Investigation**. Develop written procedures for investigation of incidents to identify the chain of events and causes so that corrective measures can be developed and implemented.
12. **Emergency Planning and Response**. Mitigation measure.
13. **Compliance Audits**. Employers must certify that they have evaluated compliance with the provisions of PSM at least every three years.
14. **Trade Secrets**. Make all information necessary to comply with the PSM to those persons who need the information, without regard to proprietary information.

- Transfer of ammonia shall be continuously monitored from the first time the connections are made until the connections are terminated, by a trained operator either on site, remotely, or electronic means such as a video camera.
- Require that the attendant conduct a walk-around inspection once transfer is completed. Attendant should walk around tanks and storage containers and ensure that hosing has been uncoupled and secured and that all steps of the transfer operation are complete.

4.4.3.2 Mitigating the Consequences of Toxic Releases of Anhydrous Ammonia

Design Features

References [34] through [43] describe the design features that are required or recommended to ***mitigate the consequences of a toxic release of anhydrous ammonia***. Examples of the types of design features to mitigate the consequences of a toxic anhydrous ammonia release are listed below (note that this list is not all inclusive; consult references [34] through [43] for detailed standards and guidance):

- Emergency water spray or fog suppression systems with adequate volumes of water to absorb ammonia vapor and reduce the vapor cloud.
- Spill containment around loading, transfer, and storage areas.
- Leak detection, alarms, and both manual and automatic isolation systems.
- Positive pressure HVAC system and structure design for a building or specific room. The room must be capable of being isolated and sealed, or has a source of clean air. Trip and isolation of space, or automatic switch to clean air source based on pre-determined ammonia detection limit. May include the control

room (and other inhabited buildings) or a designated shelter in place. NFPA 496, "Standard for Purged and Pressurized Enclosures for Electrical Equipment", 2013 Edition [47] provides guidance for the design of pressurized enclosures, and chapter 7 specifically addresses control rooms. While intended for fire protection, the design guidance can easily be applied. The clean air source may include an intake that is not located in the path of the vapor plume, filtered, or a tank. The design should be based on the ammonia release and infiltration models that the owner wishes to protect against.

- Modify a room or series of rooms as a shelter in place with a kit to seal the room with an optional installation of source(s) of clean air. Best case is a room with no windows, single door with gaskets, and all six sides finished to prevent infiltration of ammonia vapor. Sealing kit includes plastic sheeting, gasket material, and duct tape.
- Containers located sufficiently distant from occupied buildings such that the vapor cloud from a release minimizes or eliminates exposure.

Administrative Controls

References [34] through [43] describe administrative controls that are required or recommended to ***mitigate the consequences of a toxic release of anhydrous ammonia***. Examples of the types of administrative controls to mitigate the consequences of a toxic anhydrous ammonia release are listed below (note that this list is not all inclusive; consult references [34] through [43] for detailed standards and guidance).

- Full face gas masks with ammonia canisters for concentrations up to 300 ppmv (the Immediately Dangerous to Life and Health IDLH limit) of ammonia for short durations, less than 30 minutes.
- Positive Pressure Self-Contained Breathing Apparatus (SCBA) for concentrations above 300 ppmv.
- BakerRisk, a contributor to this report, recommends that any facility that handles NH3 equip all operators with 5 or 10 min escape packs. They are on person at all times and have proved very beneficial in emergencies. During initial panic of a release, BakerRisk has encountered many casualties due to personnel attempting to locate a face mask/SCBA station and inadvertently proceeding into areas of greater gas concentration. While escape packs are no substitution for face masks/SCBA, implementation of escape packs is relatively inexpensive but requires a training, management and inspection program to ensure workers understand their importance and they are on personnel at all times.
- Positive pressure air supply manifold with breathing apparatus in occupied spaces.
- Protective clothing including gloves, boots, pants, and jacket.
- Easily accessible emergency shower and plumbed eye wash unit with at least 150 gallons of clean water in an open topped container.

- Pre-defined evacuation limits and procedures with egress paths.
- Develop and implement the mitigation measures from the 14 element OSHA Process Safety Management (PSM) program [40]:
    1. (No. 13) Emergency Planning and Response. (Mitigation measure) Develop an emergency action plan for the entire plant for emergency pre-planning and training to make employees aware of, and able to execute, proper actions in the event of a release. Employers covered under PSM also may be subject to the OSHA hazardous waste and emergency response regulation (29 CFR 1910.120(a), (p), and (q). Emergency Plan includes coordination with local and state emergency response organizations.

4.4.4. Codes, Standards and Guidelines Related to Anhydrous Ammonia Safety

The following codes, standards and guidelines can be used to inform an assessment of facility design features and administrative controls that can be used to 1) identify anhydrous ammonia hazards that could lead to toxic releases and prevent them or reduce their likelihood; and 2) if a toxic release occurs, characterize and mitigate its effects:

1. ANSI Standard K61.1-1999, American National Standard Safety Requirements for the Storage and Handling of Anhydrous Ammonia [34].
2. EPRI 1004148, *Reagent Storage and Handling for SCR and SNCR Systems*, EPRI, Palo Alto, CA; May 2002 [35].
3. EPRI 1004024, *Operating and Maintenance Guidelines for Selective Catalytic Reduction Systems*, EPRI, Palo Alto, CA; December 2001 [36].
4. EPRI 1004054, *Reagent Delivery Systems for SCR and SNCR Systems*, EPRI, Palo Alto, CA; February 2002. [37].
5. Power Engineering Volume 112, Issue 6, "Safe Handling of Anhydrous Ammonia" [38].
6. 29 CFR 1910.111, "Storage and Handling of Anhydrous Ammonia" [39].
7. 29 CFR 1910.119, "Process Safety Management of Highly Hazardous Chemicals" [40].
8. US EPA, "General Guidance on Risk Management Programs for Chemical Accident Prevention Provisions (40 CFR Part 68)" [41].
9. OSHA SHIB 12/05/05, "Preventing the Uncontrolled Release of Anhydrous Ammonia at Loading Stations" [42].
10. OSHA 3132, "Process Safety Management" [43].
11. US EPA, "Technical Background Document for Offsite Consequence Analysis for Anhydrous Ammonia, Chlorine, and Sulfur Dioxide", April 1999 [44].

12. Publication Series Dangerous Substances 3, Guidelines for Quantitative Risk Analysis (Purple Book), Ministry of VROM, 2005 [45].
13. The UK Health and Safety Executive, “Methods of approximation and determination of human vulnerability for offshore major accident hazard assessment” [46].
14. NFPA 496, “Standard for Purged and Pressurized Enclosures for Electrical Equipment”, 2013 Edition [47].

Section 5: Petroleum Refining and Chemical Industry Risk Analysis Methods

This section, provided by BakerRisk, describes risk analysis methods in the petroleum refining and chemical industries for the purpose of showing how another industry approaches the problem of potential hazards that can lead to events, which in turn can lead to harmful consequences. In some cases, the fossil generation industry faces the same potential hazards, and the approaches described herein could be extended to the fossil generation industry. This section is not necessarily intended to provide guidance for fossil generation facilities; however, an owner/operator may find some useful principles and methods that could be applied to specific issues within a given facility.

5.1 Evaluating Catastrophic Risk

Major accidents that have occurred in the refining and chemical industries have highlighted the dangers to onsite personnel. Occupied buildings (including control rooms and/or control complexes) at these facilities are often located close to the processing areas to facilitate operations and communications and provide operators with an optimal location for observing and responding to events. Unfortunately, the closer the operators are to the processing areas increases their risk of exposure to the consequences of hazardous events.

Catastrophic events in the refining and chemical industries are typically associated with hazardous materials that may cause toxic exposure from unintentional chemical releases, thermal radiation exposure from fires or blast overpressure effects due to vessel ruptures or vapor cloud explosions. Table 5-1 demonstrates that over the last 40 years there have been numerous events resulting in significant vulnerability to people (as well as structures and equipment). It is noted that this is a representative sample of some high profile publicized events and is not intended to be comprehensive.

Table 5-1
Historical List of Major Industrial Events

Date	Location	Facilities	Description
2006	Danvers, MA	0	Heptane and alcohols
2005	Texas City, TX	18	Pentane/hexane release
2005	Point Comfort, TX	0	Propylene release
2002	Pascagoula, MS	0	Mononitrotoluene release
1999	Allentown, PA	5	Hydroxylamine decomposition
1998	Mustang, NV	4	High explosives
1992	La Mede, France	6	LPG Leak
1989	Pasadena, TX	23	Isobutane and ethylene release
1988	Norco, LA	7	Propane leak
1984	Mexico City	542	LPG line rupture
1978	Texas City, TX	7	Isobutane sphere failure
1974	Flixborough, UK	28	Cyclohexane release

5.2 Refining and Chemical Industry Event Characteristics

The handling of hazardous materials in any industry can result in significant consequences when deviations from normal operating conditions occur. The following subsections describe some of the events that can result from hazardous materials in a petroleum refining or chemical facility:

5.2.1 Explosions

Industrial explosions can range from vapor cloud explosions (VCEs) to bursting pressure vessels (BPVs), boiling liquid expanding vapor explosions (BLEVEs), condensed phase chemical explosions, reactive chemical explosions, and dust explosions, to name a few. If an explosion occurs in close proximity to an occupied building (for example, control room) and the building is not designed to withstand the maximum credible event (MCE), then occupant vulnerability should be expected.

Vapor cloud explosions are typically the dominant explosion scenario in refineries and chemical plants. However, for the fossil fuels /power generation industry, steam boiler explosion hazards may be more typical. Some of the hazards and related events inherent to the fossil generation industry are discussed in greater detail in Section 4.

5.2.2 Fires

Fire hazards can result from a release of high pressure gaseous material (jet fire), or through loss of containment of a combustible liquid (pool fire). Owner/operators should establish procedures to evacuate occupants from a building or provide a building that meets the criteria for a "shelter-in-place" (SIP). When designing a building system to serve as a fire SIP, the criteria to consider includes temperature rise in the building, ingress and ignition of flammable material, and ingress of smoke and flames. Windows in particular can be the most vulnerable structural component failing at relatively low thermal thresholds and durations. Ingress of potentially flammable vapor concentrations into a building can result in fire and explosion hazards for building occupants. NFPA 496 [54] provides guidance for internal building pressurization to reduce the likelihood of such hazards.

5.2.3 Toxic Releases

For a toxic release, the owner/operator should choose to either develop procedures to safely evacuate occupants or provide a building that meets toxic SIP criteria for a toxic material release. HVAC systems must be designed such that upon detection of toxic (or flammable) vapors, the HVAC unit either shuts down or goes into recirculation mode. The infiltration of a toxic material is highly dependent on the relative "tightness" of the building envelope. NFPA 496 [54] can also provide mitigation guidance for preventing toxic ingress into buildings.

5.3 Refining and Chemical Industry Governance and Guidelines

In 1992, the Occupational and Safety Health Administration (OSHA) began the enforcement of a standard called "Process Safety Management of Highly Hazardous Chemicals," with the expressed intent of reducing the number of hazardous incidents at these facilities. Specifically, facility siting was assigned as part of a facility's process hazards analysis (PHA) requirement. Facility siting is the process of managing risk to personnel from explosions, fires, and toxic material releases by identifying hazards that can affect occupied buildings, evaluating potential consequences of those hazards, and developing means to manage the risks presented by those hazards. In response to OSHA's requirement, various industry guidelines and best practice documents have been developed to provide facility siting methodologies, including:

- American Petroleum Institute (API) Recommended Practice (RP) 752, "Management of Hazards Associated with Location of Process Plant Permanent Buildings" First Edition: 1995, Second Edition: 2003, Third Edition: 2009
- API Recommended Practice 753, "Management of Hazards Associated with Location of Process Plant Portable Buildings" First Edition: 2007

- API Recommended Practice 756, “Management of Hazards Associated with Location of Process Plant Tents” First Edition: 2014
- Center for Chemical Process Safety (CCPS), “Guidelines of Evaluating Process Plant Buildings for External Explosions and Fires” First Edition: 1996, Second Edition: 2012

5.4 API Recommended Practice 752

Because this report is about the topic of MCR survivability and hardening, the remainder of this section is focused on permanent buildings following the guidance put forth in API RP 752. Similar guidance is provided for portable structures and tents in API RP 753 and API RP 756, respectively.

RP 752 provides guidance for managing the risk from explosions, fires, and toxic material releases to on-site personnel located in new or existing permanent buildings intended for occupancy. This RP was developed for use at refineries, chemical operations, natural gas liquids extraction plants, natural gas liquefaction plants, and other onshore facilities covered by OSHA 29 CFR 1910.119 [40] and serves as the industry guidance document for performing a Facility Study (FS). Buildings covered by this RP are rigid structures intended for permanent use in fixed locations.

