SPE SPE-120532-PP

Operational Risk Management Tools

Georges A. Melhem, Ph.D., Neil Prophet - ioMosaic Corporation

This paper was prepared for presentation at the 2008 SPE Middle East Health, Safety, Security, and Environment Conference and Exhibition held in Doha, Qatar, 20–22 October 2008.

Abstract

Risk management in the petrochemical industry includes a wide variety of activities, one of which is quantitative risk assessment. The quality of a quantitative risk assessment study is highly dependent on the effectiveness of the hazard identification stage - it is essential that all applicable hazards and potential hazard scenarios are considered. When analyzing large refineries, the number of hazard scenarios can run into thousands; so it is important that these hazard scenarios have a relevant risk impact on the study results, while excluding those scenarios with negligible risk contribution. Two general types of scenarios leading to loss of containment are typically considered: “generic” and “non-generic”.

This paper outlines and describes a tool to enhance operational risk management – it describes an effective methodology for streamlining hazard scenario identification and development for large, site wide, refinery quantitative risk assessments. The paper also provides practical guidance for the estimation of both “generic” and “non-generic” scenario failure rate data. Safeguards such as basic process controls and safety instrumented systems that can be used to mitigate undesirable events and to reduce risks are considered in the scenario identification and development methodology.

An Overview of Risk

Risk, as it relates to the process industries, has been defined as a measure of economic loss or human injury in terms of both the incident likelihood and the magnitude of the loss or injury. A simplified risk equation could be represented by:

$$Risk = Consequence \times Frequency \qquad (1)$$

A risk analysis is the development of a quantitative estimate of risk, based on engineering evaluation and mathematical techniques for combining estimates of incident consequences and frequencies.

Quantified Risk Assessment (QRA) can be used for a number of different purposes. However, it is most valuable as part of a Risk Management program. Risk Management is the identification and control of hazards, through both technological and management solutions. Occasionally QRA is conducted solely to meet a regulatory requirement, but this rarely precludes using the results as part of a corporate risk management program.

A QRA can typically be divided into four primary tasks, and a reporting activity. The primary tasks being:

- Hazard Identification
- Frequency Analysis
- Hazards Analysis
- Risk Determination

The purpose of this paper is to describe an effective methodology for efficiently streamlining hazard scenario identification and development, for large refinery quantitative risk assessments. Therefore, focus will be directed to the hazard identification stage.

Hazard Identification

Hazards to be considered
The history of major industrial incidents in refineries and petrochemical plants indicates that a release of hydrogen or light hydrocarbons in the range of C_2-C_6 is often involved. Examples include:

Table 1: Examples of major incidents in petrochemical facilities

Location	Facility	Released Components
Pasadena, Texas	Polyethylene Unit	Ethylene, Butane
Norco, Louisiana	FCC Gas Recovery	$C_2 – C_3$
Mexico City, Mexico	LPG Storage	Propane, Butane
Flixboro, UK	Petrochemical	Cyclohexane
Torrance, California	Hydrocracker	Hydrogen
Texas City, Texas	Isomerization Unit	$C_5 – C_6$
Kuwait	Crude Unit	NGLs

Scenario identification should focus on process equipment and piping where release conditions could lead to the following hazards:

- Vapor cloud explosion
- Fireball
- Boiling Liquid Expanding Vapor Explosion (BLEVE)
- Flame jet
- Pool fire
- Toxicity impact

The importance of the hazard identification stage should never be underestimated. As Trevor Kletz once said: “Are we sure that we have identified all the major hazards, and all the ways in which they can occur? What has not been identified can neither be assessed nor mitigated.”

Vapor Cloud Explosions
Vapor cloud explosion hazards can occur in hydrocarbon processing facilities upon immediate and/or delayed ignition. The type of explosion and magnitude of damage is strongly influenced by the sensitivity of the fuel, the amount of fuel present within the flammability limits, the strength of the ignition source, the presence of significant confinement (3 walls or more), or congestion (equipment and pipe work). Stronger explosions are produced when the fuel concentration in air is close to stoichiometric.

