Risk-Based Approach – Frequency Analysis

Estimating Frequencies of Occurrence and Conditional Probabilities of Loss of Containment Scenarios

An ioMosaic White Paper

Jordi Dunjó, Ph.D.

Marcel Amorós

Neil Prophet

Gene Gorski

Abstract

The primary purpose of this paper is to provide tools, guidance and criteria for finding and appropriately using failure rate data needed to perform a risk-based quantitative analysis. as it is critical to understand of failure rates, their origin and limitations.

Table of Contents

List of Tables

List of Figures

Introduction

A risk-based quantitative analysis requires the estimation of two key variables: the frequency that an event will occur and the consequence, which is the logical and expected impact of that event. Multiple methodologies and approaches are available to reasonably predict the consequences of a chemical release, fire and/or explosion on manufacturing equipment, people and the environment. The technology to do so is well developed and is enhanced when new information becomes available and more powerful computational tools evolve. However, frequencies and probabilities of enabling events are more difficult to predict and criteria must be established and followed from sources such as historical data, experiments and expert opinion. The primary purpose of this paper is to provide tools, guidance and criteria for finding and appropriately using failure rate data needed to perform a risk-based quantitative analysis (see **Figure 01**) as itis critical to understand failure rates, their origin and limitations.

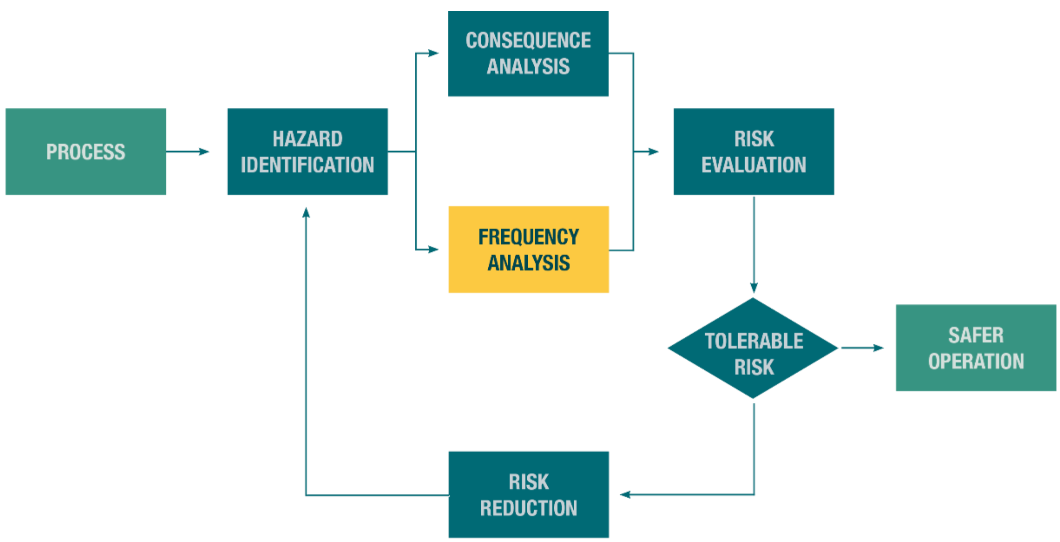

Figure 01: Risk Management Program Simplified Flowchart

The estimation of the likelihood of all Loss of Containments scenarios (LOCs) identified during the hazard identification phase is the main topic of this paper. The frequency analysis can be conducted using historical data, specific plant data (if available), using international references for **generic** process equipment failure rates and developing detailed fault trees for defining **specific** LOCs.

Generic failure data: Failure rate data generated from information collected on plant equipment failures are referred to as plant-specific data. Plant-specific data reflect the plant's processes, environment, maintenance practices and choice and operation of equipment. Data accumulated from a variety of plants and industries, such as nuclear power plants, Chemical Process Industry (CPI) or offshore petroleum platforms, is called generic data. With data from many sources, generic failure rate data can provide a much larger data set.

Specific failure data: Specific failure data should be considered when LOCs have the potential to contribute to the facility risk level. Normally, specific LOCs entail mechanical failure based on the type of process equipment and human errors, such as failure to follow procedures. Process Hazard Analysis (PHA) information can identify LOCs for analysis. Fault Tree Analysis (FTA) is a reliable tool to quantify the LOC frequency.

ioMosaic's Process Safety Office™ (PSO) Suite **[1]** provides software tools to address all steps of a risk-based quantitative analysis - from hazard identification, risk evaluation and the potential for risk reduction through sensitivity analysis. **Table 01** lists the key PSO components intended to identify LOCs and address both generic and specific frequencies.