5.4.1 Guiding Principles

API RP 752 is based on the following guiding principles:

1. Locate personnel away from process areas consistent with safe and effective operations.
2. Minimize the use of buildings intended for occupancy in close proximity to process areas.
3. Manage the occupancy of buildings in close proximity to process areas.
4. Design, construct, install, modify, and maintain buildings intended for occupancy to protect occupants against explosion, fire, and toxic material releases.
5. Manage the use of buildings intended for occupancy as an integral part of the design, construction, maintenance, and operation of a facility.

5.4.2 Risk Assessment Methods

There are three basic assessment methods described by API RP 752:

1. Facility Study method (a deterministic, “consequence-based” approach)
2. Quantified Risk Assessment method (a “risk-based” approach)
3. Spacing-Tables method

While practical guidance is provided in API RP 752 for the Facility Study method, guidance on understanding how to execute QRA and Spacing Table methods is not provided in the RP since this guidance can be obtained elsewhere [55], [56].

API RP 752 recommends consideration of MCEs, which are defined as a hypothetical explosion, fire, or toxic events that generate maximum consequence to the occupants of a particular building. An MCE should represent a realistic event with a reasonable probability of occurring during the lifetime of the facility. For example, a realistic MCE for most refining or chemical facilities is usually a failure of a major transfer line or failure of a flange gasket. Each building should have its own set of MCEs.

Per API RP 752, documentation for the Facility Study is required to include the following:

1. Description of the assessment approach used
2. The basis for the scenario selection used in the study
3. Description of the analysis methodology used in the study
4. Applicability of analysis methodology used in the study
5. Data sources used in the analysis
6. Applicability of data sources
7. Building siting criteria
8. Results
9. Documentation of prioritized mitigation plans (for existing facilities)

API RP 752 further defines how occupancy criteria is determined using the "intention for occupancy" guidance. If a building has personnel assigned to it, or a building is utilized on a recurring basis, it is considered to be "intended for occupancy" and it must therefore be included in the study. Buildings that are not intended for occupancy can be evaluated on a case-by-case basis, such as smoke shacks and storm shelters.

5.4.2.1 Facility Study Screening Assessment

Initially, the Facility Study approach take a consequence-based view to immediately "screen" which buildings are of particular concern. This approach takes into consideration the MCEs that could lead to explosions, fires, or toxic releases. Upon selection of the MCEs, a comprehensive list of hazard scenarios, along with all the required data, is taken to the consequence analysis stage. Hazard levels are selected for:

- **Blast Loading**. Overpressure generated from an explosion should take into consideration how injuries could be sustained. Very low overpressures can shatter standard windows, potentially causing injury to surrounding personnel. A high overpressure can cause structural damage that could result in building collapse and potential fatality to building occupants. Very high levels of overpressure are required to cause fatalities, but lower levels can produce serious or fatal injuries when people are thrown against equipment.
- **Radiant Heat from Fires**. For people outside, injury and fatality from heat exposure is a function of exposure time based on how long it might take someone to escape or reach a safe haven. Typical values are 5 kW/m^2 for injury and 12.5 kW/m^2 for death [57]. When considering heat exposure hazards, jet fires, pool fires, and flash fires should be considered. Flash fires outside enclosures are typically of short duration. Assessment thereof can provide guidance for areas where appropriate personal protective equipment (for example, flame retardant clothing) should be required. For personnel inside enclosures, occupant vulnerability values due to thermal impacts (jet/pool fires) may be assessed using a probit equation and data for lethality due to exposure to fireballs [57].
- **Toxic Exposure**. The response of humans to toxic exposure is extremely complex and difficult to model. A number of simple concentration-dependent data also exist; for example, a number of authorities have published "Immediately Dangerous to Life and Health" (IDLH) [58] thresholds and Emergency Response Planning Guidelines (ERPG) [59]. Other available data include lethal concentration (LC) and lethal dose (LD) data, usually expressed in terms of a particular percentage of fatality for specified exposure duration and can be found on most Material Safety Data Sheets (MSDS). Probit equations may also be used combined with data from experimental studies [60], [61], [62].

For both toxic and thermal hazards, the Facility Study should consider building internal environmental degradation (that is, when it may be unable to support life) as a result of the event. It is therefore important to consider influences such as HVAC, positive air pressure, temperature rise inside or ignition of building, ingress of flammable or toxic vapors, ingress of smoke and fumes, or thermal radiation impact to personnel located near windows or personnel who choose to evacuate. The Facility Study approach is discussed in more detail in Appendix B.

5.4.2.2 Quantitative Risk Analysis (QRA) Approach

A QRA utilizes some of the same steps as a Facility Study (hazard identification, identification of MCEs, consequence analysis, and so on), but goes further by including the *frequency* of a given event as part of the risk-based approach. QRAs typically include the following primary tasks:

1. Identify plant buildings, construction type, and population
2. Identify credible hazard scenarios (including MCEs)
3. Determine consequence of event
4. Determine frequency of event
5. Determine vulnerability of occupants
6. Calculate risk to an individual
7. Calculate the aggregate risk to building occupants
8. Compare calculated risk with company's risk-acceptance criteria

The critical factor in a quantitative risk analysis is to apply a frequency to the hazard scenarios, and therefore determine the risk. A simplified risk equation could be represented by the following equation, which is the same concept presented in Figure 3-2:

Risk = Consequence x Frequency

Multiplying the consequences of the hazards with a calculated frequency determines the risk. Typically, both individual and societal/aggregate risk results are modeled. Results are generated for daytime and nighttime populations plus a combined average. The QRA approach allows a variety of results to be generated, which enables detailed analysis and understanding of the facility siting risks involved. Additional onsite risk statistics can also be calculated showing the highest individual risk and offsite societal risk along with aggregate risk. Typical risk results, as defined by CCPS [56], are as follows:

- **Individual Risk**. This is the risk to a person in the vicinity of a hazard. This includes the nature of the injury to the individual, the likelihood of the injury occurring, and the time period over which the injury might occur. This can be displayed graphically or numerically.
- **Societal Risk**. Societal risk measures the risk to a group of people. Societal risk measures estimate of both the potential size and likelihood of incidents with multiple adverse outcomes. For example, the typical adverse outcome considered is immediate fatality resulting from fire, explosion, or exposure to toxic vapors. Societal risk results can be presented graphically or numerically.
- **Aggregate Risk**. Facility siting commonly uses aggregate risk as a tool for managing the risk associated with occupied buildings in a process plant. Aggregate risk can be defined as *societal risk applied to a specific group of people within a facility*.

The QRA approach is also discussed in more detail in Appendix B.

5.4.2.3 Spacing Tables Approach

The Spacing Tables approach uses established tables to determine minimum separation distances between equipment and buildings intended for occupancy. It is briefly described here because it is part of API RP 752. It is not described in detail in Appendix B because of it is limited to fire hazards only.

Industry groups, insurance associations, regulators, and owner/operator companies have developed the experience-based spacing tables for minimum building spacing from specific equipment. Scenario selection is not required when using experience-based fire spacing tables and these fire-specific tables are not appropriate for building siting evaluations for explosions and toxic material releases. However, other indices exist for explosions and toxics but they are extremely qualitative. For example, Dow's Fire & Explosion Index [63] and the Mond Index [64] are intended for explosion assessments. Spacing tables may be found in various references including CCPS [56].

5.5 Extending the Catastrophic Risk Evaluation Approach to the Fossil Generation Industry

A skeptic might think that hazards in fossil generation facilities are fundamentally different from those found at refining or chemical facilities, or that design features or administrative controls in a fossil generation facility are more robust than those found in a refining or chemical facility, therefore requiring a much greater deviation to result in an event. But skeptics should also consider that:

- Many potential hazards are identical or very similar in both types of facilities, including (but not limited to):
  - Flammable gases and liquids (for example, high pressure natural gas, hydrogen cooled turbine generators)
  - Toxic materials (for example, ammonia)
  - Combustible dusts (for example, pulverized coal)
  - High pressure steam
- Both types of facilities generally use the same types of passive equipment (for example, pipes, tanks, pressure vessels, structures, and so on) and active equipment (for example, breakers, valves, pumps, and so on)
- The event sequences are generally the same in both types of facilities (for example, a release of hydrogen coupled with an ignition source leads to an explosion, and in the end, harm to unprotected people and equipment)

As noted in Section 5.1, handling of flammable gases and liquids, combustible dusts, and toxic materials can generate significant events if they are not adequately controlled. The U.S. Department of Labor has published a Technical Information Bulletin [65] that references a 1999 event in which an explosion at a power plant in Middletown, Connecticut killed six workers and caused 14 serious injuries. Findings from the investigation indicated that a primary explosion occurred due to natural gas buildup in a furnace which, when ignited, caused a secondary explosion from coal dust. The bulletin recommends owner/operators follow specific National Fire Protection Association (NFPA) standards that focus primarily on care, maintenance and operating procedures to prevent the primary event. Interestingly, the bulletin does not specifically address mitigation of the secondary (coal dust) explosion which likely caused which likely contributed significantly to the resulting consequence in this particular incident. However, NFPA 654 [66] does provide guidance for preventing combustible dust explosions, with housekeeping measures as the primary focus.

For the most part, these NFPA standards and guidelines address equipment-specific issues, such as the potential for an explosion within a boiler. But what if the natural gas line serving the boiler furnace is severed and a release of flammable gas is emitted into the facility? How is the consequence of a resulting fire or explosion evaluated in terms of consequence to operators in a control room? The issue with adopting and following prescriptive guidelines and standards alone is that it can lead to a false sense of security to the owner/operator. That is, there is often a perception that by simply following these guidelines, they will prevent and/or manage all operating hazards.

While there is inherent value in adopting and following industry standards and guidelines, the process of managing the implementation of the prescriptive measures is often difficult, and particularly for larger corporations, can incur significant cost. Furthermore, a heavy dependence is often placed on administrative tasks (for example, operator intervention, response to control alarms) to manage most of the risk. This dependence on administrative controls introduces the potential for human error, which is a well-documented phenomenon, and in many cases, a small deviation from the prescriptive methods outlined in a given standard or guideline can have significant repercussions.

Therefore, a more holistic approach is recommended that includes assuming the worst-case event *does* occur, using a Facility Study approach to screen for potential consequences, and using a QRA approach to quantify and assess the risk to people, equipment and structures. Both approaches are described in detail in Appendix B.

Section 6: Conclusions and Recommendations

6.1 Conclusions

This report describes the results of interviews with EPRI members, a literature search, and some input by domain experts in the fossil generation, petroleum refining, and chemical industries. This report is not a guideline, nor does it provide detailed guidance for 1) systematically identifying and assessing the full range of hazards that may be found in fossil generation facilities, 2) assessing the survivability due to significant events in such facilities, or 3) hardening a facility to improve survivability when a significant event occurs.

Instead, this report describes a way to systematically consider 1) some potential hazards in fossil generation facilities, 2) some events that could result from hazards, even if their likelihood is very low, and 3) some of the potential consequences of events, including injury or death, if the effects of those events are not adequately limited or controlled.

This report demonstrates that some potential hazards exist in fossil generation facilities, events do happen, and events have consequences that can challenge survivability. The good news is that in many cases, existing or proposed design features and/or administrative controls can prevent or reduce the likelihood of a hazard leading to an event, as well as design features and/or administrative controls that can mitigate the consequences of an event. Thus, means are available for both preventing and mitigating events, and if they are effectively applied and maintained, survivability can be reasonably assured, and if necessary, improved significantly.

The end result is a report that can be used by EPRI members concerned about surviving significant events. EPRI members can consider potential hazards, potential events, and potential consequences within their own facilities. Four specific events were selected to illustrate these concepts, and the literature search turned up a number of references that EPRI members can use to perform their own assessments of these specific types of events. In addition, information provided by experts (BakerRisk) in the petroleum refining and chemical industries as cross-sector input includes a description of qualitative and quantitative risk assessment methods and how they can be extended to the fossil generation industry.

For some types of events, such as hydrogen explosions or toxic ammonia releases, event modelling is necessary to fully understand the consequences. For other types of events, such as turbine wrecks that can throw missiles, a qualitative approach may be sufficient (for example, simply examining whether or not the steam turbine is in a favorable orientation as discussed in Section 4.2.3.2).

6.2 Recommendations

6.2.1 Systematically Identify and Rank Typical Hazards in Fossil Generation Facilities

EPRI members interviewed for this project were asked if potential hazards were listed and ranked for their facilities. The result is that most hazards are more or less understood, but there is no clear list or ranking in terms of their likelihood of leading to an event, or their relative significance. In some cases, interviewees reported certain hazards or events of personal interest (such as steam line breaks or hydrogen explosions), but their responses were based on personal experience.

