

## Operational Risks in QRAs

Angel Casal<sup>\*a</sup>, Håkon Olsen<sup>b</sup>

<sup>a</sup> Lloyd's Register Consulting - Energy Ltd, WTC Moll Barcelona s/n, Edif. Sur, 2a planta, 08039 Barcelona, Spain

<sup>b</sup> Lloyd's Register Consulting - Energy AS, Havnegata 9, 7010 Trondheim, 7462 Trondheim, Norway  
[angel.casal@lr.org](mailto:angel.casal@lr.org)

Quantitative Risk Assessments (QRAs) are instrumental in critical safety decisions such as licensing operations, siting equipment and occupied buildings and periodically investing in safeguarding as part of continuous risk-reduction programmes. QRAs are mostly based on process information such as Piping and Instrumentation Diagrams (P&IDs) and Heat and Material Balances (H&MBs). This basic information is sufficient to identify inventories of hazardous substances within isolatable pressure-containing segments, and the number and type of mechanical component within the segments to estimate the likelihood of releases.

However, recent history is showing several accidents where mechanical components such as those identified in standard QRAs did not fail, prior to the release. We call these accidents operational accidents.

Operational accidents are rarely found in current QRAs. Consequently, this raises the question of whether operational risks are adequately covered in QRAs to ensure the calculated risk pictures are realistic and valid for the above mentioned critical decisions.

This paper looks at some of these accidents to illustrate operational risks and discusses some of the uncertainties present in current QRAs such those associated with failure rates provided in widely-accepted databases. The paper proposes a methodology for including operational risks in QRAs systematically using existing Process Hazard Analysis (PHA) techniques such as HAZID, HAZOP, Layers of Protection Analysis (LOPA) and Fault Tree Analysis (FTA).

### 1. Current practice in QRAs

The vast majority of onshore and offshore Quantitative Risk Assessments (QRAs) identify process-related hazards using the following methodology:

1. Identification of hazardous substances (toxic, flammable, etc.) via desktop exercises using process information such as Heat and Material Balances (H&MBs); or team-based reviews such as Hazard Identification (HAZID) studies.
2. Identification of isolatable process segments containing hazardous substances and process conditions such as inventory, pressure, temperature, flow, composition, etc. based on Process Flow Diagrams (PFDs), Piping and Instrumentation Diagrams (P&IDs) and H&MBs.
3. A "parts-count" is undertaken based on P&IDs, and relevant discretised leak sizes are defined for each segment based on distributions of leak sizes.
4. Hazardous releases are postulated for each segment based on the relevant leak sizes, and the frequency of each leak size is assessed using generic failure databases and the parts-count. Frequencies of final events are calculated with conditional probabilities in Event Tree Analysis (ETA).
5. Consequence modelling is carried out and, risk is calculated for all hazardous releases, and evaluated against risk acceptance criteria to enable decisions based on the resulting risks.

The above methodology has been used for years for demonstrating that the risks are acceptable compared with risk acceptance criteria. This approach has worked well for external risk assessments i.e. risks for the public beyond the boundary of the facility; however, this might not be the case for onsite risk studies.

## 2. Real accidents vs. QRA accidents

Recent history is showing several accidents where mechanical failures of pressure-containment equipment and components such as those identified in standard QRAs was not the primary cause for the release. These incidents are rarely included in standard QRAs and therefore one could question whether the calculated risk picture for a facility is realistic. We will refer to these accidents as “operational accidents”.

A review of major accidents between 2000 and 2014 has been undertaken from the following sources: Marsh (2014) and US EPA, US CSB and UK HSE (2014). The review concentrated in large accidents with severely adverse consequences such as fires, explosions and significant toxic releases resulting in a fatality or property loss exceeding 100 m\$. These accidents are presented in Table 2 in the Appendix.