When sensitive fuels such as hydrogen, acetylene, ethylene, propane, propylene, etc. are present in sufficient quantity an explosion can transit from a deflagration to detonation. The risk assessment should focus on loss of containment events that can produce:

(a) *Liquid and two-phase streams* composed of hydrocarbons with carbon numbers from 1 to 6 and above their normal boiling point such that flashing upon release will occur, and
(b) *Gas streams* composed of hydrogen or hydrocarbons with carbon numbers from 1 to 6 and operating at elevated pressure (> 1 barg).

Pool Fires
The ignitability of liquid hydrocarbons increases with increasing processing and/or storage temperature. Flash point and auto-ignition temperature are important parameters that relate to the potential for ignition. A release temperature at or above the autoignition point signifies 100% likelihood of ignition.

Consider the following process conditions when evaluating pool fire risks:

i. Liquids stored at temperatures above their flash point but less than their autoignition point can form liquid pools upon release. If and when ignited, these releases can yield pool fires.
ii. Liquids stored at temperatures at or above their auto-ignition point will immediately ignite upon release. A pool fire or a flame jet will result depending on the degree of superheat of the stored materials.

A plot of auto-ignition temperature as a function carbon number is provided below and clearly shows that typical

hydrocarbons with a carbon number of 9 or more will autoignite upon release if discharged at temperatures equal to or greater than 200ºC.

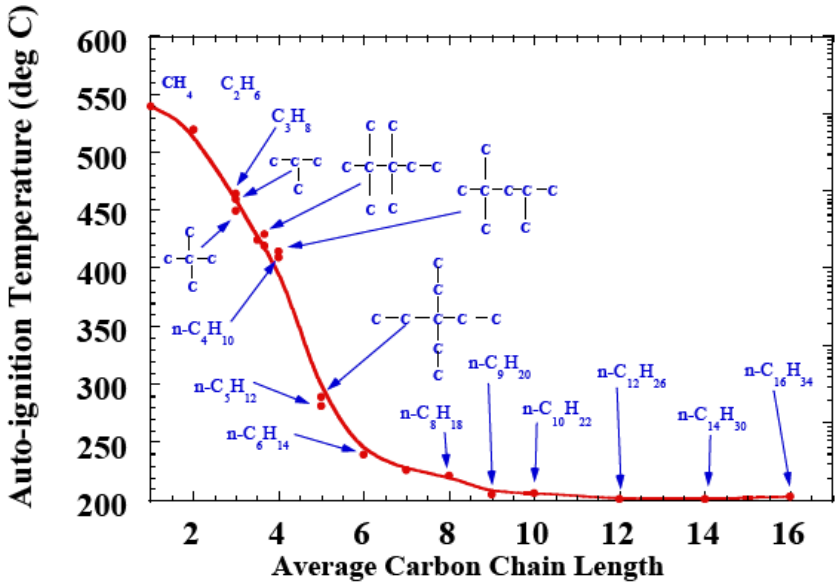

Figure 1. Graph of Auto-Ignition Temperature compared with Average Carbon Chain Length

Refinery process areas where releases are likely to auto-ignite include the bottoms of heavy oil columns in units such as:

- Crude and Vacuum Distillation
- FCC and Coker Fractionation

Pool fire hazards are localized and as a result thermal radiation effects (burns) are typically confined to within one or two pool diameters from the edge of the flame. Thermal radiation is absorbed by water moisture and carbon dioxide present in the air. In addition, thermal radiation intensity decays in proportion to 1/(distance squared). Typically, a person exposed to a thermal radiation flux of 5 kW/m^2 will feel pain in 20 seconds. Second degree burns are possible. 5 kW/m^2 is often used as an injury threshold.

Typical values of flame emissive powers for hydrocarbon pool fires range from 280 kW/m^2 (LNG) to 25 kW/m^2 (kerosene). Due to the presence of curbing, drainage, etc. in process areas, liquid spills are usually confined. API 521 suggests a range of fire circles from 2500 to 5000 ft^2 (232- 465 m^2). Using the upper bound as a probable pool area, the calculated radiation distances are shown below for a C8 hydrocarbon. Note that the hazard distances are quite limited and would be contained within the battery limit of the process units. Heavier oil burns with a smoky flame which further lowers the emissive power.