The list of hazards and related events provided in Table 3-1 is only anecdotal. Additional research within and among several operating facilities could be performed to systematically identify and rank typical hazards. The research would use facility design information, as well as walkdowns at each participating facility and/or interviews with engineering, operations and maintenance personnel. The research would briefly identify and characterize hazards, the potential events due to those hazards, and their potential consequences. Consider the following criteria for identifying and ranking hazards, using anhydrous ammonia as an example:

- Hazard type and magnitude (how many pounds of stored anhydrous ammonia?)
- Existing models or assessments that characterize hazards, events, and consequences (if you store more than 10,000 pounds of ammonia, what does your Process Safety Management (PSM) program say about it?)
- Existing design features to prevent events (where and how is the ammonia stored? How is it delivered from the storage location to endpoint devices?)
- Existing administrative controls to prevent events (what procedures are used to transfer ammonia?)
- Existing design features to mitigate event consequences (how are ammonia releases detected? What barriers are in place between people and the likely paths of an ammonia release?)
- Existing administrative controls to mitigate event consequences (what do you do when you detect an ammonia release?)

If hazards can be systematically identified and ranked in terms of their likelihood of leading to an event, or the potential consequences of related events, then detailed guidance could be targeted and developed for preventing and/or mitigating events due to the highest ranked hazards.

6.2.2 Perform a Facility Study and QRA Demonstration Project

The Facility Study and Quantitative Risk Assessment (QRA) methods described in Section 5 and Appendix B could be applied on a demonstration project at an existing fossil generation facility. Specific hazards or events of interest could be identified using the results of the recommendation described above.

A demonstration project would start by identifying one or more specific hazards of interest, then perform a Facility Study to characterize the potential consequences of maximum credible events, then perform a QRA to characterize the risks due to the selected hazards and related events. The deliverable would include recommendations for improving survivability.

6.2.3 Revise this Report to Include Additional Hazards and Events

The first two recommendations described above (especially the Facility Study and QRA) would provide EPRI members with detailed technical information and guidance related to specific hazards, events, and survivability. But if they are not pursued, and EPRI members find the initial results provided in this report to be helpful as-is, then Section 4 could be expanded to include information about additional hazards and events. Interviews with interested members would be performed to identify which additional hazards and related events to include.

6.2.4 Improved Use of Operating Experience

While some operating experience reports within the fossil generation sector were found in the public domain, they are scant and do little to convey the causes of reported events. In addition, EPRI members and other domain experts interviewed for this project said that there is no effective or formal means for reporting and sharing operating experience events and their causes within the fossil generation sector.

The fossil generation sector could benefit from sharing their operating experience related to hazards, events (including near misses), the consequences of events, and most importantly, the causes of events and measures to prevent their recurrence. A means for reporting and sharing event information should be developed that meets the guidance of EPRI 1012783 [69].

Section 7: References

1. API 752 “Management of Hazards Associated With Location of Process Plant Buildings”.
2. API 753 “Management of Hazards Associated With Location of Process Plant Portable Buildings”.
3. API 500 “Recommended Practice for Classification of Locations for Electrical Installations at Petroleum Facilities”.
4. OSHA “Process Safety Management of Highly Hazardous Chemicals”, 29 CFR 1910.119.
5. NFPA 654: "Standard for the Prevention of Fire and Dust Explosions from the Manufacturing, Processing, and Handling of Combustible Particulate Solids.”
6. NFPA 496: “Standard for Purged and Pressurized Enclosures for Electrical Equipment”, 2013.
7. FEMA 453, “Design Guidance for Shelters and Safe Rooms”, May 2006.
8. NFPA 850, “Recommended Practice for Fire Protection for Electric Generating Plants and High Voltage Direct Current Converter Stations”, 2010.
9. ISO 11064, “Ergonomic Design of Control Centres, Parts 1–7”, 1999–2013.
10. OSHA Safety and Health Information Bulletin (SHIB) 07-31-2005, “Combustible Dust in Industry: Preventing and Mitigating the Effects of Fire and Explosions”.
11. OSHA Technical Information Bulletin TIB 00-11-06 “Potential for Natural Gas and Coal Dust Explosions in Electrical Power Generating Facilities”.
12. U. S. Chemical Safety and Hazard Investigation Board (US CSB) “*Urgent Recommendations*”.
13. OSHA 3132, “Process Safety Management” 2000.
14. OSHA 3133, “Process Safety Management – Guidelines for Compliance”.
15. 29 CFR 1910.119, “Process Safety Management of Highly Hazardous Chemicals”.
16. 29 CFR 1910.269, “Electric Power Generation, Transmission, and Distribution”.

17. "Engineering a Safer World – Systems Thinking Applied to Safety," by Dr. Nancy G. Leveson; MIT Press, Cambridge MA; ISBN 978-0-262-01662-9.

18. "Hydrogen Safety" (http://en.wikipedia.org/wiki/Hydrogen_safety).

19. "Muskingum River Plant Hydrogen Explosion January 8, 2007," (http://web.archive.org/web/20080409155509/http:/www.eei.org/meetings/nonav_2007-04-29-cs/Citations_Accident_Review.pdf).

20. High-Altitude Electromagnetic Pulse (HEMP): A Threat to Our Way of Life," by William A. Radasky, Ph.D., P.E.; IEEE-USA Today's Engineer Online, 2008 (http://www.todaysengineer.org/2007/Sep/HEMP.asp).

21. ANSI/AIAA G-095-2004, "Guide to Safety of Hydrogen and Hydrogen Systems," American Institute of Aeronautics and Astronautics (AIAA), 1801 Alexander Bell Drive, Reston, VA 20191 (ISBN: 1-56347-675-4 (hardcopy).

22. "Steam Turbine Failure During Overspeed Test" (https://www.scribd.com/doc/61342541/Duvha-2011-Overspeed-Testing-Failure-V2).

23. ANSI/ISA 77.14.01-2010, "Fossil Fuel Power Plant Steam Turbine Controls".

24. API Std. 670, 4th Edition, "Machinery Protection Systems," American Petroleum Institute, December, 2000.

25. EPRI 1013461, *Turbine Overspeed Trip Modernization – Requirements and Implementation Guidance*, Final Report; EPRI, Palo Alto, CA; November 2006.

26. NUREG-1275, Volume 11, "Operating Experience Feedback Report – Turbine – Generator Overspeed Protection Systems," US NRC, April 1995.

27. EPRI NP-2429-LDV1, *Steam Turbine Disc Cracking Experience – Volume 1: Literature and Field Survey*, Final Report, EPRI, Palo Alto, CA, June 1982.

28. "Structural Integrity of Large Steam Turbine Rotors," Rogers, Wells & Johnson; Proceedings of the Twelfth Turbomachinery Symposium, 1983; Texas A&M University http://turbolab.tamu.edu/proc/turboproc/T12/T1231-44.pdf).

29. "Rotating Equipment Loss Prevention – An Insurer's Viewpoint," Clark, Proceedings of the Twenty-Fifth Turbomachinery Symposium, 1997; Texas A&M University (http://turbolab.tamu.edu/proc/turboproc/T25/T25103-122.pdf).

30. TIL-1904 Booklet, by Structural Integrity Associates, Inc. (http://www.structint.com/files/TIL1904_Booklet.pdf).

31. Regulatory Guide (RG) 1.115, Revision 2, "Protection Against Turbine Missiles" US NRC, January 2012.

32. EPRI 1009665, *Guidance for Performing a Simplified Risk-Informed Turbine Missile Analysis*, EPRI, Palo Alto, CA; March 2005.

33. "Coupling Credible Failure Modes and Owner Options to Intervene," by Locke, et al; Proceedings of the Fort-Second Turbomachinery Symposium, 2013; Texas A&M University (http://turbolab.tamu.edu/proc/turboproc/T42/LectureT08.pdf).

34. ANSI Standard K61.1-1999, American National Standard Safety Requirements for the Storage and Handling of Anhydrous Ammonia.

35. EPRI 1004148, *Reagent Storage and Handling for SCR and SNCR Systems*, EPRI, Palo Alto, CA; May 2002.

36. EPRI 1004024, *Operating and Maintenance Guidelines for Selective Catalytic Reduction Systems*, EPRI, Palo Alto, CA; December 2001.

37. EPRI 1004054, *Reagent Delivery Systems for SCR and SNCR Systems*, EPRI, Palo Alto, CA; February 2002.

38. Power Engineering Volume 112, Issue 6, "Safe Handling of Anhydrous Ammonia".

39. 29 CFR 1910.111, "Storage and Handling of Anhydrous Ammonia".

40. 29 CFR 1910.119, "Process Safety Management of Highly Hazardous Chemicals".

41. US EPA, "General Guidance on Risk Management Programs for Chemical Accident Prevention Provisions (40 CFR Part 68)".

42. OSHA SHIB 12/05/05, "Preventing the Uncontrolled Release of Anhydrous Ammonia at Loading Stations".

43. OSHA 3132, "Process Safety Management".

44. US EPA, "Technical Background Document for Offsite Consequence Analysis for Anhydrous Ammonia, Chlorine, and Sulfur Dioxide", April 1999.

45. Publication Series Dangerous Substances 3, Guidelines for Quantitative Risk Analysis (Purple Book), Ministry of VROM, 2005.

46. The UK Health and Safety Executive, "Methods of approximation and determination of human vulnerability for offshore major accident hazard assessment".

47. NFPA 496, "Standard for Purged and Pressurized Enclosures for Electrical Equipment", 2013 Edition.

48. OSHA Technical Information Bulletin TIB 00-11-06 "Potential for Natural Gas and Coal Dust Explosions in Electrical Power Generating Facilities".

49. http://newsroom.cpsenergy.com/latest-news/update-deely-coal-plant-explosion/.

50. "Dust Explosion and Fire Prevention Handbook: A Guide to Good Industry Practices", Nicholas P. Cheremisinoff, 2014.

51. NFPA 654: "Standard For The Prevention Of Fire And Dust Explosions From The Manufacturing, Processing, And Handling Of Combustible Particulate Solids" 2013.

52. NFPA 68: "Standard On Explosion Protection By Deflagration Venting" 2013.

53. EPRI 3002001229, *Dust Mitigation Methods for Coal Combustion Products*, EPRI, Palo Alto, CA; August 2013.

54. NFPA 496: "Standard for Purged and Pressurized Enclosures for Electrical Equipment," 2013 Edition.

55. "CCPS Guidelines for Chemical Process Quantitative Risk Analysis," 2nd Edition, Center for Chemical Process Safety (CCPS), Institute of Chemical Engineers (AIChE) 1999.

56. "CCPS Guidelines for Facility Siting and Layout," Center for Chemical Process Safety (CCPS), Institute of Chemical Engineers (AIChE), 2003.

57. "Vulnerability of Humans," International Association of Oil and Gas Producers, Report No 434-14.1 (2010).

58. National Institute for Occupational Safety and Health (NIOSH) – http://www.cdc.gov/niosh/idlh/intridl4.html.

59. American Industrial Hygiene Association (AIHA) - Emergency Response Planning Guidelines (EPRG) 2014 https://www.aiha.org/.

60. Perry, W. W., and W. P. Articola (1980), Study to Modify the Vulnerability Model of the Risk Management System. U.S. Coast Guard, Report CG-D-22-80, February, 1980.

61. HSE, Major Hazard Aspects of the Transport of Dangerous Substances. Health and Safety Executive, Advisory Committee on Dangerous Substances, London, United Kingdom, 1991.

62. World Bank, "Technique for Assessing Industrial Hazards", Technical Paper No.55, A manual of Technica Ltd. 1988.

63. Dow's Fire & Explosion Index Hazard Classification Guide, Wiley-American Institute of Chemical Engineers (AIChE).

64. Imperial Chemical Industries, "The Mond Index," ICI PLC, Explosion Hazards Section, Technical Department, Winnington, UK, 1985.

65. Technical Information Bulletin TIB 00-11-06, "Potential for Natural Gas and Coal Dust Explosions in Electric Power Generating Facilities," U.S. Department of Labor.

66. NFPA 654: Standard for the Prevention of Fire and Dust Explosions from the Manufacturing, Processing, and Handling of Combustible Particulate Solids, 201300.

67. CCPS "Guidelines for Vapor Cloud Explosion, Pressure Vessel Burst, BLEVE and Flash Fire Hazards", 2nd Edition, 2010.

68. CCPS "Guidelines for Process Equipment Reliability Data with Data Tables" Wiley Online Library 28 September 2010.

69. EPRI 1012783, *Guidelines for Obtaining and Using Operating Experience at Fossil Power Plants*, EPRI, Palo Alto, CA; February 2007.

70. IEEE Std. 610.12-1990, "

Appendix A: Interview Questions and Results

A series of informal interviews were conducted with plant personnel, engineering firms, and consultants from the fossil generation industry and petro-chemical industry. The questions were designed to discover any 1) relevant guidance, standards, and best practices, 2) operating experience, and 3) EPRI member objectives for the report.