According to the primary causes, the majority of these accidents occurred due to causes other than standard mechanical degradation of pressure-containing equipment such as vessels, tanks and piping. The causes of these major accidents are very diverse. Based on a review of these accidents and Lloyd’s Register experience in process safety, the following are the most common causes of operational accidents:

- Inadvertent opening to the atmosphere of pressurized equipment due to operator error;
- Liquid overflow of columns, vessels, storage tanks;
- Gas blow-by;
- Confined explosion in equipment such as storage tanks, furnaces, boilers, etc.;
- Liquid releases through flare;
- Tube failures in shell-and-tube heat exchangers;
- Runaway reactions; and,
- Reverse flows i.e. flammable explosion in combustion air lines.

There may be many reasons why these accidents do not appear in standard QRAs. The following paragraphs attempt to explain the reasons why.

One possible reason is that standard QRAs normally only include hazards relevant to the steady-state mode of operation and typically do not include other modes such as shutdowns, restarts, on-line maintenance, etc. As it can be seen from the list of accidents presented in in Table 2 in the Appendix, many accidents occurred in in these abnormal modes of operation.

Other potential explanation can be found in the assumptions commonly postulated in standard QRA studies, some of which are briefly explained below:

- Component failure rates are representative for all possible failure modes resulting in releases from these components and not only mechanical degradation mechanisms such as human errors, process excursions, etc.
- Inherent hazards of materials as per the Material Safety Datasheets (MSDS) are representative for the all hazards associated with incidents involving these substances. Unwanted chemical reactions such as runaways would be excluded as per this assumption.
- Prevention barriers are excluded and only mitigation barriers are included. To fully understand and evaluate the risk of operational accidents, detailed understanding of the causes and the barriers to prevent them is required which increases complexity. This approach has been applied for many years in other risk studies such as the Layers of Protection Analysis (LOPA), and Fault Tree Analysis (FTA) with good results, although this is rarely used in standard QRAs.

Other limitations to including operational hazards in QRAs could be that depending on the project phase, Process Hazard Analyses (PHAs) such as HAZOPs might not be available for early design stages such as concept or Front End Engineering Design (FEED).

Despite the above-mentioned reasons, leaving operational hazards out of QRAs raises serious issues over the completeness and accuracy of the calculated risk picture.

Finally, another common characteristic of operational accidents is that the consequences were contained within the site boundaries in the majority of cases, with minimal direct consequences offsite other than significant public outrage and damage to reputation. This could mean that including operational accidents in QRAs could be more critical for onsite risk assessments than for offsite studies, but this might be uncertain as there is evidence of operational accidents such as the Bhopal accident in 1984 with extensive damage and casualties beyond the site boundary.

## 3. Uncertainty: failure modes and failure rates

Bearing in mind the above arguments, the following definitions can be made:

- “Fabric failures” are Loss of Containment (LOC) events from valves, piping, vessels, pumps, etc. due to mechanical degradation mechanisms such as corrosion, erosion, external impact, etc. that could initiate a major accident; and,

- “Operational failures” are process upsets that do not result from fabric failures but can lead to a major accident.

However, the difference between “fabric failures” and “operational failures” can be sometimes hard to grasp. Many risk practitioners believe that recognized data sources of failure data have been compiled in facilities where “operational failures” also occurred, and therefore “operational failures” might be already counted as “fabric failures”. That argument could be valid for some operational failures such as process upset, leading to overpressure and LOC. However, this would not be acceptable for leaks where no mechanical failures occurred (e.g. vessel overfilling, drain valve left opened after maintenance, etc.).

One could hope that failure modes and failure rates in recognized data sources are clear and well defined so risk practitioners know what to use in their QRAs. Unfortunately, the failure modes and failure rates quoted in recognized “fabric failure” data sources are debatable.

For example, according to Section 3.2 Assumptions of the Purple Book (2009), “...the failure frequencies for pressure vessels apply to the situation in which failure due to corrosion, fatigue caused by vibrations, operator errors and external impact is ruled out. No additional failure frequencies are included in a default QRA for these specific causes of failure. Consequently, a more generic text has now been included, namely that ‘sufficient measures have been taken against all foreseen failure mechanisms’. Clearly, the failure frequencies in the Purple Book (2009) correspond to “fabric failures” and hence, “operational failures” should be assessed separately and include in the analysis.