Table 2: Pool fire heat flux hazard distances

Criteria (kW/m^2)	Hazard Distance (m)
5	43
10	26
12.5	23
25	Maximum flux reached equals 15 kW/m^2

Due to the limited hazard of pool fires, this methodology proposes that they are not considered for process units. However, pool or dike fires in tank farms should be included for light products such as gasoline or naphtha. Jet fires due to ignition of vapor or two-phase pressurized releases should also be considered.

Flame Jets and Vapor Cloud (Flash) Fires

Flame jets can occur as a result of high pressure gas and/or two-phase releases. Flame jets can produce intense heating with flame emissive powers ranging up to 350 kW/m^2. Flame jets impinging on nearby structures and/or vessels can lead to catastrophic failures in less than 10 minutes.

If immediate ignition does not occur and the high pressure releases are not confined, the jet will continue to disperse until delayed ignition occurs or the release ends. Under these circumstances the lower flammability limit is usually reached while the jet momentum is still higher than ambient turbulence. When delayed ignition occurs, and depending on the sensitivity of the fuel and the strength of the ignition source, a small fireball/explosion may be experienced followed by a flame jet that will continue until the release ends. The amount of material involved in the fireball/explosion is limited and typically equivalent to no more than 10 seconds of flow.

If immediate ignition does not occur and the high pressure jet is confined and/or obstructed (such as jets pointing vertically downwards or striking other nearby objects) the jet loses its momentum and will continue to disperse until delayed ignition occurs or the release ends. When delayed ignition occurs a flash fire will occur. Depending on the sensitivity of the fuel, the degree of confinement, and the strength of the ignition source, the flash can accelerate and lead to an explosion. The amount of material involved in the flash fire/explosion can be substantial.

Flash fires typically proceed at flame speeds ranging from 10 to 20 m/s. In general, indoor population is expected to survive a flash fire. In flash fire exposure, a building is expected to burn from the outside to the inside. This often provides sufficient time for the occupants to escape.

Fireballs and BLEVEs

These events are common simultaneous outcomes of a catastrophic vessel failure containing flammable materials. A BLEVE produces mechanical damage (overpressure) from the stored PV energy in the vessel contents. Vessels containing saturated liquids or two-phases also contribute additional overpressure from the flashing process. If the vessel contents are flammable and the contents ignite immediately after vessel failure, a fireball/vapor cloud explosion can result. The magnitude of the outcomes/damage will depend on the amount of material present within the flammability range, the strength of the ignition source, and the sensitivity of the contents.

Catastrophic vessel failure can occur due to construction defects, pool fire exposure with a deficient relief system, a runaway chemical reaction, or a flame jet impingement on the vapor space causing localized heating and weakening of the metal. Note that a BLEVE can occur with nonflammable materials such as water in steam explosions. Typically, pressure vessels will fail catastrophically when the contents pressure exceeds three times the MAWP or 2/3 the ultimate tensile strength of the metal at the temperature of the event. The overpressure produced from the catastrophic failure of vessels containing gases or saturated liquid can produce substantial damage in the near field.

Toxic Dispersion from Sour Water

Sour Water containing H_2S, ammonia and CO_2 is generated in several refinery processes. It presents a potential toxic exposure hazard to hydrogen sulfide gas. Hydrogen sulfide dissociates into the ionic species HS^- and S^{-2} in water. The dissociation is enhanced by high pH conditions. Due to the presence of NH_3 (i.e., NH_3OH) in the water, the pH of typical sour water is 8 or higher. A recent publication (Woodward) indicates that the equilibrium vapor pressure of dissociated H_2S compared with nondissociated H_2S is significantly less under such conditions by as much as 96% or better. The publication concluded that for a large spill of sour water, the H_2S hazard zone extended 50 meters to an ERPG 2 (30ppm) endpoint. ioMosaic's own analysis of a line rupture carrying 40,000 kg/hr of sour water containing 0.7 mol % H_2S (average sour water stream coming from the process units) indicated similar results.

Based on this information, sour water lines within process units do not need to be considered unless there is population within 50 meters of the release point, and/or:

- All sour water (Liquid) streams with H_2S at or greater than 0.5 mol% AND temperature at or greater than 100 C should be considered.
- Sour water (Liquid) streams with temperature less than 100 C do not need to be considered, unless the spill location is within 50 meters to a marked control room or occupied building.
- Vapor/gas and two-phase streams with H_2S at or greater than 0.5 mol% should all be considered for toxic hazards.