1. **Was your control room designed to provide protection, or did the designers consider design criteria to offer protection against any of the following hazards?**
   - Turbine missiles
   - External environmental conditions (floods, gases, tornado, hurricane, and so on)
   - Fires
   - Explosions
   - Physical attacks
   - Others?

   Fossil Generation Industry Responses:

   - Control rooms are designed for ergonomics and human factors, but are not designed based on hazard analysis to mitigate any particular hazards.
   - Some control rooms are designed for positive pressure to protect against dust and fire; however it is not based on a formal hazard analysis.
   - Some control rooms have upgraded fire doors for fire rating and insurance, but may not have upgraded the frames and structure to the same design standard as the door.
   - Some newer plants have located the control room away from the main plant. That is based on general knowledge that distance from a hazard is an effective mitigation, and not on specific hazard analysis.
   - In some coastal locations, there are separate safe rooms for personnel protection from hurricanes or flooding. Uncertain about hazard analysis contributing to the structure design.

Petro-Chemical Industry:

- Petro-chemical owners have been developing habitable area (including control room) design criteria based on site specific hazard analysis and consequences.
- In the last 5 years hazard risk analysis has been introduced. If risk analysis is performed in conjunction with consequence analysis, the control room design is based on a risk versus consequence analysis.
- Retrofits of older plants are being performed based on the design criteria.
- The primary hazards in petro-chemical are explosion and toxic release.
- The refinery industry has been the leader with the chemical industry catching up.

2. **What design criteria should be considered in control room design?**

Fossil Generation Industry Responses:

- Protect personnel in the habitable areas (administrative spaces, break rooms, and so on) to allow them to survive an event and evacuate.
- Develop criteria to determine which habitable spaces to protect outside the control room.
- Cost versus hazard characterization and ranking based on highest probability and consequence.

Petro-Chemical Industry:

- See number 1.

3. **What hazards should be considered? How would you rank the hazards?**

Fossil Generation Industry Responses:

- Fire (Combustibles, Switchgear)
- Explosion (Dust, Hydrogen, Transformer)
- Chemical Release (Ammonia)
- High Pressure Steam Break
- Flood (extreme weather, tsunami, dam break, pipe break)
- Missiles (turbine blade)
- Environmental (adjacent facility, seismic, chemical, thermal, and so on)
- Interviewees were unable to provide ranking.

Petro-Chemical Industry:

- Hazards and ranking based on site specific analysis.

4. **Are you aware of any standards and/or guidance that are available?**

   Fossil Generation Industry Responses:

   - No known control room design guidance or standards.
   - NFPA for doors and structures.

   Petro-Chemical Industry:

   - A variety of guidance and standards are available and are used based on the owner policy, engineer recommendations, and insurance requirements. Some notable standards are listed below.
   - API 752 "Management of Hazards Associated With Location of Process Plant Buildings" for Permanent Buildings.
   - API 753 "Management of Hazards Associated With Location of Process Plant Portable Buildings" for Portable Buildings.
   - API 500 "Recommended Practice for Classification of Locations for Electrical Installations at Petroleum Facilities" for location of electrical equipment as a combustion source.
   - OSHA "Process Safety Management of Highly Hazardous Chemicals", 29 CFR 1910.119.
   - NFPA 654: "Standard for the Prevention of Fire and Dust Explosions from the Manufacturing, Processing, and Handling of Combustible Particulate Solids."
   - NFPA 496: "Standard for Purged and Pressurized Enclosures for Electrical Equipment", 2013.
   - FEMA 453, "Design Guidance for Shelters and Safe Rooms", May 2006.

5. **Do you have any internal guidance or specifications on control room design? If so, will you share them?**

   Fossil Generation Industry Responses:

   - No documented guidance or specifications.
   - Some specifications have been developed on a project basis from one utility. (We were unable to obtain copies.)

   Petro-Chemical Industry:

   - See number 4.
   - Some plant owners have formed an Explosion Research Cooperative (ERC) to collaborate on hazard analysis and control room design. Their documents are not available outside of the ERC.

6. **Do you believe that it is technically or commercially feasible to maintain positive control room air pressure?**

   Fossil Generation Industry Responses:

   - Some plants do maintain positive air pressure and are able to maintain the structure to keep positive air pressure.
   - Positive air pressure to manage dust contamination and to mitigate fire effects.

   Petro-Chemical Industry:

   - Yes. NFPA 496 is used as the standard.

7. **What other spaces should be considered for hardening and survivability, such as a computer room or safe shutdown room?**

   Fossil Generation Industry Responses:

   - See number 2.

   Petro-Chemical Industry:

   - See number 2.

8. **To what degree do you believe that technical human performance should be considered?**

   Fossil Generation Industry Responses:

   - Not something that has been specifically considered.

   Petro-Chemical Industry:

   - Personnel training and procedures to limit time in hazardous areas have been implemented in some plants. Maintenance and Operations personnel are sometimes resistant because they believe that they must be near the equipment to perform their duties.

9. **Do you believe that a control room and the equipment within it should survive long enough to provide for safe shutdown of the plant to preserve the asset investment?**

   Fossil Generation Industry Responses:

   - Only for personnel safety and evacuation. An event that would endanger control room personnel would also have a catastrophic effect on the plant, and the plant would shut down on its own.
   - In some coastal locations, there are separate safe rooms for personnel protection from hurricanes or flooding. These rooms may contain redundant control system functions for safe shutdown, communications, and monitoring.

Petro-Chemical Industry:

- Same.

10. **Do you believe that a control room should survive long enough to provide for evacuation of personnel?**

    Fossil Generation Industry Responses:

    - Yes. Typical emergency procedures are to trip the plant and evacuate.

    Petro-Chemical Industry:

    - Yes. The hazard analysis that has been performed will sometimes include safe egress in addition to initial survival of an event.

11. **Would you consider retrofitting existing control rooms to allow for personnel safety and safe shutdown?**

    Fossil Generation Industry Responses:

    - Only if there is a business case to support the cost.

    Petro-Chemical Industry:

    - Yes. Retrofits of existing plants are performed based on hazard analysis and consequence versus risk.

12. **Is a remote control facility an important consideration for the future?**

    Fossil Generation Industry Responses:

    - Not sure. This has not been considered except for remote control rooms in new plants.

    Petro-Chemical Industry:

    - No. Only for personnel safety.

13. **Do you believe that FERC/NERC will regulate or provide guidance in this area in the future?**

    Fossil Generation Industry Responses:

    - Unknown.

    Petro-Chemical Industry:

    - Not Applicable.

Appendix B: Overview of Facility Study and QRA Methods

A Facility Study (FS) and quantitative risk assessment (QRA) are typically performed in separate phases. Phase I (FS) is a consequence-based study that focuses on evaluating the hazards associated with facility operations. Phase II (QRA) is a risk-based study that is usually an optional additional study if the consequences predicted by the FS are not tolerable. The QRA accounts for the likelihood events will occur, therefore providing an estimate of risk to onsite personnel (building occupants and outdoor personnel).

To support development of a systematic technical approach for the mitigation of potential toxic, fire and explosion hazards associated with operation of the facility, an FS includes flammable and toxic dispersion and blast results for postulated maximum credible events (MCEs) identified during the study. The FS also includes thermal and toxic occupant vulnerability analyses that distinguish between shelter-in-place and non-shelter-in-place buildings and outdoor personnel.

The QRA identifies societal risk contribution by source, societal risk distribution by building/outdoor area, building/outdoor area individual risk values, and individual risk values for work groups identified by the facility. The QRA can also incorporate simple mitigation credits such as HVAC isolation and personal protective equipment when applicable. Details of the process generally performed for each phase are provided in the following sections.

B.1 Conducting a Facility Study

The key components to performing a Facility Study are described below.

- Define credible (MCEs) to determine fire, explosion, and toxic hazards by reviewing process flow diagrams (PFDs) and material balance sheets to identify representative release cases and their locations. Documenting the source selection process (for example, highlighted PFDs) can be useful to illustrate process streams considered as part of a possible release scenario. A range of release cases up to full-bore rupture should be assessed for each representative source, and each source should be evaluated for release in multiple directions.

- Assess potential explosion scenarios including, but not limited to, vapor cloud explosions (VCEs), bursting pressure vessels (BPVs), boiling liquid expanding vapor explosions (BLEVEs), condensed phase chemical explosions, reactive chemical explosions, steam drum ruptures, firebox explosions, dust explosions, and so on.
- Calculate blast loads and resulting building damage levels and occupant vulnerability values for buildings assessed in the study. Determine the maximum blast loads and the scenarios causing those loads for each building assessed in the study. Blast effects should be calculated using a recognized blast prediction method (for example, the Baker-Strehlow-Tang (BST) methodology for calculating blast loads from VCEs).
- Perform a review of the occupied buildings of interest and model them using a relevant assessment model (for example, Single-Degree-of-Freedom [SDOF]) to estimate the predicted blast response of buildings.
  - Buildings should be modeled based on either visual inspection by a qualified structural engineer or review of available structural drawings.
- Calculate flammable and thermal end points and potential impacts to each occupied building of interest for each scenario assessed.
- Calculate building occupant vulnerability values for jet/pool fire scenarios assessed on each occupied building of interest.
- Flammability concentration contours at different thresholds should be developed and documented (for example, Upper Flammability Limit (UFL), Lower Flammability Limit (LFL), and ½ LFL).
- Thermal radiation contours (resulting from jet fires or pool fires) at different thresholds should be developed and documented (for example, 37.5 kW/m^2, 12.5 kW/m^2, 4 kW/m^2).
- Overpressure contours at different thresholds should be developed and documented (for example, 0.6, 0.9, 3, 5, and 10 psig).
- Document inputs, calculations and results in a report.
- Recommend further actions (for example, retrofit susceptible occupied buildings; perform a QRA to estimate risk of governing events and so on).

B.2 Conducting a Quantitative Risk Assessment

The key components to performing a quantitative risk assessment are described below. These typically follow on from the completion of the FS.

- Estimate a release frequency for each scenario modeled using industry-average failure rate data. Release frequencies should take into account the release size, piping size and length, and type and amount of process equipment.

- Estimate event frequencies for consequences that are unrelated to equipment count (for example, steam drum rupture, firebox explosions, or loading/unloading scenarios) based on a generalized fault tree analysis (FTA) of the event.
- Evaluate conditional probabilities that will be used for each scenario. These probabilities should include ignition and ignition timing, time of day, weather conditions, and wind directions. Statistical local meteorological data should be used to derive weather-related probabilities.
- Estimate occupancy at the facility during normal operations in order to determine the consequences of each modeled event. This should include differentiating between areas where personnel spend their time (for example, specific outdoor areas versus inside specific buildings).
- Evaluate the risk based on frequency estimates and consequence results for each scenario assessed. Explosion consequence results should be assessed using a reputable blast prediction methodology (for example, Baker-Strehlow-Tang (BST) methodology for calculating blast loads from VCEs). Sum results to determine aggregate (societal) risk values.
- A QRA report should be prepared that documents the analysis and summarizes results. Societal and individual risk results should be presented in the following forms:

    1. Societal risk identifies the total amount of risk posed by the plant operation, accounting for the number of people impacted by the scenarios assessed. Societal risk results should be presented in terms of FN curves and tables that list the contributions to risk by source and building/location. This enables risk to be effectively managed by focusing attention on high-risk sources and areas and buildings incurring the most risk.
    2. Individual risk is measured in terms of Building Individual Risk (BIR) and Workgroup Individual Risk (WIR). BIR is defined as the amount of risk an individual would incur if he spent 24 hours a day in a building or an area. This information should be utilized to identify buildings for possible worker relocation. WIR is defined as the amount of risk a worker incurs, based on the amount of time he spends in each building/area and the level of risk associated with those locations.
    3. Provide high-level recommendations for risk mitigation.

B.3 Typical FS and QRA Deliverables

Reports should be issued for each study performed to document all assumptions, methodologies employed, and results.