The HSE UK failure database for onshore QRAs (2012) provides no clear explanation as to what failure modes are included, so it is not possible to conclude. Furthermore, the HSE UK failure database for offshore QRAs (2015) does not provide either a clear explanation as to what failure modes are included.

The last source consulted was DNV (2009). This publication is based on the HSE UK offshore failure database but it brings a new approach to QRAs. The main difference essentially is that it considers three types of leaks as opposed to the standard practice which was to consider all leaks as full pressure leaks:

- Full pressure releases: these are the same as the former leaks;
- Limited releases: these are leaks that are quickly isolated; and,
- Zero pressure releases: these are leaks that occur with the system being isolated and depressurized for example during maintenance.

The above approach is already recognizing that some failures (e.g. zero pressure releases) are separate to normal leaks, however it is still lacks clarity of what failure modes are actually included in each category.

Consequently, it is difficult to know for sure what failure modes are included in standard failure frequencies database normally used in QRAs.

#### 4. Proposed methodology

Lloyd’s Register has developed an approach to ensure that QRA results are realistic by including operational failures systematically. The approach has been applied to three major QRAs (new chemical plant, existing petrochemical plant and existing oil refinery) with successful results (See Section 5).

The proposed methodology includes quantifying the risk of operational accidents in addition to the standard “fabric failures” QRAs. The methodology relies in a good identification of operational accidents which are not included in the “fabric failures” QRA and hence, it proposes to review process-specific hazard studies such as Hazard and Operability (HAZOP) studies, in addition to the HAZID.

A workflow diagram of the proposed methodology is presented in Figure 1.

The assessment of frequency of operational accidents can be easily done utilizing existing LOPAs or Safety Integrity Level (SIL) studies which typically provide information on causes, barriers and integrity of barriers expressed as the Probability of Failure on Demand (PFD). LOPA and SIL studies are typically available for onshore and offshore assets so this should not be a problem. If such studies are not available, then it is recommendable to assess the frequency using LOPA or FTA.

The assessment of consequences of operational accidents needs to account for the specific conditions of the accident. These conditions may differ from those stated in H&MBs in the cases of process upsets, temperature or pressure excursions, runaways, etc. However, the standard consequence modelling tools are able to deal with these events.

Finally, quantification of the overall risk is carried out by summing the risks from both fabric failure accidents and operational accidents.

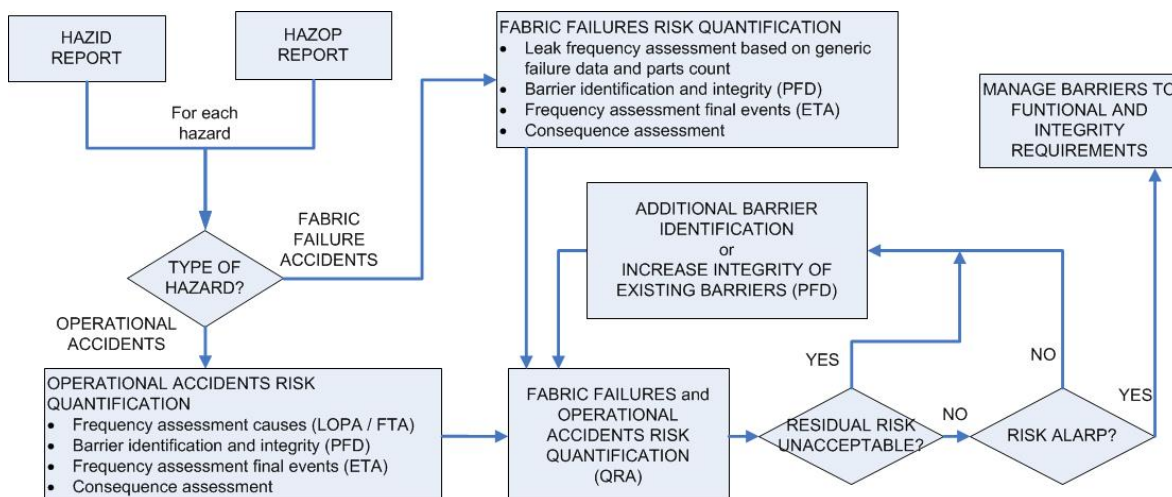


Figure 1: Lloyd's Register methodology for operational risks in QRAs

## 5. Case study, results and validation

As mentioned earlier, this method has been successfully applied in three recent projects. The results presented below are for a QRA including operational accidents in a new chemical plant.