Rich amine (MEA/DEA/water containing sour gas) streams can be treated similarly, as the presence of the alkanolamines would also produce a high pH condition.

Hazard Scenarios

Very broadly speaking a refinery consists of storage and process vessels, process units and pipelines. In this broad breakdown, pumps, compressors, heat exchangers, and some valves are considered to be parts of storage and process vessels or process units. Flanged joints, small bore fittings and some other valves are considered as parts of the pipeline infrastructure.

A two-pronged approach can be utilized during the hazard scenario identification stage – classifying the hazards as either "generic" and "non-generic". "Generic" scenarios consider loss of containment from piping and equipment – leaks, full-bore piping ruptures, or catastrophic vessel failures. "Non-generic" scenarios consider more unusual failure modes, which are specific to the process being analyzed, such as a refinery operation.

In each case, the purpose of the hazard identification stage is to provide a comprehensive list of hazard scenarios, along with all the required data, to be taken to the hazard analysis stage. A comprehensive list of the required data for each scenario is provided below:

- Scenario Name
- Process Flow Diagram / Piping & Instrumentation Diagram
- Fluid Conditions (Temperature, Pressure, Phase, Composition, Explosion Reactivity, Toxicity)
- Release Flowrate
- Release Coordinates
- Equipment Type and Size
- Hole Diameter(s)
- Piping Length (if applicable)
- Release Duration
- Release Geometry (1D, 2D, 2.5D, 3D)
- Degree of confinement
- Release Frequency

Generic Scenarios

For "generic" loss of containment scenarios including the large amount of pipelines (including flanges, valves, small bore connections, etc.) present, it is possible to use a simplified, but reasonably accurate method that ties the likelihood of a chemical or oil release from a pipeline directly to the total length of pipeline of all types at the facilities. The line lengths, which will affect the release frequency, can be estimated from plot plan and elevation drawings. These estimated lengths are then adjusted utilizing a set of general rules to ensure that the ultimate risk calculations are reasonable. The set of rules used to "adjust" the length of pipe increases the overall pipe length and hence the frequency of release. The rules include the following criteria:

- The total calculated line length is factored by a default value of 1.5, to allow for the fact that piping typically does not follow direct paths
- This factor should be increased to 2, where items are close together
- A factor of 2 is also used if the equipment item is very large, such as for air heat exchangers or columns
- Where more than one of the above cases occurs, such as measuring between large items that are close together, a factor of 3 should be used

Non-Generic Scenarios

"Non-generic" scenarios consider pump seal failures, corrosion failures of dead legs or water boots on receivers due to sour water attack; or overpressure failure of low pressure vessels downstream of high pressure separators where maintaining a liquid interface is preventing pressure blow through, and the upstream pressure is > 3 times the MAWP of the downstream vessel.

The selection process requires Process Flow Diagrams (PFD) and Mass Balances (MB) to locate areas of the process units that meet the process conditions specified above. Then, the Piping and Instrumentation Drawings (P&ID) for those areas should be reviewed to assess the potential for the "non-generic" failure modes listed above and for sufficient pressure and/or inventory.

Vessel Selection

The methodology considers hydrocarbon containing vessels with 5 or more cubic meters of inventory. That is between 3 and 4 metric tons of hydrocarbon contents depending on the typical range of hydrocarbon specific gravity. Note this is a recognized

and generally accepted good engineering practice criterion for installation of remotely operated isolation valves for some energy companies.

Release Duration

Release duration can have a significant impact on the consequences of a hazardous event. For toxic scenarios, exposure duration is a critical factor. For flammable or explosive scenarios, the amount of flammable mass available is dependent on release duration.

When considering release duration, guidance can be derived from API Publication 581. This methodology takes into account type of detection system, type of isolation system, and the condition of the fluid being released.