The FS or QRA report should include:

- Executive Summary that lists maximum building damage levels (BDLs), flammability concentrations, and thermal intensity levels for each building assessed *(FS only)*
  - The executive summary in the QRA report should include FN curves, risk results tables identifying the highest risk contributing buildings, and highest risk sources *(QRA only)*.
- Study work scope and plant description
- Methodology
- Input data and assumptions
- Calculations
- Results:
  - Consequences analysis, discussion and evaluation *(FS only)*
    - Fire
    - Explosion
  - Risk summaries *(QRA only)*
    - Societal risk – FN curves, building risks, source risks
    - Individual risk – building individual risk, work group individual risk.
- Conclusions and recommendations
- Appendices that show:
  - Representative source definitions (highlighted PFDs, plot plans showing locations and piping routes, table summarizing pressure, temperature, composition, and release sizes assessed) *(FS only)*
  - Structural Analysis for SDOF buildings *(FS only)*
  - Composite contours of flammable and toxic hazard boundaries *(FS only)*
  - Dispersion and explosion overpressure contours for significant cases *(FS only)*
  - Composite overpressure contours *(FS only)*
  - Building damage level, overpressure, impulse, and occupant vulnerability values for each new and existing building for each significant blast scenario assessed *(FS only)*
  - Portable building BDL contours *(FS only)*
  - Statistical meteorological data used for the study *(QRA only)*

B.4 BakerRisk FS and QRA Methodologies

A Facility Study assesses potential vulnerabilities posed by identified fire, explosion, and toxic hazards, but does not consider the likelihood or the consequences (number of people who may perish) of the accidents assessed.

BakerRisk utilizes several key technologies while performing an FS. These technologies have been developed over time using experimental data and a database of industry experience. BakerRisk operates several large-scale test sites and is a leader in explosion, jet fire, and structural field tests. In addition to leading edge test data, BakerRisk has conducted hundreds of accident investigations and combines knowledge from both fields (testing and investigation) and applies them to our proprietary state of the art software. This ensures that high quality and realistic methods are employed in every study. Some of the unique tools BakerRisk utilizes include discharge, dispersion, explosion, and consequence models as well as the BakerRisk failure rate database.

B.4.1 Facility Study Methodology

The primary objective for an FS is to assess the potential vulnerabilities posed by fire, explosion, and toxic hazards associated with operation of facilities. To support development of a systematic technical approach for this assessment, the analysis includes hazard identification, discharge calculations, dispersion, fire, and blast analysis with building damage, and occupant vulnerability for potential accidents that are identified.

Blast Load Calculations

Typical explosion events to be modeled range from vapor cloud explosions (VCEs) to bursting pressure vessels (BPVs), boiling liquid expanding vapor explosions (BLEVEs), condensed phase chemical explosions, reactive chemical explosions, dust explosions, to name a few. BPVs are modeled using methods published by BakerRisk along with proprietary adjustments. Other explosion types are modeled using published methods [67].

Vapor Cloud Explosions (VCE)

For VCE analyses, BakerRisk assumes that discrete sections of the process area are filled with a stoichiometric concentration of flammable material and the blast effects are determined using BakerRisk's SafeSite$_{3G}$® program. The zones of confinement/congestion in the process area are based on a BakerRisk consultant's walk-down of the process area during the site visit.

VCEs occur when obstacles are present within a cloud of combusting gas. As the gas combusts, it expands, forcing the unburned gas to flow past the obstacles. The obstacles induce turbulence in the flow, which enhances the combustion process. The increased combustion rate accelerates flow, which intensifies turbulence, which accelerates flow, and so on. These obstacles are referred to as ***congestion*** since they restrict the free expansion of the gas. If a roof or other restraint is present, the burning cloud is unable to expand three-dimensionally and gases flow in the two remaining dimensions at a higher rate. This restraint is referred to as ***confinement*** since it confines the dimensionality of the combusting cloud's expansion. An accelerated flame front resulting from congestion and confinement produces a pressure wave as it travels. Pressure builds as the front accelerates, and the result is a higher pressure blast wave.

More reactive fuels burn faster and produce stronger blast waves. The Baker-Strehlow-Tang (BST) methodology classifies congestion and reactivity into categories of **high, medium,** and **low**. Confinement is classified by the number of dimensions in which the cloud is free to expand (for example, a solid roof prevents vertical expansion and is considered to be 2-D confinement).

The combination of ***congestion***, ***confinement***, and ***reactivity*** is used to predict an effective flame speed Mach number. This Mach number, along with the energy contained in the cloud, can be used to predict pressure and impulse (impulse is defined as the integral of pressure over time) by interpolating between the numerically modeled BST blast curves. BakerRisk has also extended the methodology on its own to account for the effect of multiple volumes of congestion and confinement being involved in a single explosion. This produces blast contours that account for the shape, extents, and variations in the congested and confined volumes. An example blast contour set is provided in Figure B-1. In the course of investigating over 200 industrial explosions and 500 medium-scale experiments, these extensions have been found to provide good predictions of the blast produced by VCEs.

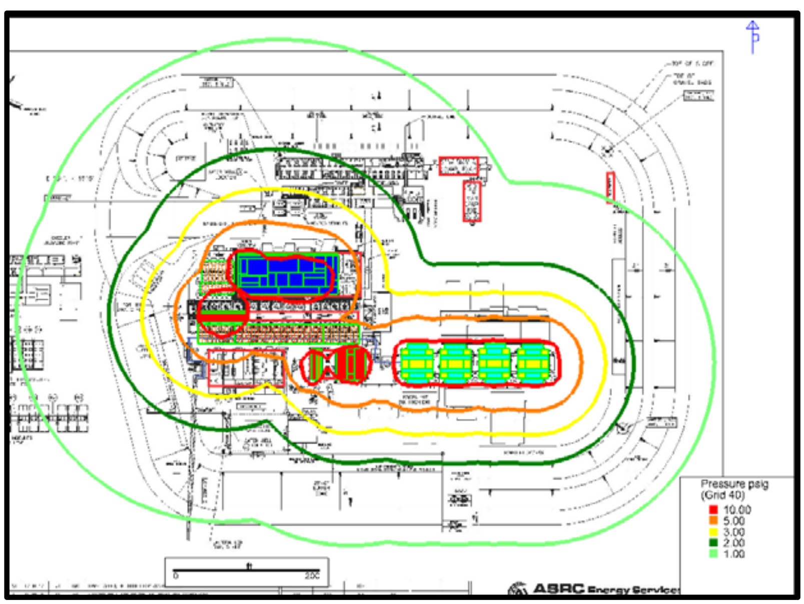

Figure B-1
Example Blast Contour Set

Figure B-2: Flammable Dispersion Intersecting with Volumes of Congestion/ Confinement illustrates an example of a flammable release from a vessel (note LFL and ½ LFL portions of cloud in dark and light green shades, respectively) that intersects with the zones of congestion and confinement to then calculate the explosion energy.

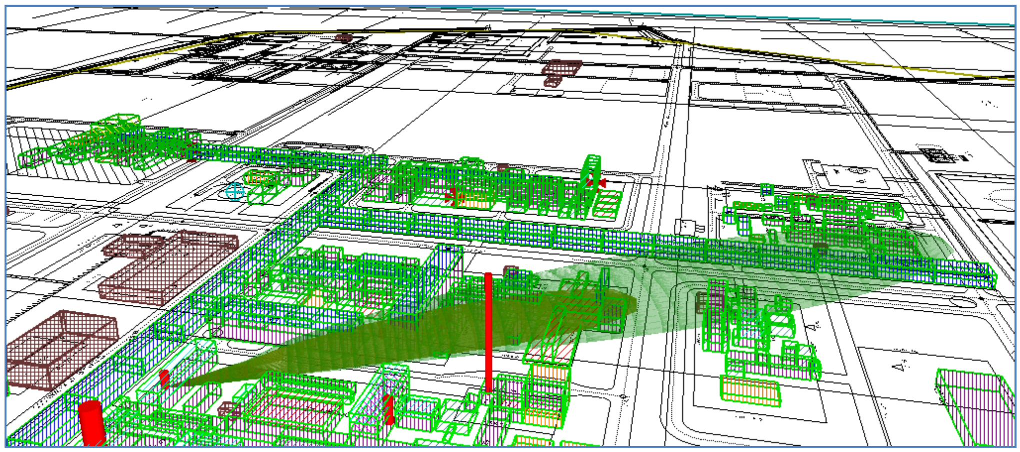

Figure B-2
Flammable Dispersion Intersecting with Volumes of Congestion/Confinement

Structural Analysis and Methodology

BakerRisk utilizes several key concepts within the methodology for calculating building blast response and explosion impact. These key concepts are:

- Overpressure, Impulse, and Duration
- Building Damage Level
- Building Damage (P-i) Curves
- Occupant Vulnerability

Overpressure, Impulse, and Duration. Assessment of blast-loaded structures requires dynamic structural analyses or other simplified methods that take into account the blast pressure history (pressure vs. time). The duration of a blast can be approximated using the peak pressure and the impulse, as shown in Figure B-3: Idealized Blast Load History.

Building Damage Level (BDL). BDLs are qualitative categories of damage used for screening purposes in consequence analyses. The damage levels that range from cosmetic damage to building collapse are associated with building occupant vulnerability. A brief description for each of five BDLs is provided in Table B-1 with photo examples of the damage levels shown in Figure B-4: Building Damage Levels (BDL).

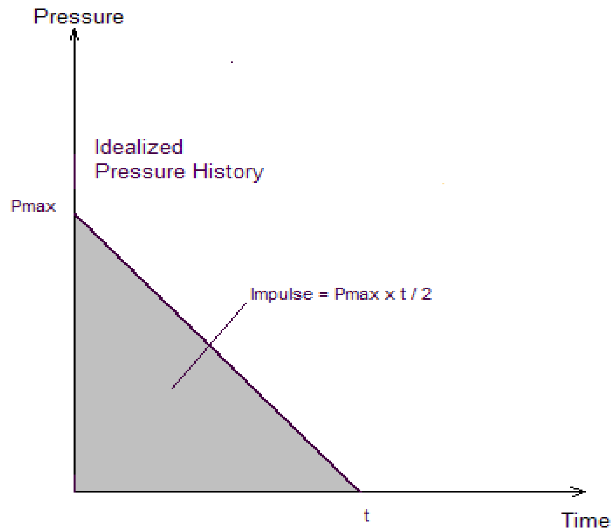

Figure B-3
Idealized Blast Load History

Table B-1
BDL Descriptions

BDL	Damage Description
1	Minor damage to roof and walls.
2	Moderate or lower damage to roof and load-bearing components.
2.5	Localized major damage to roof or walls. Moderate damage to other components.
3	Major damage to load-bearing elements or roof.
4	Failure of load-bearing elements or roof collapse.

Figure B-4
Building Damage Levels (BDL)

Building Damage Curves. Pressure-impulse (P-i) curves define potential explosion loads that cause the same response (damage) to a building or building component. A "P-i diagram" can be used to graphically determine the building response (that is, BDL) for a blast load defined by the peak pressure and impulse. A large number of blast loads can be plotted on a P-i diagram to assess the building damage from multiple explosions. The P-i curves can be developed empirically or analytically; however, they are specific to each building or component. The regions bounded by the curves correspond to areas of building damage, as illustrated in Figure B-5.

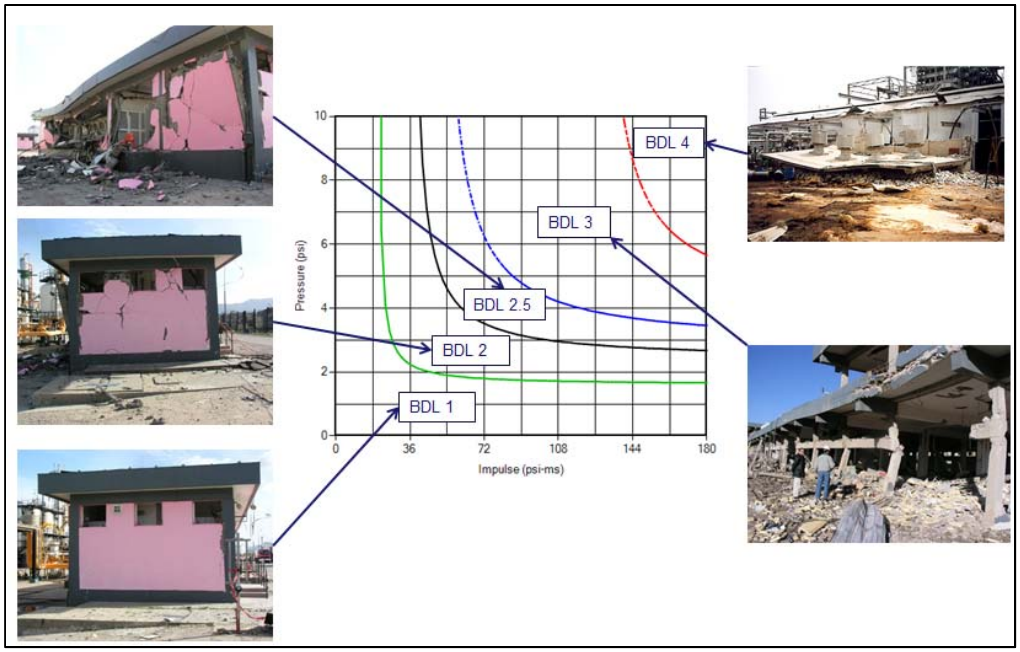

Figure B-5
Building Damage Levels and P-i Diagrams

Occupant Vulnerability. OV is the fraction of the building population that would sustain life-threatening injuries in an explosion. OV is dependent on the type of building construction, population distribution within the building, and the BDL. OV values for typical building types are summarized in Table B-2.