Table 1: Summary of hazards in a recent QRA

Study	Hazards	Major Accidents	Fabric Failures Accidents	Operational Accidents
HAZOP	306	183	66	117
HAZID	70	31	9	22
TOTAL	376	214	75	139

As it can be seen, including operation accidents in this QRA increased the number of accidents in the QRA from 75 to 214, which represents an increase of 185%. This in itself represents a success since the more accidents included, the better the understanding of the risks and the decisions that can be made.

The cumulative assessment of risks taking into account both "fabric failures" and "operational risks" revealed that 80% of the risk at 7 random points nearby the site was caused by the operational accidents. This plant will manufacture a product which is classified as an oxidizer. Hence, leaks of this substance would only increase the probability of fires when in contact with combustible materials. When the operational hazards were included in the QRA, it was found that several process upsets could result in detonations of this product, although the product is not classified as an explosive. This is the reason why there is such a high contribution from operational accidents risks in this QRA. Omitting operational accidents from this QRA would have led to an incorrect picture of the risks for the operators and the public.

To conclude, a remarkable outcome of this study was that the designer and the operator were able to optimize the design using the results of the QRA taking into account realistic risks. Furthermore, the QRA results allowed them to determine integrity requirements for several barriers and the optimal location of occupied buildings onsite. Should the QRA only include fabric failures, this would not have been possible.

## 6. Challenges

The main challenges identified in applying this methodology are summarized below:

- This methodology, albeit comprehensive, is subjective. In particular, distinguishing failure modes that may be covered in generic failure frequencies from those that need to be quantified separately is highly subjective. This activity should be carried out by an experienced process safety engineer;
- Reviewing HAZOP studies is a time-consuming activity thus the overall man hours to prepare the QRA will increase; and,
- The overall complexity of the QRA will increase due to the increased number of scenarios and due to the number of operational barriers included such as the Basic Process Control System (BPCS), alarms and operator response, Safety Instrumented System (SIS), Pressure Relieve Valves (PRVs), fire and gas detectors, etc.

## 7. Conclusions

In conclusion, QRAs are instrumental in risk-based decisions and therefore it is critical that the results are accurate and representative from the facility. However, failure modes and their frequencies are not well explained in commonly used failure rate databases. Furthermore, a review of recent major accidents found that the majority of these accidents would not be included in standard QRAs.

Lloyd's Register has developed a method that combines standard fabric failures with operational accidents. This method relies on a strong identification of operational hazards and assessment of whether they are already covered in the generic failure frequencies.

The complexity and efforts of the QRA will increase. It is estimated that QRA costs will increase between 10% and 20%. However, the results will be more accurate. Furthermore, this enhanced method allows for inclusion of barriers to prevent accidents which enable operators to manage risk actively by investing in barriers.

## Reference

- DNV, 2009, Offshore QRA – Standardised Hydrocarbon Leak Frequencies  
 Marsh, 2014, The 100 largest losses 1974-2013, 23rd Edition  
 Purple Book 2009, "Reference Manual Bevi Risk Assessments", RIVM, The Netherlands, Rev 3.2  
 UK Health and Safety Executive (HSE), 2015, <[www.hse.gov.uk](http://www.hse.gov.uk)> accessed in 2014  
 UK Health and Safety Executive (HSE) 2012, Failure Rate and Event Data for use within Risk Assessments  
 UK Health and Safety Executive (HSE) 2015, Hydrocarbon Releases Database System.  
 U.S. Chemical Safety and Hazard Investigation Board (CSB), 2015, <[www.csb.gov](http://www.csb.gov)> accessed in 2015  
 U.S. Environmental Protection Agency (EPA), 2015, <[www.epa.gov](http://www.epa.gov)> accessed in 2014