The tables below provide an illustration of how release duration can be estimated:

Table 3: Guidelines for Establishing Continuous Release Detection and Isolation Times Based On API 581

Detection Type	Isolation Type	Liquid T > AIT	Liquid FP < T AIT	Vapor or Two-Phase
A	A	5 min. 1" to 4" leak	5 min. 1" to 4" leak	5 min. 1" to 4" leak
B	B	20 min. 1" leak 10 min. 4" leak	20 min. 1" leak 10 min. 4" leak	20 min. 1" leak 10 min. 4" leak
C	B	40 min. 1" leak 30 min. 4" leak	40 min. 1" leak 30 min. 4" leak	40 min. 1" leak 30 min. 4" leak
B	C	30 min. 1" leak ** min. 4" leak	30 min. 1" leak ** min. 4" leak	30 min. 1" leak 20 min. 4" leak
C	C	40 min. 1" leak ** min. 4" leak	40 min. 1" leak ** min. 4" leak	40 min. 1" leak 20 min. 4" leak

** Determined from inventory and release rate.
AIT = Auto-ignition temperature
FP = Flashpoint

Table 4: Classification of Detection and Isolation Systems Based on API 581

Class	Type of Detection System
A	Instrumentation designed specifically to detect material losses by changes in operating conditions (i.e., loss of pressure or flow) in the system.
B	Suitably located detectors to determine when the material is present outside the pressure-containing envelope.
C	Visual detection, cameras, or detectors with marginal coverage.
Class	**Type of Isolation System**
A	Isolation or shutdown systems activated directly from process instrumentation or detectors, with no operator intervention.
B	Isolation or shutdown systems activated by operators in the control room or other suitable locations remote from the leak.
C	Isolation dependent on manually-operated valves.

Failure Frequencies

There are several effective methods that can be used to establish consequence-frequency pairs for detailed QRA studies including (a) fault or event tree analysis, (b) historical failure rate data, and (c) layer of protection analysis (LOPA). LOPA is a relatively new method and is gaining widespread usage.

In fault or event trees analysis, one describes in a systematic fashion the logical sequence of events (fault or event trees) that can lead to a hazard scenario. The trees are then quantified to provide an estimate of the hazard scenario frequency.

The use of historical failure rate data approach is good for "generic" failures, but is not recommended for "non-generic" process-related failures or venting from stacks or relief devices. In addition, one cannot easily consider the impact of safety instrumented systems on risk reduction.

The frequency analysis of scenarios can also be conducted using the layer of protection analysis (LOPA) technique that is described in the CCPS publication *Layer of Protection Analysis, Simplified Process Risk Assessment.*

This methodology recommends the use of adjusted historical failure rate data for generic scenarios, and the LOPA methodology for non-generic scenarios.

Generic Failure Frequency Data for Equipment

Generic frequency data for equipment failure can be based on values summarized in API-581, Risk Based Inspection Base Resource Document, 2000. The API values are based on variety of sources.

Table 5: Generic Equipment Failure Rate Data from API-581 (hydrocarbon service)

Equipment Type	Leak Frequency (per year for four hole sizes)			
	¼ inch	1 inch	4 inch	Rupture
Atmospheric Storage Tank	$4x10^{-5}$	$1x10^{-4}$	$1x10^{-5}$	$2x10^{-5}$
Column	$8x10^{-5}$	$2x10^{-4}$	$2x10^{-5}$	$6x10^{-6}$
Compressor, Centrifugal		$1x10^{-3}$	$1x10^{-4}$	
Compressor, Reciprocating		$6x10^{-3}$	$6x10^{-3}$	
Filter	$9x10^{-4}$	$1x10^{-4}$	$5x10^{-5}$	$1x10^{-5}$
Fin/Fan Coolers	$2x10^{-3}$	$3x10^{-4}$	$5x10^{-8}$	$2x10^{-8}$
Heat Exchanger, Shell	$4x10^{-5}$	$1x10^{-4}$	$1x10^{-5}$	$6x10^{-6}$
Heat Exchanger, Tube	$4x10^{-5}$	$1x10^{-4}$	$1x10^{-5}$	$6x10^{-6}$
Piping, ¾" diameter, per ft	$1x10^{-5}$			$3x10^{-7}$
Piping, 1" diameter, per ft	$5x10^{-6}$			$5x10^{-7}$
Piping, 2" diameter, per ft	$3x10^{-6}$			$6x10^{-7}$
Piping, 4" diameter, per ft	$9x10^{-7}$	$6x10^{-7}$		$7x10^{-8}$
Piping, 6" diameter, per ft	$4x10^{-7}$	$4x10^{-7}$		$8x10^{-8}$
Piping, 8" diameter, per ft	$3x10^{-7}$	$3x10^{-7}$	$8x10^{-8}$	$2x10^{-8}$
Piping, 10" diameter, per ft	$2x10^{-7}$	$3x10^{-7}$	$8x10^{-8}$	$2x10^{-8}$
Piping, 12" diameter, per ft	$1x10^{-7}$	$3x10^{-7}$	$3x10^{-8}$	$2x10^{-8}$
Piping, 16" diameter, per ft	$1x10^{-7}$	$2x10^{-7}$	$2x10^{-8}$	$2x10^{-8}$
Piping, >16" diameter, per ft	$6x10^{-8}$	$2x10^{-7}$	$2x10^{-8}$	$1x10^{-8}$
Pressure Vessels	$4x10^{-5}$	$1x10^{-4}$	$1x10^{-5}$	$6x10^{-6}$
Pumps, reciprocating	0.7	0.01	0.001	0.0001
Pump, single seal	$6x10^{-2}$	$5x10^{-4}$	$1x10^{-4}$	
Pump, double seal	$6x10^{-3}$	$5x10^{-4}$	$1x10^{-4}$	
Reactor	$1x10^{-4}$	$3x10^{-4}$	$3x10^{-5}$	$2x10^{-5}$