Table B-2
Example BDL vs. OV Summary

BDL	Occupant Vulnerability		
	Steel Frame with Metal Siding	Masonry Building with Load-Bearing Walls	Concrete Frame with Masonry Walls
1	Negligible		
2			
2.5	0.015	0.02	0.02
3	0.17	0.25	0.3
4	0.47	0.79	0.94

B.4.2 Quantitative Risk Assessment Methodology

The primary objective of a QRA is to quantify the fire, explosion, and toxic risks to onsite personnel and/or the public from process hazards associated with operation of the facility. Results of the QRA should be presented in terms of societal (aggregate) and individual risk.

Figure B-6 shows the classic QRA method of assessing and managing risk followed by BakerRisk when performing a QRA. The process shown in Figure B-6 is an iterative process. If calculations show risk to be significant, calculations can be refined until a satisfactory level of detail, confidence, accuracy and resolution has been achieved, or mitigation strategies can be implemented and risk re-assessed. This process is repeated until risk is determined to be tolerable and reduced as much as practical.

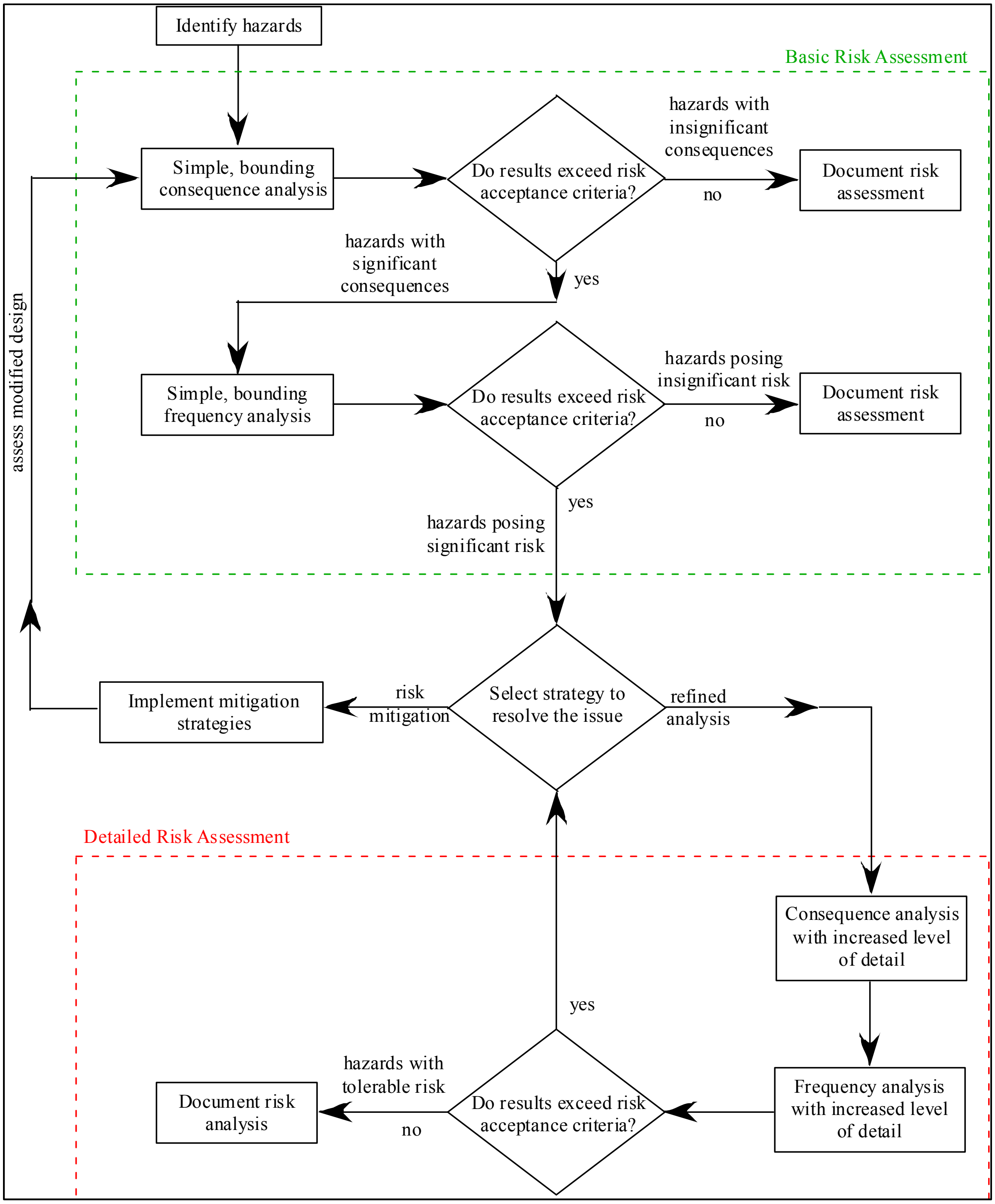

Figure B-6
Classic Risk Assessment Flowchart

The QRA assesses impacts and frequencies for identified hazards to determine risk levels.

- What accidental events can occur in the system? (identify hazards)
- What are the consequences of each event? (consequence analysis) *Note that if consequences do not merit further analysis, frequency is not evaluated.*
- How frequently would each event occur? (frequency analysis)
- What are the risks, that is, the product of frequency and consequence for the event?
  Note that if risk is insignificant, no further analysis is required.
- Are cost effective risk mitigation measures available? If so, what will be the risk after implementing these measures?

Risk can be assessed for small, medium, and large (full bore) releases, using computational models (for example, BakerRisk's computer software programs SafeSite$_{3G}$® and QRATool™). Impacts of explosion, fire, and toxic dispersion will be evaluated together with associated release frequencies, conditional probabilities of ignition, weather conditions, wind direction, time slot, and exposure of people. Risk will then be evaluated, and results will be presented in terms of total societal risk, FN curves, source risk, building societal risk, building individual risk, and work group individual risk or other data as specifically requested.

Total societal risk is a measure of risk posed by facility operations to all onsite personnel and/or the public. Results can be compared with client specific or typical industry risk criteria to determine tolerability of risks posed by facility operation. If risk is intolerably high, a combination of analysis refinement and/or risk mitigation strategies is required to reduce risk within tolerable levels. If risk is significant but tolerable, potential risk mitigating strategies are still sought and evaluated, but only ones that are determined to be cost effective (safety benefit outweighs the cost of implementation) are implemented. If risk is low, resources are not spent searching for ways to further lower risk.

FN curves are graphs that plot the frequency (F) of events predicted to cause N or more fatalities to onsite personnel. Figure B-7 is an example of FN curves for a set of process units. Figure B-8 shows an example of FN curves for a set of hazard category (toxic, jet/pool fire, flash fire, and explosion). These graphs include typical risk tolerance criteria lines.

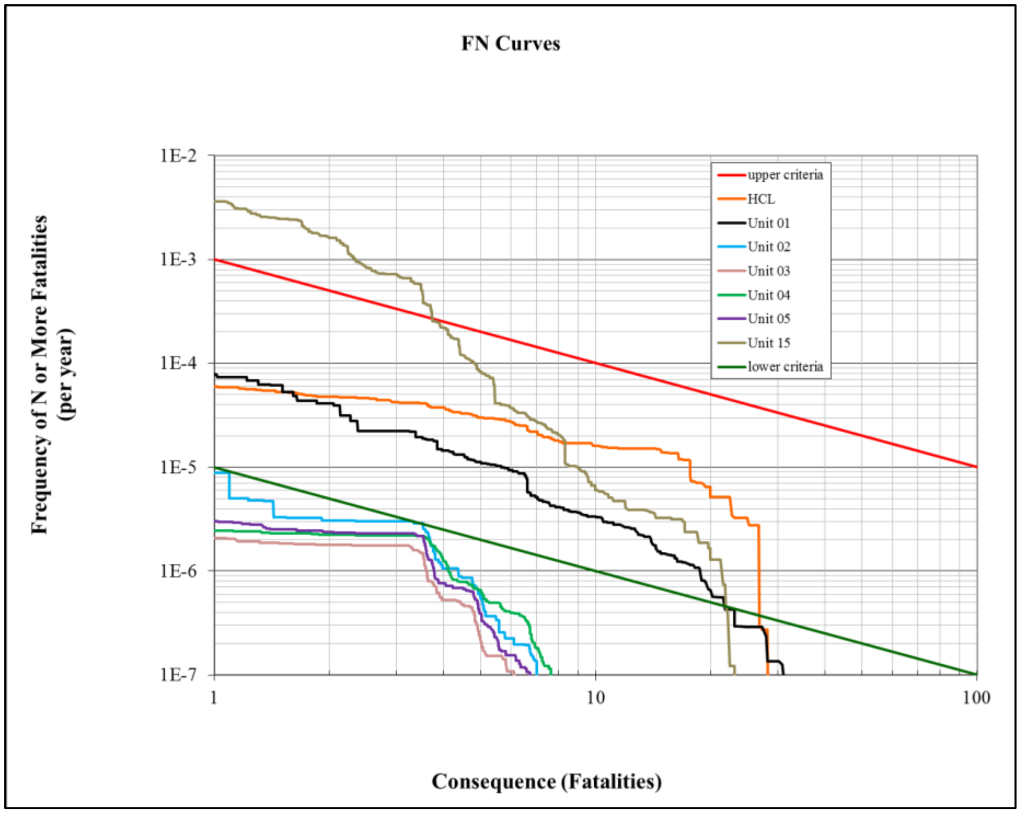

Figure B-7
Example Set of FN Curves (Risk Per Process Unit)

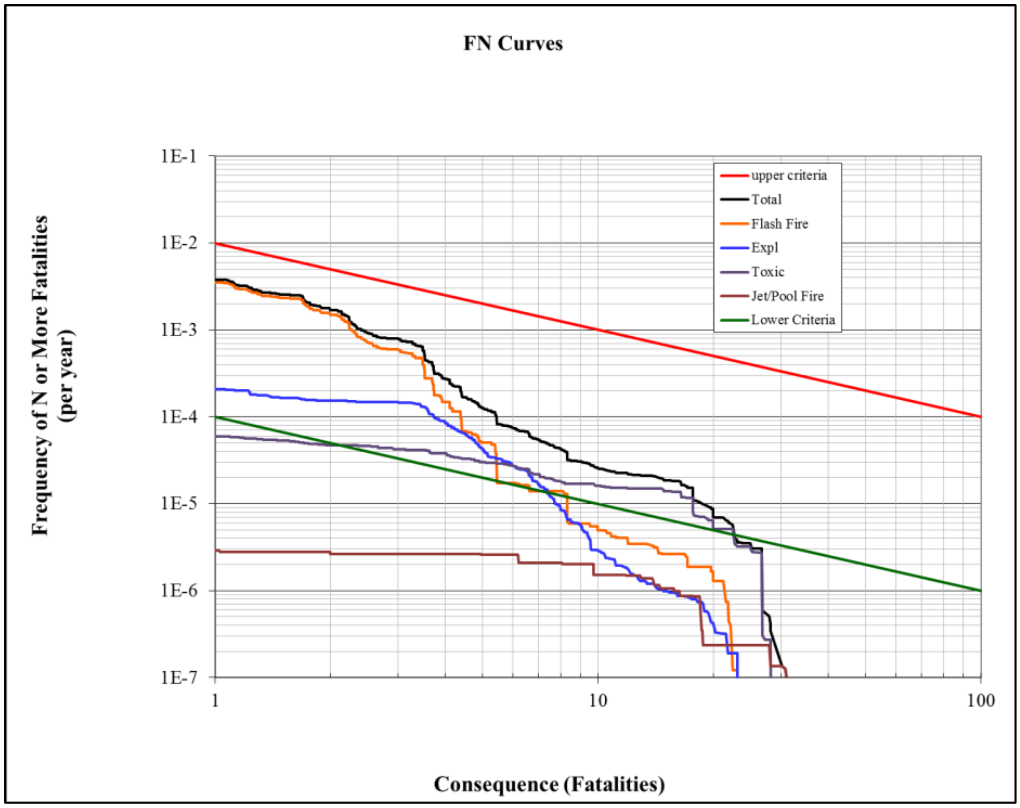

Figure B-8
Example Set of FN Curves (Total Plant Risk Per Hazard Category)

Source societal risk is a measure that identifies the total amount of risk posed by each hazard source assessed. It provides insights into high-risk sources to assist in the identification and evaluation of effective risk mitigation strategies (see Table B-3 for an example). It also identifies sources that should be reviewed to determine if simplifying assumptions can be refined.