## Appendix

Table 2: Major accidents reviewed between 2000 and 2014

Incident / Facility	Year	Location	Deaths/ Injured/ Losses	Causes	Type
Release and explosion in refinery	2000	Mina Al-Ahmadi, Kuwait	5 / 50 / 433m\$	Corrosion and erosion	Mech
Release and fire in chemical plant	2001	Augusta, US	3 / 0 / NA	Runaway	Op
Explosion, release of acid in refinery	2001	Delaware City, US	1 / 8 / NA	Failure of the CO2 blanketing system	Op
Vapour cloud explosion in refinery	2003	Puertollano, Spain	3 / 8 / NA	Unstabilised naphtha in atmospheric tank	Op
LNG release, fire & explosion in terminal	2004	Skikda, Algeria	27 / 74 / NA	Unknown	NA
VCM release and explosion in chemical plant	2004	Illioopolis, US	5 / 3 / Closure	Operator error	Op
Distillate release and fire in refinery	2005	Texas City, US	15 / 170 / 2b\$	Overfill of column	Op
Vapour cloud explosion in depot	2005	Hemel Hempstead, UK	0 / 0 / 1b\$	Overflow of petrol tank	Op
Runaway reaction and explosion in chemical plant	2007	Jacksonville, US	4 / 32 / NA	Runaway on reactor	Op
Gas release and fire in gas plant	2007	Hawaiyah, Saudi Arabia	40 / 9 / NA	Leaking gas pipe	Mech
Explosion and fire in pesticides plant	2008	Institute, US	2 / 8 / NA	Runaway in reactor	Op
Explosion and fire in power plant	2010	Garner, US	4 / 67 / NA	Flushing pipes with natural for cleaning	Op
Fire and explosion in refinery	2010	Humberside, UK	1 / 2 / NA	NA	NA
Explosion and fire in refinery	2010	Anacortes, US	5 / 2 / NA	High temperature hydrogen attack	Mech

Incident / Facility	Year	Location	Deaths/ Injured/ Losses	Causes	Type
Blowout, explosion and fire (offshore drilling)	2010	Gulf of Mexico, US (offshore)	11 / 17 / NA	Gas blow-out	Mech
Fire and explosion in refinery	2011	Fort McKay, Canada	0 / 4 / 380m\$	Coke drum was opened inadvertently	Op
Confined explosion in tank in refinery	2011	Pembroke, UK	4 / 1 / NA	Failure to isolate	Op
Fire and explosion in chemical plant	2012	Map Ta Phut, Thailand	12 / 129 / 140m\$	Operator error during clean-up	Op
Vapour cloud and fire in refinery	2012	Richmond, California, US	0 / 6 / NA	Sulfidation corrosion and pipe rupture	Mech
Fire and explosion in chemical plant	2013	Geismar, Louisiana, US	2 / 76 / 510m\$	Failure in heat exchanger	Op
Ammonium nitrate explosion in depot	2013	West, Texas, US	15 / 160 / Closure	Fire detonated ammonium nitrate storage	Op
Release of hydrocarbons, fire and explosion in refinery	2013	La Plata, Argentina	NA / NA / 500m\$	Flash-floods overwhelmed the drainage	Op
Methyl mercaptan release in refinery	2014	Houston, US	4 / 1 / NA	Unknown	NA
Reactor explosion in chemical plant	2014	Moerdijk, Holland	0 / 2 / NA	Runaway in reactor	Op
Fires and explosions in freight train	2014	Lac-Mégantic, Canada	47 / NA / NA	Unattended oil freight train rolled derailed	NA
Explosion on FPSO	2015	Brazil (offshore)	5 / 10 / NA	Fire in machine room	NA

Mech: Mechanical

NA: Not available

Op: Operational