Table 01: Process Safety Office™ – Key Components for Frequency Analysis

PSO Component	Description
PHAGlobal®	A tool with dedicated templates for generic LOCs identification and a generic frequencies data base
ioLogic™	A powerful tool for fault tree construction
SuperChemsTM	An advanced consequence modeling tool that includes data correlated with probabilities of ignition and equipment failure rates

Generic Loss of Containment Scenarios

Generic LOCs frequencies are a function of the type of process equipment identified by reviewing the Piping and Instrumentation Diagrams (P&IDs) during the hazard identification step **[2]**. Different international standards and guidelines are available for the definition of generic LOCs. While each standard or guideline proposes specific criteria, most of them account for three to five LOCs; i.e., catastrophic failure, large leak, medium leak and small leak. Failure rates proposed in these standards/guidelines are based on available historical data and are validated to produce a consistent set of LOC frequencies.

Table 02 lists some of the established references that address LOCs identification and their associated frequency. **Table 03** lists examples of LOCs and associated frequencies scenarios for pressure vessels and their associated frequencies.

Table 02: Key References for Gathering LOCs Failure Rate Data

References
Guidelines for Quantitative Risk Assessment “CPR-18E; Purple Book” **[3]**
Risk Based Inspection Technology “API RP 581” **[4]**
Failure Rate and Event Data for use with Risk Assessment “UK HSE” **[5]**
Risk Assessment Data Directory; Storage Incident Frequencies “OGP” **[6]**
Offshore and Onshore Reliability Data (OREDA) **[7]**

Other valuable sources of failure rate data are references **[8]**, **[9]**

UK HSE **[5]** provides one of the most complete list of generic process equipment (see **Table 04**). Additionally, very specific generic failure rates can be found as a function of equipment type. For example, reference **[6]** provides specific information for refrigerated storage tanks (see **Table 05**).

ioMosaic

Table 03: Example of LOCs for a Pressure Vessel

Reference	Type of Release	Meaning	Frequency [yr^{-1}]
CPR-18E **[3]**	Instantaneous release of the complete inventory	Catastrophic Failure	5.00E-07
	Continuous release of the complete inventory in 10 minutes at a constant release rate	Large Leak	5.00E-07
	Continuous release from a hole with an effective diameter of 10 mm	Small Leak	1.00E-05
API RP 581 **[4]**	Catastrophic failure of the equipment	Catastrophic Failure	6.00E-07
	Release from a hole with an effective diameter of 4 inches (101.6 mm)	Large Leak	2.00E-06
	Release from a hole with an effective diameter of 1 inch (25.4 mm)	Medium Leak	2.00E-05
	Release from a hole with an effective diameter of 0.25 inches (6.35 mm)	Small Leak	8.00E-06
UK HSE **[5]**	Catastrophic failure of the equipment	Catastrophic Failure	2.00E-06
	Release from a hole with an effective diameter of 50 mm	Large Leak	5.00E-06
	Release from a hole with an effective diameter of 25 mm	Medium Leak	5.00E-06
	Release from a hole with an effective diameter of 13 mm	Medium-Small Leak	1.00E-05
	Release from a hole with an effective diameter of 6 mm	Small Leak	4.00E-05

Table 04: Examples of Failure Mechanisms for Different Equipment*

Failure Mechanism	Main Item	Specific Items Included
Mechanical	Vessels	Ambient Temperature and Pressure Vessels; i.e., large, small and medium, non-metallic / plastic
		Refrigerated Vessels; i.e., Liquefied Natural Gas (LNG) (, Liquid Oxygen (LOX)
		Pressure Vessels; i.e., Chlorine, Liquefied Petroleum Gas (LPG), Spherical
		Chemical Reactors
	Components	Valves
		Pumps
		Hoses and Couplings
		Flanges and Gaskets
	Pipework	Pipework
	Pipelines	Buried
		Above Ground
		Compressors
Bulk Transport	Tankers	ISO Tankers
		Road Tankers (i.e., LPG Road Tanker, Incompatible Deliveries)
		Rail Tankers
	Ship Freight	Ship Hardarms
Moveable Storage	Containers	Drums 1 tone
		Drums 210 liters
		Cylinders
		Intermediate Bulk Containers (IBCs)
		Small Containers

***Based on reference [10]**

Table 05: Refrigerated Storage Tank Leak Frequencies*

Tank Design	Catastrophic Failure [yr^{-1}]		Leak [yr^{-1}]
	Primary Containment[1]	Secondary Containment[2]	Primary Containment
Existing Single Containment Tanks	2.30E-05	7.30E-06	1.00E-05
New Single Containment Tanks	2.30E-06	7.30E-07	1.00E-05
Double Containment Tanks	1.00E-07	2.50E-08	1.00E-05
Full Containment Tanks[3]	1.00E-07	1.00E-08	0.00
Membrane Tanks[3]	1.00E-07	1.00E-08	0.00

[1] The pool area is that of the secondary containment
[2] For single containment tanks this scenario corresponds to bund overtopping
[3] No collapse is considered for these tank types if they have a concrete roof

***Based on reference **[6]**

Specific Loss of Containment Scenarios

Expertise and judgement are required to establish credible characterization of hazardous LOCs. Previous facility PHA studies can provide valuable information on the LOC scenarios. Therefore, it is important to review these studies to include specific scenarios. If information is unavailable, a team-based approach for identification analysis should be performed to identify potential specific LOCs. The evaluation of specific scenarios should be detailed and performed on a case-by-case basis by experienced personnel. Examples include overfilling a vessel, runaway reaction and overpressure due to either a failure of a control valve or a manual blocked outlet. Detailed information on hazard identification can be found in references **[2]**, **[11]** and **[12]**.