Table B-3
Source Risk – Example

Source	Societal Risk (Fatalities/Year)					% of Total	
	Explosion	**Flash Fire**	**Toxic**	**Jet/Pool Fire**	**Total**	**Source**	**Cumulative**
Unit 02 – reac1 – hexane	1.3E-4	5.9E-4	2.1E-3	2.0E-3	4.8E-3	20.5%	20.5%
Unit 01 – reac2 – hexane	1.4E-4	2.0E-3	2.1E-3	1.7E-4	4.4E-3	18.8%	39.4%
Unit 15 – reac4 – hexane	1.8E-4	3.0E-3	5.6E-4	1.7E-4	3.9E-3	16.7%	56.1%
Unit 15 – reac3 – hexane	1.7E-4	2.9E-3	3.5E-4	3.5E-4	3.8E-3	16.3%	72.3%
Unit 03 – P514 – hexane	5.6E-5	3.4E-5	5.2E-4	1.3E-3	1.9E-3	8.1%	80.5%
Unit 04 – C531 – hexane	2.8E-5	1.4E-4	3.6E-4	3.9E-4	9.2E-4	3.9%	84.4%
HCL – 01 – Truck	1.7E-4	1.4E-4	1.6E-4	3.2E-4	7.9E-4	3.4%	87.8%
Unit 01 – E54 – ethylene	9.3E-5	2.5E-4	2.8E-4	2.8E-5	6.5E-4	2.8%	90.6%
Remainder of Sources	*3.6E-4*	*5.5E-5*	*1.6E-3*	*1.6E-4*	*2.2E-3*	*9.4%*	*100.0%*
Total	**1.3E-3**	**9.1E-3**	**8.0E-3**	**4.9E-3**	**2.34E-2**		
	6%	**39%**	**34%**	**21%**			

Building/outdoor area societal risk is a measure that identifies the total amount of risk operations pose on building occupants and outdoor area populations, accounting for the number of people in each building/area (see Table B-4 for an example). It provides insights into high risk buildings and outdoor process areas to assist in the identification and evaluation of effective risk mitigation strategies associated with protecting personnel by focusing attention on areas and buildings of highest risk.

Table B-4
Building and Operation Area Societal Risk – Example

Building/Area	Avg. Occ.	Building Societal Risk (Fatalities/Year)				% of Total	
		Blast	Fire	Toxic	Total	Bldg/Area	Cumulative
Maintenance Shop	9.1	5.6E-5	2.0E-5	**1.1E-3**	1.2E-3	45.3%	45.3%
E&I Shop	2.4		4.3E-6	**8.1E-4**	8.1E-4	31.4%	76.6%
Admin Building	3.7	2.7E-8	4.1E-7	**1.6E-4**	1.6E-4	6.2%	82.8%
Training Building	6.8	**9.5E-5**	1.5E-6	4.8E-5	1.4E-4	5.6%	88.4%
Contractor Bldg	0.9	9.7E-7	3.3E-7	**7.6E-5**	7.7E-5	3.0%	91.4%
Process 2 CR	0.7	1.1E-7	2.7E-7	**4.0E-5**	4.0E-5	1.6%	92.9%
Process 1 CR	3	**2.9E-5**	7.3E-7	9.1E-6	3.9E-5	1.5%	94.4%
Process 3 CR	3.1	**3.0E-5**	1.1E-6	1.7E-6	3.3E-5	1.3%	95.7%
Area – Process 1	1.5		7.3E-7	**2.2E-5**	2.3E-5	0.9%	96.5%
Carpenter/Pipe Shop	2	4.50E-10	2.9E-7	**1.9E-5**	1.9E-5	0.7%	97.3%
Area – Process 3	0.4	7.8E-6	4.6E-8	**8.4E-6**	1.6E-5	0.6%	97.9%
Rail Loading Shack	0.5	1.9E-6	1.60E-10	**1.4E-5**	1.6E-5	0.6%	98.5%
Area – Loading	4.2	**9.0E-6**	1.0E-6	5.0E-6	1.5E-5	0.6%	99.1%
Boiler House	0.1	1.2E-6	3.6E-8	**7.1E-6**	8.3E-6	0.3%	99.4%
Area – Process 2	2.6	4.80E-11	2.3E-7	**5.1E-6**	5.3E-6	0.2%	99.6%
West Warehouse	0.3	2.80E-10	7.8E-8	**3.1E-6**	3.2E-6	0.1%	99.7%
Laboratory	0.1	4.20E-11	3.6E-8	**2.1E-6**	2.1E-6	0.1%	99.8%
East Warehouse	0.3	3.80E-11	3.3E-8	**1.3E-6**	1.3E-6	0.1%	99.9%
Engineering Bldg	0.2	1.9E-6	7.4E-8	**1.1E-6**	3.1E-6	0.1%	100.0%
Total	41.9	**2.3E-4**	**3.1E-5**	**2.3E-3**	**2.6E-3**		
		11%	**1%**	**87%**			

* Highlighted blue cells represent outdoor areas.

** Blank cell represents negligible risk.

Building individual risk (BIR) is a measure that identifies the level of risk incurred by a person who continuously occupies a given building (24 hours per day). See Table B-5 for an example. It reflects the fact that individuals will escape a hazardous event if possible. It can be used to assist in decisions regarding location of personnel and protective equipment and training requirements.

Table B-5
Building and Outdoor Area Individual Risk – Example

Building/Area	Building Individual Risk (POD/Year)			
	Blast	**Fire**	**Toxic**	**Total**
E&I Shop		1.8E-6	**3.4E-4**	3.4E-4
Maintenance Shop	6.2E-6	2.2E-6	**1.2E-4**	1.3E-4
Contractor Bldg	1.1E-6	3.7E-7	**8.4E-5**	8.6E-5
Boiler House	1.2E-5	3.6E-7	**7.1E-5**	8.3E-5
Process 2 CR	1.6E-7	3.9E-7	**5.7E-5**	5.8E-5
Admin Building	7.3E-9	1.1E-7	**4.3E-5**	4.3E-5
Area – Process 3	2.0E-5	1.2E-7	**2.1E-5**	4.1E-5
Rail Loading Shack	3.8E-6	3.20E-10	**2.8E-5**	3.2E-5
Laboratory	4.20E-10	3.6E-7	**2.1E-5**	2.1E-5
Training Building	**1.4E-5**	2.2E-7	7.1E-6	2.1E-5
Engineering Bldg.	9.5E-6	3.7E-7	**5.5E-6**	1.5E-5
Area - Process 1		4.9E-7	**1.5E-5**	1.5E-5
Process 1 CR	**9.7E-6**	2.4E-7	3.0E-6	1.3E-5
West Warehouse	9.30E-10	2.6E-7	**1.0E-5**	1.1E-5
Process 3 CR	**9.7E-6**	3.5E-7	5.5E-7	1.1E-5
Carpenter/Pipe Shop	2.30E-10	1.5E-7	**9.5E-6**	9.6E-6
East Warehouse	1.30E-10	1.1E-7	**4.3E-6**	4.4E-6
Area – Loading	**2.1E-6**	2.4E-7	1.2E-6	3.6E-6
Area – Process 2	1.80E-11	8.8E-8	**2.0E-6**	2.1E-6

*Highlighted blue cells represent outdoor areas.

Work group individual risk is a measure of risk incurred by a given employee. A separate work group individual risk value is calculated for each group of workers identified for the site (see Table B-6 for an example). It reflects the amount of time spent in each building or area on site. This measure focuses attention on workers who incur the highest levels of risk to determine if working conditions can be modified to reduce their risk. It is also used to ensure that no workers exceed individual risk tolerance criteria.

Table B-6
Worker Individual Risk (Annual Probability of Death) – Example

Work Group	WIR
Maintenance	7.9E-5
E&I	7.2E-5
Administration	7.1E-5
Lab personnel 2	6.3E-5
Lab personnel 1	3.5E-5
Process 1 field operator	3.0E-5

Frequency Calculations

To produce individual and societal risk values and FN curves, the frequency of each accident scenario assessed is taken into account.

Initiating Event Frequencies ($F_{release}$)

Equipment failure rate data is publically available [68] and a propriety database has been generated by BakerRisk. Release frequencies are estimated based on equipment counts and failure rates identified in the database. In some cases, release frequency estimates are supplemented with site specific data. BakerRisk works with site personnel to define failure rates for special cases such as runaway reactions, firebox explosions, and steam drum ruptures.

Ignition Probabilities

Estimating the probability that a flammable cloud will ignite is not an exact science, and there are many factors that contribute to this uncertainty. The likelihood of ignition depends on the presence, location, and energy of potential ignition sources as well as the duration of the flammable release. The flammable properties of the material in the cloud, concentration at the time it encounters a potential ignition source, the possibility of static discharge, transient ignition sources, or other less predictable sources, and numerous other factors all contribute to the likelihood of ignition.

Studies have been performed to give ignition probability as a function of leak rate, flammable cloud size, duration of release, density of identifiable ignition sources, type of location, and type of material released, and other factors. Ignition probability will be assessed as a function of release magnitude, based on industry experience. In general terms, the larger the release, the more likely ignition occurs.

Ignition probabilities for indoor releases of flammable material may be evaluated in the same manner as outdoor scenarios or may use a more detailed method that accounts for minimum ignition energy of the material being released, building ventilation flow rate, flammable material discharge rate, electrical classification of the area, duration of release, and other factors.

Weather and Wind Direction Probabilities

The conditional probabilities of weather condition (P_w) and release/wind direction (P_{dir}) are based on statistically significant local meteorological data. This may be gathered from on site or at a nearby airport. Example summary tables of weather conditions and wind directions and associated probabilities are provided below in Table B-7 and Table B-8. Wind direction probabilities are shown graphically in Figure B-9.

Table B-7
Example Weather Condition Distribution

Stability		Wind Speed (m/s)	Prob.
B	Unstable	3	0.1
D	Slightly unstable	4	0.21
D	Slightly unstable	7	0.24
F	Stable	3	0.45

Table B-8
Example Wind Direction Distribution

Direction	Prob.
N	0.129
NNE	0.082
NE	0.046
ENE	0.050
E	0.091
ESE	0.056
SE	0.035
SSE	0.026
S	0.018
SSW	0.015

Table B-8 (continued)
Example Wind Direction Distribution

Direction	Prob.
SW	0.025
WSW	0.050
W	0.046
WNW	0.079
NW	0.107
NNW	0.145

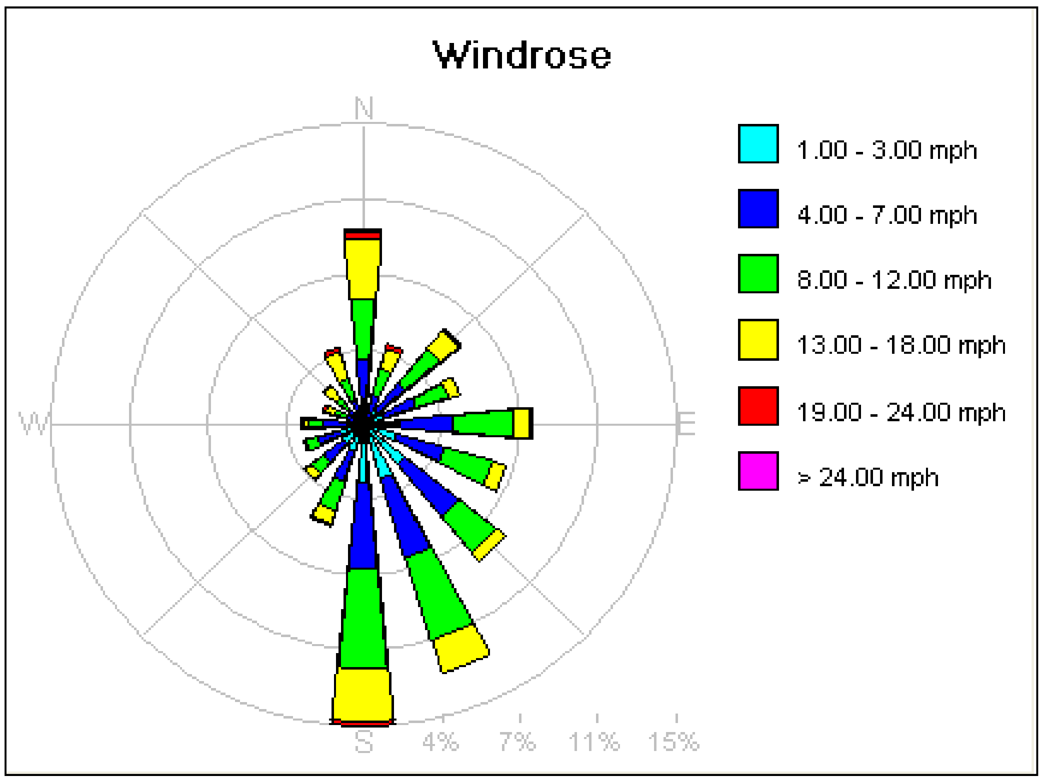

Figure B-9
Example Wind Rose

Other Conditional Probabilities

The time slot is assigned a probability that reflects the portion of the week that the time slot represents. For example, "regular business hours" may represent 40 hours per week and be assessed as a probability of 40/168 = 24%.