The generic frequency values provided above are suggested values from API-581. API-581 offers a systematic method by which these generic frequency values can be adjusted to reflect the actual operating facility management systems and equipment conditions.

$$F_{adjusted} = F_{generic} \times F_{Equipment\ Factor} \times F_{Management\ Factor} \qquad (2)$$

The Management Systems Factor ranges from a value of 0.1 to 10 and applies to all the generic failure frequency data shown above. The equipment factor only applies to the specific equipment it is estimated for. These values are based on questionnaires which assess the quality of a particular site's mechanical integrity and process safety systems.

Non-Generic Failure Frequency Calculation

For non-generic scenarios, a more detailed frequency analysis is required. This methodology recommends the use of the Layer of Protection Analysis (LOPA) technique. There are advantages to using LOPA for non-generic scenarios, compared with more traditional risk assessment methodologies such as fault tree analysis and the use of historical failure rate data:

- LOPA facilitates the determination of more precise cause-consequence pairs, and therefore improves scenario identification.

- The frequencies and probabilities provided in the CCPS LOPA text reflect the most recent consensus of data from companies in the chemical process industries since the book was published in 2001. This data does not require extrapolation of old data to current equipment or data developed from other industries (i.e., nuclear) to the chemical industry.

LOPA Methodology

For each scenario developed, the frequency of the event that produces the described consequences is determined. Table 6 shows a simple format used for documenting the frequency of each scenario. The overall scenario frequency may consist of a number of events:

The **initiating event** which causes an undesirable deviation from normal operation. This could be a human error, equipment or instrument failure or external event, such as fire. The initiating event may be expressed as an annual frequency or as a probability per opportunity. For example, scenarios that have an initiating event based on human error are typically expressed as a failure rate per opportunity. The enabling event would then be expressed as the number of opportunities per year (frequency).

An **enabling event** which is typically related to time the system is exposed to the undesirable deviation while it is in a hazardous state. An example would be failure of an unloading hose on a trailer due to the cab pulling away while still connected. If the trailer is empty when this happens, then no spill of hazardous chemical will result. The enabling event is typically expressed as a probability, but may also be expressed as a frequency when the scenario involves human actions that are done at repetitive intervals.

The number of similar **units** that could experience the same scenario. These could be the number of vessels or equipment, or length of piping.

A **conditional event** that must occur for the undesirable consequences to result. An example is a failure to purge a vessel containing flammable material with nitrogen prior opening for maintenance. If the undesirable consequences are a fire, then the conditional event is the ignition of the flammable vapors in the vessel. A conditional event is included in the scenario frequency when the event is taken to a pre-defined consequence. Most loss of containment scenarios involving flammable materials do not include the conditional event in the frequency, but rather is developed as part of an event tree that evaluates all possible consequences including: no ignition, immediate ignition, and delayed ignition. This event tree analysis would also be part of the risk assessment. A conditional event is expressed as a probability.