Fault Tree Analysis

One of the most used and recognized structural techniques for quantifying the frequency of occurrence of a specific LOC is Fault Tree Analysis (FTA).

The FTA is a deductive methodology which uses a graphical representation of the combination of faults leading to a predefined undesired event, i.e., Top Event (LOC). The methodology uses Boolean logic gates (such as, AND, OR) qualitatively and quantitatively describe (i.e., how equipment failures and human errors combine to cause a main system failure). While Event Tree Analysis (ETA) identifies outcomes from an initiating event (inductive) to final outcomes (see reference **[13]**), FTA proceeds in the opposite direction, identifying most of the basic events that could lead to a predetermined outcome (deductive). As in ETAs, it is conducted after performing hazard identification techniques (see reference **[2]**), the results of which may entail further analysis of specific LOCs. Thus, while FTA is useful for identifying the whole set of initiating events that can lead to an undesired outcome (e.g., runaway reaction), it also can provide tools for quantitative data of Top Event (LOC) frequencies.

The development of a fault tree involves the execution of the following steps:

- Top Event or LOC Definition: Normally defined by using information developed during the execution of related PHAs. Undesired events are used to make the fault tree. One event creates one fault tree.

- Identification of Causes: All causes with probabilities and/or frequencies of occurrence affecting the undesired event are evaluated. These causes are then numbered and sequenced in the order of occurrence.

- Fault Tree Development: Trees are based on Boolean logic which define the major characteristics of the fault tree, accounting for the sequence of all identified causes from the Top Event up to the basic events. The key symbols to be used during the fault tree development stage are listed in **Table 06** and an example of a generic fault tree is illustrated in **Figure 02**.

- Fault Tree Evaluation: Using Boolean methodology, the final Top Event frequency of occurrence is calculated by the estimated frequencies and probabilities of the interrelated causes identified during the fault tree development. The numerical solution of the fault tree involves the determination of the *****"Cut Sets," which allows for quantifying the likelihood of the top event and conducting a sensitivity analysis for the identification of the key causes leading to the top event.

*****Cut sets are unique combinations of component failures that can cause system failure. Specifically, a cut set is said to be a minimal cut set if, when any basic event is removed from the set, the remaining events collectively are no longer a cut set. Minimal cut sets can be used to understand the structural vulnerability of a system. The longer a minimal cut set is, the less vulnerable the system (or top event in fault trees) is to that combination of events. Also, numerous cut sets indicate higher vulnerability. Cut sets can also be used to discover single point failures, which is whereone independent element of a system causes an immediate hazard to occur and/or causes the whole system to fail.

Table 06: Fault Tree Analysis Symbols

Type	Description	Symbol
Event	**Primary Event – Basic**: failure or error of a system component or element	
	Primary Event – External: normally expected to occur	
	Primary Event – Undeveloped: event with insufficient available information	
	Primary Event – Conditioning: conditions that restrict or affect logic gates	
	Intermediate Event: event that needs further development until ensuring a basic event	
Gate	**OR**: the output occurs if any input occurs	
	AND: the output occurs only if ALL inputs occur	
	Exclusive OR: the output occurs if exactly one input occurs	
	Priority AND: the output occurs if the inputs occur in a specific sequence specified by a conditioning event	
	Inhibit: the output occurs if the input occurs under an enabling condition specified by a conditioning event	
Transfer	**Transfer IN / Transfer OUT**: connects the outputs (IN) or the inputs of related fault trees (OUT)	