A generic event tree (Figure B-10) is used to assist in defining scenarios and to graphically depict those sequences. The event tree shows sources, split of various sizes, weather conditions, wind directions, ignition source timing, and toxic ingression/infiltration calculations, and other factors. Because each source may be evaluated for hundreds of different scenarios, the event tree is abbreviated to show example branches.

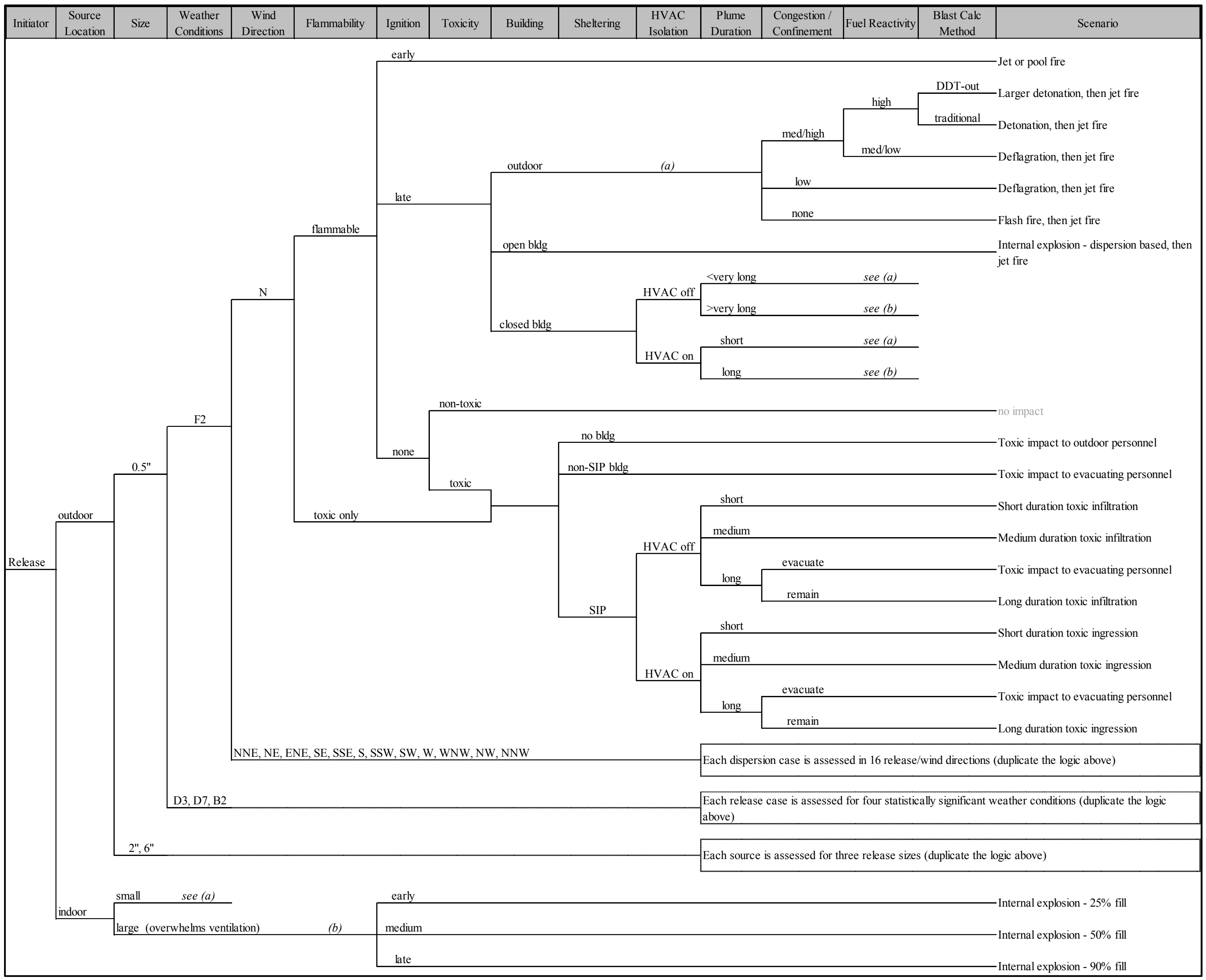

Figure B-10
Sample Event Tree

The analysis methodology is more complex than the event tree shows, but this gives a simplified summary of the method that hazard sources are assessed. Following are details of the event tree:

- *Initiator:* The starting point (far left end of the event tree) is a release of hazardous material from the process. Note that other events such as firebox explosion, steam drum rupture, runaway chemical reaction, and so on, are not processed using this event tree.
- *Source Location:* The first branch splits indoor scenarios from outdoor releases.
- *Size:* The second branch splits each release into a range of release sizes. Outdoor scenarios are typically assessed for small, medium, and large releases. Indoor scenarios may only distinguish between cases that may overwhelm ventilation and ones that are small enough to behave like regular dispersion cases. A small indoor release is assumed to only impact people within the building where the release occurs if it is a fire or toxic event, but it is treated the same as an outdoor release for explosion scenarios.
- *Weather Condition:* This branch is only applicable to outdoor release scenarios. Each release will be assessed for a range of two statistically significant weather conditions.
- *Wind Direction:* Each dispersion is assessed in 16 evenly spaced horizontal directions.
- *Flammability:* Hazards are split into flammable and non-flammable (toxic only) categories because they get assessed for different things depending on whether or not they pose fire/explosion hazard.
- *Ignition:* Outdoor flammable releases are assessed for early, late, and non-ignition. Early ignition scenarios are assessed as jet or pool fire depending on the material conditions. Late ignition scenarios are further divided later in the event tree. Flammable releases that are not toxic and not ignited are non-events (no impact). Flammable releases that are also toxic and are not ignited are grouped together with non-flammable toxic sources and treated together hereafter. Indoor cases are split into three categories for delayed ignition (early, medium, and late). These represent the portion of the room that is filled with a flammable mixture at the time of ignition and are typically assessed as 25%, 50%, and 90% of the energy of a stoichiometric mixture for the entire room volume.
- *Building:* This split is applied to outdoor delayed ignition scenarios. The branch splits scenarios into outdoor areas, open buildings, and closed buildings. Open buildings are assessed as congestion/confinement zones and are assessed for blast and flash fire effects. Closed buildings and outdoor impacts are further split later in the event tree.

- *Sheltering:* This branch is only applicable to toxic impacts. It splits the scenario into outdoor populations (address consequence based on lethality of toxic concentration and assumed duration within the plume), non-SIP buildings (evaluate vulnerability of a person evacuating the building and traveling crosswind to a safe location), and SIP (further refined later in the tree).
- *HVAC isolation:* This branch splits scenarios where flammable or toxic vapors reach a closed building into two possibilities. One has HVAC successfully isolated, and the other reflects continued HVAC operation.
- *PlumeDduration*: This branch splits flammable and toxic scenarios that impact closed buildings into a range of durations. For a closed building with HVAC successfully isolated, an indoor explosion is only considered possible if the plume lasts a very long time (infiltration will eventually allow indoor concentration to exceed LFL). Those cases are shown as a transfer to the indoor explosion branch (although these scenarios can be dismissed as occupants would likely evacuate the building before the bulk concentration reached flammable levels). Shorter duration plumes would not have a significant impact within the building, so they transfer to the branch treating outdoor dispersions. If HVAC remains running, the same two outcomes are possible, but they are shorter duration events because of ingression through the HVAC system. For toxic scenarios impacting a SIP, the indoor concentration profile is calculated, and the resulting exposure is converted to occupant vulnerability.
- *Congestion/Confinement*: This branch shows how flammable clouds are evaluated for delayed ignition. If the flammable plume is outside of congestion/confinement, the scenario is a flash fire, followed by a jet fire from the source. If the plume intersects low congestion, a deflagration is predicted, followed by a jet fire. Intersection with medium or high congestion has a range of possible outcomes, so those scenarios are further split later in the event tree. Although it is unrelated to congestion/confinement, toxic impacts at SIPs are split under this heading into scenarios where people either evacuate or remain in the building. This is to show that the site may have a fallback plan where the SIP is equipped with indoor toxic monitoring, and occupants don escape packs and evacuate if the toxic concentration in the SIP reaches a certain threshold.
- *Fuel Reactivity*: Scenarios involving a flammable plume encountering medium or high congestion are split into low or medium reactivity fuel cases and high reactivity fuel cases. Low and medium reactivity fuel plumes are predicted to deflagrate followed by a jet fire. High reactivity fuel scenarios are predicted to detonate, and the calculation is done two ways, treated by the final branch in the event tree.
- *Blast Calculation Method*: The final branch shown in the event tree is limited to scenarios involving high reactivity fuel intersecting medium or high congestion levels. These scenarios are all predicted to detonate followed by a jet fire. The DDT-out branch assumes the cloud is allowed to reach steady state and then ignition occurs within the medium/high congestion, so the

blast energy involves gases outside of congestion. The traditional blast calculation branch represents a scenario where the ignition occurs outside of congestion so fuel outside of congestion burns as a flash fire, and the detonation energy is limited to the volume of fuel within congestion.

The event tree does not show the split of time slots. Each scenario is assessed for consequences, which depends on the number of people present. Because the number of people present depends on the time of day, each scenario is evaluated for a range of time slots. Typically these include regular business hours, lunch time, and off shift, although additional time slots can be added to accommodate special situations. The event tree also does not distinguish between liquid and vapor scenarios, although fires scenarios are actually evaluated for jet fire when flammable vapors are generated and pool fires for liquid releases.

Risk Calculations

Risk for a given event is defined as the product of consequence (fatalities/event) and frequency (events/year) and is presented in terms of fatalities per year.

$$\text{Risk}_{\text{scenario}} = F_{\text{scenario}} \times \text{Consequence}_{\text{scenario}}$$

Risk is additive, so it is calculated for each scenario, and results are summed to determine the amount of risk posed by facility operations.

$$\text{Risk}_{\text{Total}} = R_{\text{scenario-1}} + R_{\text{scenario-2}} + \ldots\ R_{\text{scenario-N}}$$

Export Control Restrictions
Access to and use of EPRI Intellectual Property is granted with the specific understanding and requirement that responsibility for ensuring full compliance with all applicable U.S. and foreign export laws and regulations is being undertaken by you and your company. This includes an obligation to ensure that any individual receiving access hereunder who is not a U.S. citizen or permanent U.S. resident is permitted access under applicable U.S. and foreign export laws and regulations. In the event you are uncertain whether you or your company may lawfully obtain access to this EPRI Intellectual Property, you acknowledge that it is your obligation to consult with your company's legal counsel to determine whether this access is lawful. Although EPRI may make available on a case-by-case basis an informal assessment of the applicable U.S. export classification for specific EPRI Intellectual Property, you and your company acknowledge that this assessment is solely for informational purposes and not for reliance purposes. You and your company acknowledge that it is still the obligation of you and your company to make your own assessment of the applicable U.S. export classification and ensure compliance accordingly. You and your company understand and acknowledge your obligations to make a prompt report to EPRI and the appropriate authorities regarding any access to or use of EPRI Intellectual Property hereunder that may be in violation of applicable U.S. or foreign export laws or regulations.

The Electric Power Research Institute Inc., (EPRI, www.epri.com) conducts research and development relating to the generation, delivery and use of electricity for the benefit of the public. An independent, nonprofit organization, EPRI brings together its scientists and engineers as well as experts from academia and industry to help address challenges in electricity, including reliability, efficiency, affordability, health, safety and the environment. EPRI also provides technology, policy and economic analyses to drive long-range research and development planning, and supports research in emerging technologies. EPRI's members represent approximately 90 percent of the electricity generated and delivered in the United States, and international participation extends to more than 30 countries. EPRI's principal offices and laboratories are located in Palo Alto, Calif.; Charlotte, N.C.; Knoxville, Tenn.; and Lenox, Mass.

Together...Shaping the Future of Electricity

Program:
Operations Management & Technology

© 2014 Electric Power Research Institute (EPRI), Inc. All rights reserved. Electric Power Research Institute, EPRI, and TOGETHER...SHAPING THE FUTURE OF ELECTRICITY are registered service marks of the Electric Power Research Institute, Inc.

3002003205

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com