An **independent protection layer (IPL) event** that either prevents or reduces the likelihood of the scenario. An IPL is expressed as a probability of failure on demand.

Table 6: Sample Scenario Identification and Frequency Estimation Summary Sheet using LOPA

Scenario Frequency Summary	Description	Value
Scenario Reference	Sample scenario - 1	
Unit	Reaction	
Initiating Event (frequency per year)	Hose failure due to movement of trailer (see comment 1)	8.3×10^{-3}
Units	Five trailers normally onsite	5
Enabling Event (probability)	Trailer is not empty when hose fails (see comment 2)	0.1
IPL 1	Unit procedure requires a device to be installed on trailer which prevents hookup of the tractor prior to commencing unloading (see comment 3)	0.1
IPL 2		1
IPL 3		1
Final Scenario Frequency		4.15×10^{-4}
Comments	1) Based on plant history, this is .0083 per year per trailer. 2) Assume 10% chance that trailer is not empty 3) Assume 0.1 PFD due to human error failing to install	

An IPL is a device, system, or action that is capable of preventing a scenario from proceeding to its undesired consequence independent of the initiating event or the action of any other layer of protection associated with the scenario. In order to be considered an IPL, the device, system or action must be:

- Effective in preventing the consequence
- Independent of the initiating event and the components of any other IPL
- Auditable through validation of design and effectiveness

The initiating causes and likelihood of failure are shown in Table 7. Items such as procedures and training and mechanical integrity would be factored into the initiating event frequency, but are not considered IPLs. Similarly, fire protection is typically considered in determining the duration of the event.

Table 8 shows the probability of failure on demand (PFD) for IPLs. This methodology recommends Approach B, as defined in the CCPS LOPA text which allows more than one IPL to be in the same basic process control system (BPCS) or a BPCS IPL with a BPCS initiating event. This approach is based on the assumption that if a BPCS function fails, it is much more probable that the component that induced the failure is the detection device or the final control element and not the common logic solver.

Table 7: Initiating Causes and Likelihood of Failure

Initiating Cause	Likelihood of Failure (per year)
BPCS instrument loop failure	**0.1**
Cooling water failure (redundant CW pumps, diverse drivers)	**0.1**
Crane load drop	**1×10^{-4}**
Fixed Equipment Failure (E.g. exchanger tube failure)	**0.01**
Gasket / packing blowout	**0.01**
Human Error - (Non-Routine task, High Stress)	**1.0**
Human Error - (Non-Routine task, Low Stress)	**0.1**
Human Error - (Routine Task, Once-per-Day Opportunity)	**1.0**
Human Error - (Routine Task, Once-per-month Opportunity)	**0.1**
Large external fire (aggregate causes)	**0.01**
Lightning strike	**1×10^{-3}**
Loss of Power (redundant power supplies)	**0.1**
LOTO (lock-out tag-out) procedure failure	**1×10^{-3}**
Operator failure to execute routine procedure, assuming well trained, unstressed, not fatigued)	**0.01**
Pumps and other Rotating Equipment	**0.1**
Regulator failure	**0.1**
Safety valve opens spuriously	**0.01**
Small external fire (aggregate causes)	**0.1**
Third party intervention (external impact by backhoe, vehicle, etc.)	**0.01**
Turbine / diesel engine over speed with casting breach	**1×10^{-4}**
Unloading / loading hose failure	**0.1**

Source: CCPS Guideline for Layers of Protection Analysis

Where historical plant data is available, this data should be used in place of the generic data available in the CCPS LOPA text.