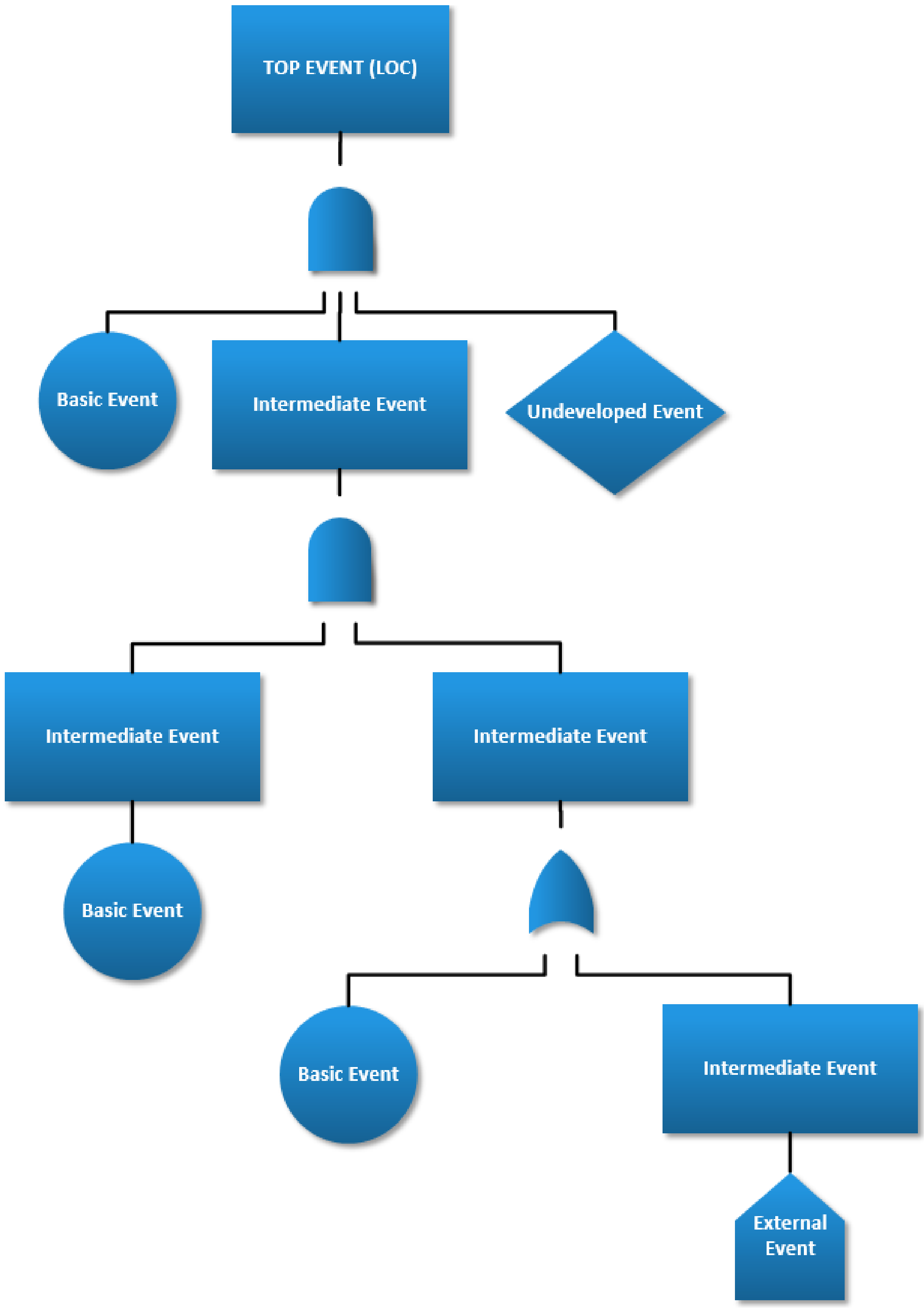

Figure 02: Generic Fault Tree Example

Frequency of Occurrence of All Outcomes

Reference **[14]** introduced the Event Tree Analysis (ETA) as a useful tool for identifying ALL potential outcomes from generic and/or specific LOCs. ETA is valuable for quantifying the final frequency of occurrence of all identified outcomes when the LOC frequency is known and when probabilities of enabling considered during the development of the event tree are also known. **Figure 03** illustrates the generic structure of an event tree.

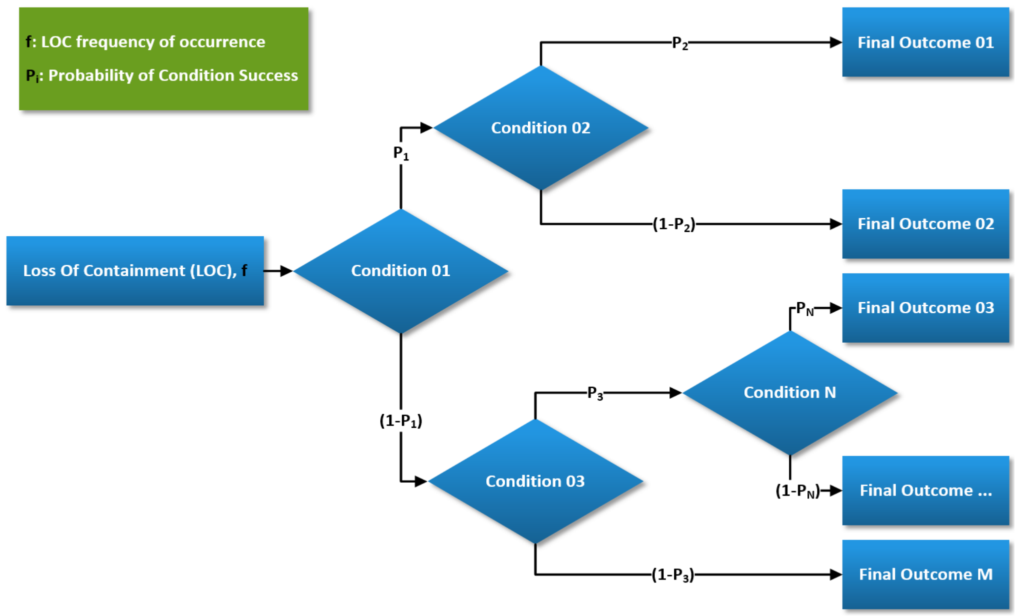

Figure 03: Generic Event Tree Structure Example

By connecting the fault tree and event tree structures, the hazardous scenario is completely characterized. This is the definition of the Bow-Tie methodology, defined as a visual diagram capable of providing with an overview of all the sequence of causes leading to the LOC (fault tree) and all outcomes that conditionally could arise (event tree). **Figure 04** illustrates a generic example of the Bow-Tie approach. The center of the diagram is the LOC, the left-hand side is the fault tree portion and the right-hand side is the event tree portion. Finally, note that for estimating the final outcome frequencies, it is necessary to quantify the probabilities of the enabling events that were considered during the event tree construction. The following section discusses guidance on estimating probabilities.

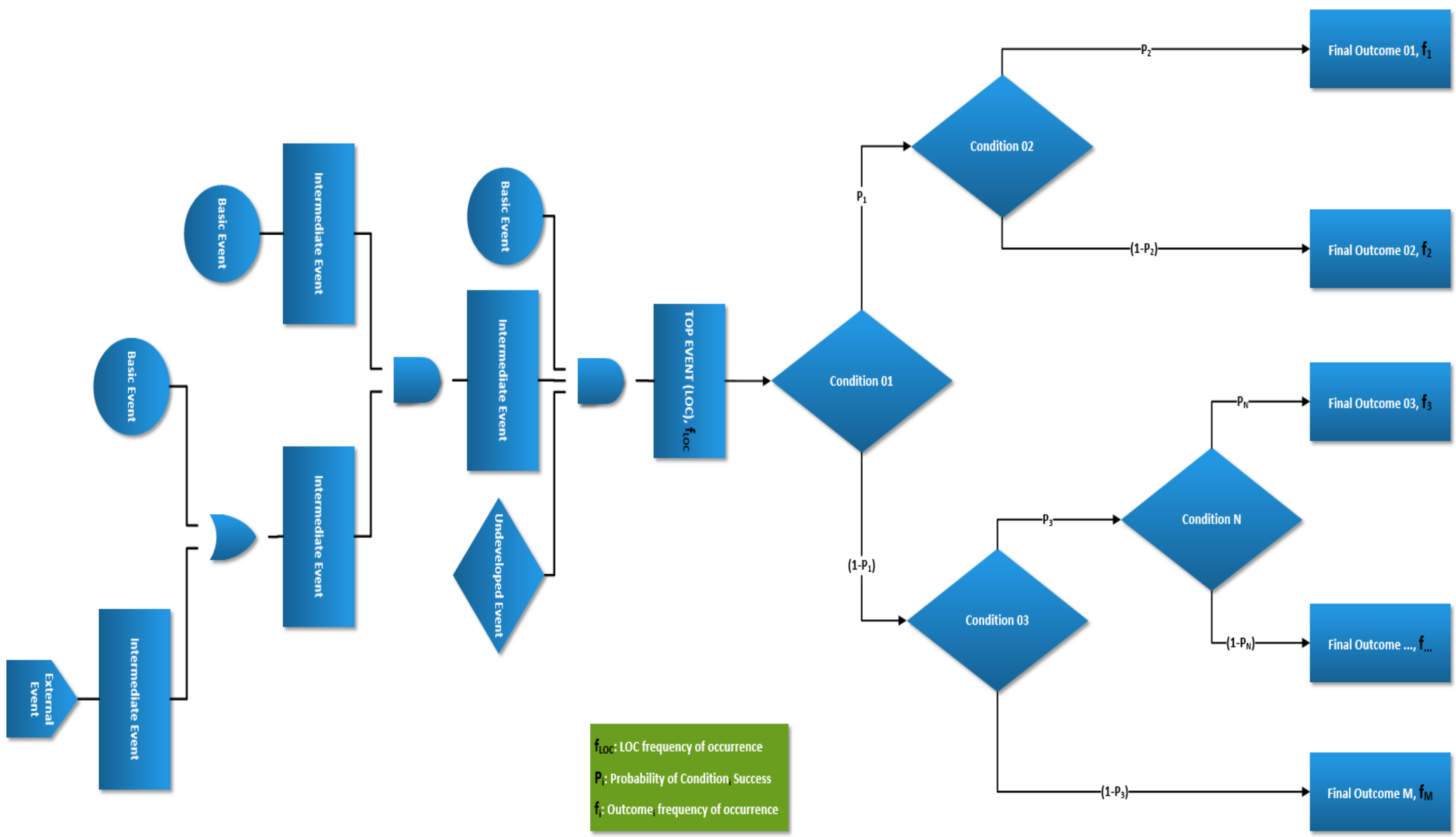

Figure 04: Example of a Bow-Tie Diagram

Note that if the frequency of the LOC has been is a generic value, then the fault tree portion is omitted and only the event tree portion is needed for the complete overview of a hazardous scenario.