Table 8: Probability of Failure on Demand (PFD) for Independent Protection Layers (IPLs)

Independent Protection Layer	Probability of Failure on Demand
Basic Process Control System, if not associated with the initiating event being	0.1
Blast-wall / Bunker	0.001
Dike	0.01
Diverse Redundant Equipment High Value	0.1
Diverse Redundant Equipment Low Value	0.01
Fireproofing	0.01
Flame / Detonation Arrestors	0.01
Identical Redundant Equipment	0.1
Instrumented Pump Seal Pot with Alarm	0.1
Open Vent (no valve)	0.01
Operator response to alarm with at least 10 minutes response time	0.1
Relief valve	0.01
Rupture disc	0.01
SIL 1 SIF	0.1
SIL 2 SIF	0.01
SIL 3 SIF	0.001
Underground Drainage System	0.01

Source: CCPS Guideline for Layers of Protection Analysis

Application of Methodology

While the hazard scenario development criteria and considerations described above may appear complex, the process can be summarized neatly in a relatively straightforward methodology. This methodology is repeated numerous times to ensure each equipment item, and all piping, is considered for each unit (and subsequently, the entire refinery). The basic data required to develop the scenarios include the unit plot plans, process flow diagrams, material balances, piping and instrument diagrams (P&IDs) and equipment lists.

Typically, a spreadsheet can be used to record the scenarios as they are identified. The spreadsheet can be automated through the use of macros, and color-coding, to simplify the data input and output stages.

Hazard scenario identification typically involved the following steps:

1. A piece of equipment is first identified on the plot plan and its coordinates established.

2. Any piping feeding the equipment is then identified and its length measured based on the plot plan scale. An adjustment factor is applied to the measured pipeline length to account for elevation differences. The standard factor is 1.5. A factor of 2 is applied when piping went to or from a main pipe rack or 3 if the interconnecting piping is

between close coupled equipment. The failure frequency of piping in sour water or rich amine service (containing more than 0.5 mole percent hydrogen sulfide and above 100ºC) should be increased by a factor of around 10 to account for increased risk of corrosion. Pipe diameter can be obtained from the P&IDs.

3. Stream composition and process conditions are obtained from the mass balance.

4. Release elevation is estimated. Two meters is a good approximation for piping between equipment, except for piping in pipe racks which is usually around six meters.

5. Detection and isolation time for the release is then determined.

6. Release geometry, degree of confinement and explosion reactivity is determined for releases containing flammable components. For example, compressor shelters would have a release geometry of 2.5D vs. 3D for unconfined areas. In addition equipment located on platforms with equipment above or below should be given a medium or high degree of confinement. Streams containing mostly natural gas have a low explosion reactivity and streams containing at least 1 mole % hydrogen would be considered to have high explosion reactivity.

7. For equipment-related release scenarios, equipment type and dimensions are then assessed. Any pumps with an instrumented seal pot to detect incipient failure of a seal should be identified. For vessels receiving material from another vessel operating at a pressure above the design pressure of the receiving vessel, the number of independent protection layers was estimated based on the instrumentation shown on the P&IDs.

Upon completion of the Hazard Scenarios Identification stage, there still remains significant effort in completing the quantitative risk assessment. The remaining stages include:

- Consequence analysis
- Meteorological data analysis
- Population analysis
- Ignition source analysis
- Risk calculation

Those stages are not considered in this paper, but require considerable effort in themselves. The use of automated computerized tools such as SuperChems Expert™ drastically reduces the cost of conducting a quantitative risk assessment, especially if mitigation and sensitivity analyses are to be performed. SuperChems Expert™ offers the most detailed and versatile platform for quantitative risk assessment and facility siting for both fixed facilities and pipelines.

Conclusion

The methodology outlined in this paper provides an effective methodology for streamlining hazard scenario identification and development for large, site wide, refinery quantitative risk assessments. As such, it is a tool which can be used in the overall operational risk management process. Within the paper, practical guidance for the identification and estimation of both “generic” and “non-generic” scenarios is presented. Safeguards such as basic process controls and safety instrumented systems that can be used to mitigate undesirable events and to reduce risks can be considered in the scenario identification and development methodology.

Following this methodology should ensure a thorough and consistent approach for developing hazard scenarios, which should provide a solid basis for the rest of the quantitative risk assessment, and therefore enhance operational risk management.

References

1. CCPS (1989), “Guidelines for Chemical Process Quantitative Risk Analysis”, AIChE/CCPS.
2. CCPS (2001) , “Layer of Protection Analysis – Simplified Process Risk Assessment”, AIChE/CCPS.
3. API Publication 581 (2000), Risk-Based Inspection Base Resource Document.
4. Woodward, J.L. (2007) , “Analyzing hazards of sour water spills” AIChE Spring 2007 Conference.