Enabling Events and Condition Probabilities

When developing a risk-based quantitative approach, most of the LOCs of interest that contribute to the risk level are toxic and/or flammable. Toxic releases do not require taking into account enabling events to predict a final outcome, which is toxic dispersion. However, flammable releases require identifying the enabling events to characterize potential fires and explosions, or if it is not ignited, predict outcomes with no serious consequences. Accordingly, the main purpose of this section is to provide criteria that can be used to estimate the probability of ignition for a flammable gas and/or liquid released to the environment. The immediate and delayed ignition probabilities are the two key enabling events that are addressed. However, the identification of potential ignition sources in the facility is the first step for addressing their probabilities. Some potential ignition sources to be considered are listed in **Table 07**.

Table 07: Potential Ignition Sources

Potential Ignition Sources
Welding and machine shops
Smoking shelters
Diesel generators
Diesel driven engine pumps,
Power generation, etc.
Hot surfaces,
Flames and hot gases Mechanically generated sparks
Static Electricity
Adiabatic compression and shock waves
Exothermic reactions, including self-ignition of dusts
Fire heaters
Boilers

Based on contents illustrated in reference **[14]**, it can be observed that until the 1990s, many companies maintained groups of process safety specialists whose experience and expertise in different areas allowed in-house problem solving. Often, companies maintained safety test laboratories and performed safety research as well. Unfortunately, as safety technology has advanced it has become more complicated and difficult for most companies to apply it. Reference **[14]** addresses one of the most difficult areas; i.e., estimating the probability of ignition of a given vapor cloud with the aim to develop:

- A standardized methodology for estimating probability of ignition that is open-source and can be applied consistently across the process industry
- Methods and tools that allow a user to estimate ignition probability quickly
- Ability to account for mitigation measures to reduce ignition probability

Accordingly, criteria for detailed ignition probabilities estimation can be found in reference **[14]**.

However, when risk-based quantitative assessments have to be developed with the aim to estimate the risk level of an entire refinery, a detailed estimation of ignition probabilities would be time-consuming and expensive. Instead, internationally recognized criteria are used for these studies. The following two sections are intended to provide criteria and guidelines for estimating immediate and delayed ignition probabilities.

Finally, an additional sub-section has been developed with the aim to account for the quantification of enabling events correlated with safeguards installed in the process that contribute on the reduction of the outcomes frequencies. These safeguards can be classified as Safety Instrumented Systems (SIS), which require the estimation of the Probability Of Failure on Demand (PFD) and specific Fire & Gas Detectors (FGD), which are a particular case of SIS when following criteria from ISA 84.07 **[15]**.

Probability of Immediate Ignition

Cox et al. **[10]** estimated immediate ignition probability for gases and liquids as a step-function of the leak flow rate. Starting from the previous work of Kletz **[16]** and on the basis of data from Dahl et al. **[17]**, they provide the method which is most widely used in modern risk assessments. The probabilities as a function of release rate are listed below in **Table 08**.

Table 08: Immediate Ignition Probability Criteria - Example

Release Rate	Probability of Ignition		Probability of Explosion given ignition
	Gas/Vapor	Liquid	
Minor (≤ 1 kg·s^{-1})	0.010	0.010	0.04
Major (1-50 kg·s^{-1})	0.070	0.030	0.12
Massive (≥ 50 kg·s^{-1})	0.300	0.080	0.3

Probability of Delayed Ignition

The probability of delayed ignition caused by an ignition source can be modeled as:

$$P(t) = P_{Present} \cdot (1 - e^{-\omega t}); \quad \text{where:}$$

- P(t): probability of an ignition in the interval time 0 to t (-)
- $P_{Present}$: probability that the source is present when the cloud passes (-)
- ω: ignition effectiveness (s-1)
- t: time (s)

The ignition effectiveness, ω, can be calculated given the probability of ignition for a certain time interval. **Table 09** lists the probability of ignition for a time interval of one minute for many sources **[3]**.

Table 09: Delayed Ignition Probability Criteria - Example

Type of Ignition Source: Point	Probability of Ignition [-]
Motor Vehicle	0.4
Flare	1.0
Outdoor furnace	0.9
Indoor furnace	0.45
Outdoor Boiler	0.45
Indoor Boiler	0.23
Ship	0.5
Ship transporting flammable materials	0.3
Fishing vessel	0.2
Pleasure craft	0.1
Diesel Train	0.4
Electric Train	0.8
Type of Ignition Source: Line	**Probability of Ignition [-]**
Transmission line	0.2 per 100 m
Road (i.e., it is a function of the average traffic density)	To Be Determined
Railway (i.e., it is a function of the average traffic density)	To Be Determined
Type of Ignition Source: Area	**Probability of Ignition [-]**
Chemical plant	0.9 per site
Oil refinery	0.9 per site
Heavy industry	0.7 per site
Light industrial warehousing	as for population
Type of Ignition Source: Population	**Probability of Ignition [-]**
Residential (i.e., function of the average number of people present in the population source)	0.01 per person
Employment force (i.e., function of the average number of people present in the population source)	0.01 per person

Other Enabling Events - Conditions

Safety Instrumented Systems (SIS), Fire and Gas Detectors (FGD), Deluge Systems, Sprinklers, Pressure Relief Valves (PRVs), etc. are examples of mitigation measures that can be taken into account during the development of an event tree. However, the credibility of these additional conditions must be justified via a robust probability of success that is technically defendable and proven when used during the event tree development.

For example, in an effort to formalize and standardize the process for designing fire and gas systems, industry experts developed the ISA 84.00.07 Technical Report **[15]**. This report has built on the performance-based quantitative approaches of the IEC 61511 standard **[18]**, including safety integrity level (SIL) and added requirements specific to fire and gas detection arrays, notably coverage requirements. Since its release, most sophisticated process industry companies have incorporated the concept of achieving quantitative coverage targets into their fire and gas design philosophy. These targets allow process safety engineers to account for fire and gas detectors as credible safety measures when a fire and gas mapping study has been developed in the facility (see **Figure 05**). The reliability evaluation of FGS differs from SIS and the following key parameters have to be quantified for Fire and Gas System (FGS) design purposes:

- FGS Detection Coverage: The statistical probability that a fire or gas release is detected by the system.
- FGS Availability: An evaluation of the probability that a FGS component will fail to function as intended, which would inhibit the FGS from activation; i.e., Probability of Failure on Demand (PFD). This safety availability calculation is very similar to the SIL calculations performed for a typical Safety Instrumented System (SIS) intended to prevent the hazardous scenario. With the aim to justify the availability of FGS, requirements established in the generic IEC 61511 and the specific ISA TR84.00.07 must be complied.
- Mitigation Effectiveness: An additional condition intended to quantify the probability that the consequence of the gas leak will be mitigation.

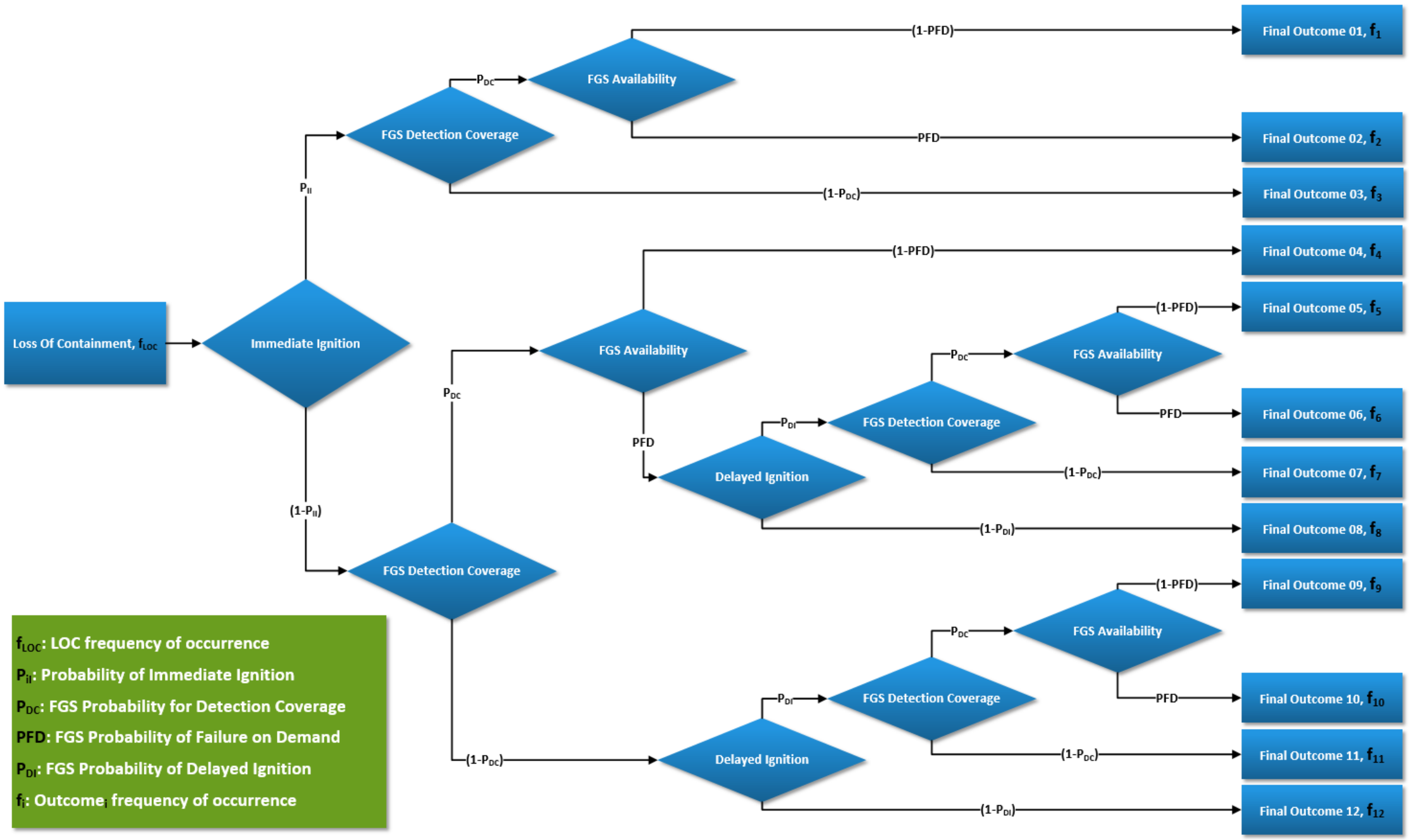

Figure 05: Generic Event Tree with Fire and Gas Detectors

Conclusions

The primary purpose of this paper is to provide tools, guidance and criteria for finding and appropriately using failure rate data needed to perform a risk-based quantitative analysis:

- Internationally recognized references have been identified with the aim to provide robust sources of information with generic failure data.
- The Fault Tree Analysis (FTA) methodology has been identified as a valuable tool for estimating frequencies of specific loss of containment scenarios.
- Enabling events and/or additional conditions have been introduced with the aim to provide with a clear path from identification of generic/specific loss of containment to final outcomes.

References

[1] ioMosaic Corporation, SuperChems™ a Component of Process Safety Office™, ioMosaic; http://www.iomosaic.com/software/process-safety-office-.

[2] Dunjó, J., Amorós, M. Prophet, N., Gorski, G., 2016. "Risk-Based Approach – Hazard Identification. Guidance for Identifying Loss of Containment Scenarios". An ioMosaic White Paper, ioMosaic Corporation.

[3] VROM, 2005. "Guidelines for Quantitative Risk Assessment". Publication Series on Dangerous Substances (PGS3), (CPR-18E).

[4] API-581, 2016. "Risk Based Inspection Technology". American Petroleum Institute Third Edition.

[5] Health and Safety Executive (HSE), 2012. "Failure Rate and Event Data for use within Risk Assessments". United Kingdom.

[6] OGP, 2010. "Risk Assessment Data Directory. Storage Incident Frequencies". International Association of Oil and Gas Producers.

[7] OREDA, 2015. "Offshore and Onshore Reliability Data Handbook". Prepared by OREDA Participant, SINTEF Industrial Management; 6th Edition, Volume I and II.

[8] CCPS, 1989. "Guidelines for Process Equipment Reliability Data with Data Tables". Center for Chemical Process Safety of the American Institute of Chemical Engineers. New York, New York.

[9] CCPS, 1998. "Guidelines for Improving Plant Reliability Through Data Collection and Analysis". Center for Chemical Process Safety of the American Institute of Chemical Engineers. New York, New York.

[10] Cox, A.W., Lees, F. P. and Ang, M.L., 1990. "Classification of Hazardous Locations", Rugby: Instn Chem. Engrs.

[11] Dunjó, J., 2010. "New Trends for Conducting Hazard & Operability (HAZOP) Studies in Continuous Chemical Processes". Ph.D. Thesis Manuscript.
Link: http://www.tdx.cat/bitstream/10803/6481/1/TJDD.pdf

[12] Dunjó, J., 2014. “HAZard & OPerability (HAZOP) Guidelines – Minimizing Risk, Maximizing Hazard Identification”. An ioMosaic White Paper, ioMosaic Corporation.

[13] Dunjó, J., Amorós, M. Prophet, N., Gorski, G., 2016. ”Risk-Based Approach – Consequence Analysis. An Introduction to Consequence Modeling and Determination of Outcomes from Loss of Containment Scenarios”. An ioMosaic White Paper, ioMosaic Corporation.

[14] CCPS, 2014. “Guidelines for Determining the Probability of Ignition of a Released Flammable Mass”. Center for Chemical Process Safety of the American Institute of Chemical Engineers. New York, New York.

[15] ISA-TR84.00.07-2010, 2010. “Guidance on the Evaluation of Fire, Combustible Gas and Toxic Gas System Effectiveness”, Version 1.

[16] Kletz T A, 1977. “Unconfined Vapour Cloud Explosions”. Loss Prevention, Vol 11, p 50, American Institute of Chemical Engineers. New York, New York.

[17] Dahl E., Bern T.L., Golan M., Engen G., 1983. “Risk of Oil and Gas Blowout on the Norwegian Continental”.

[18] IEC 61511, 2016. “Functional Safety – Safety Instrumented Systems for the Process Industry Sector – Part I, Part II and Part III”. International Electrotechnical Commission.