# HOW LAYER OF PROTECTION ANALYSIS IN EUROPE IS AFFECTED BY THE GUIDANCE DRAWN UP AFTER THE BUNCEFIELD ACCIDENT

Richard Gowland, European Process Safety Centre, Rugby, UK

Prior to the Buncefield explosion, the most likely consequences from the overflow of an atmospheric storage tank could have been assumed to be a flash fire and/or pool fire potentially leading to a single fatality on site. Following the explosion at Buncefield, the most severe human safety consequence should now be assumed to be an explosion that may cause damage to occupied buildings accompanied by a flash fire and multiple pool fires with resultant more severe effects on people and the environment. In the case of the environment, there were effects on the environment caused by the overflow, fire and by the necessary emergency response measures.

When risk assessment has been carried out for storage and distribution facilities possible failures and their possible consequences are normally used as a starting point for addressing the likelihood of their occurring. Layer of Protection Analysis (LOPA) is one of a number of techniques which can be used for risk assessment.

KEYWORDS: Buncefield, Layer of Protection Analysis, Independent Protection Layer, Conditional Modifier

## SCENARIO BASED RISK ASSESSMENT

LOPA has traditionally been based on Scenario-based safety risk assessment, where the technique's calculation estimates the frequency with which a hazardous scenario consequence could occur. For example – a certain number of fatalities within the total exposed population. Using the scenario basis allows a detailed examination of a particular set of risks without necessarily considering all the risks at an establishment. The scenario risk calculation is not an individual risk calculation which might be required for a COMAH Safety Report.

## INDIVIDUAL RISK ASSESSMENT

Individual Risk assessment, where the calculation is typically performed for a specified individual (often characterised by "the person most at risk" and referenced to a specific job role or a physical location).

## SOCIETAL RISK ASSESSMENT

Where the scenario contributes significantly to the societal risk from the establishment an assessment should be made and included in the Safety Report for the establishment. LOPA is not optimal for calculating societal risk.

## ESTIMATING THE CONSEQUENCES OF A BUNCEFIELD-TYPE EXPLOSION

### EFFECTS ON PEOPLE AND STRUCTURES

Given the limitations on current understanding, it is appropriate to apply the precautionary principle as outlined in 'Reducing Risks, Protecting People'.[1]

Currently there is no widely available methodology for estimating the size, shape and rate of development of the flammable cloud that could be formed from a storage tank overflow. Nor can the behaviour of the explosion in the near-field be reproduced by more commonly used models such as the multi-energy model.

In estimating the spread of the flammable cloud, the simplest assumption is to assume that it spreads in all directions equally. This assumption is conservative and is considered reasonable if there are no topographical factors influencing directionality. At wind speeds of less than 2m/s, it is assumed that the wind direction is too variable and hard to measure reliably to have a significant directional impact. However, the spread of the flammable cloud at Buncefield was influenced by local topography and the cloud did not spread equally in all directions even under very low wind-speed conditions. The following distances (Table 1) are considered to be a conservative approximation of the hazard zones for a Buncefield-type explosion and, in the absence of other information, are recommended as a method by which operators can determine relevant hazard zones. Table 1 shows how these zones are interpreted.

Note that the distances in Table 1 are radii from the tank wall as this is the location of the overflow (see diagram below). Bund layouts can vary significantly, so measuring the distances from the bund wall would not provide a consistent approach.

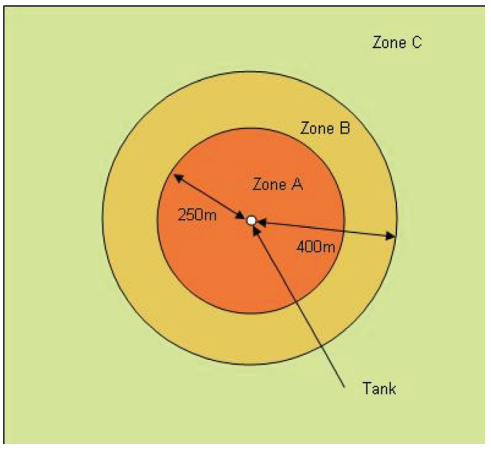
The zones within Table 1 are provided as a conservative basis. The zones may be adjusted on a case by case basis, due to site specific factors.

Other factors that should be considered when estimating the consequences to people are:

a. Hazards resulting from blast overpressure can be from direct and indirect sources. For example, indirect sources of fatal harm resulting from an explosion can be missiles, building collapse or severe structural damage (as occurred at Buncefield).

**Table 1.** Interpretation of Hazardous Zones for a Buncefield-type explosion

| Zone Name | Zone Size (measured from the tank wall) | Comment |
|---|---|---|
| A | r < 250m | HSE research report RR718 [2]on the Buncefield Explosion Mechanism indicates that overpressures within the flammable cloud may have exceeded 2 bar (200 kPa) up to 250m from the tank that overflowed (see Figure 11 within RR718). Therefore within Zone A the probability of fatality should be taken as 1.0 due to overpressure and thermal effects unless the exposed person is within a protective building specifically designed to withstand this kind of event. |
| B | 250m < r < 400m | Within Zone B there is a low likelihood of fatality as the overpressure is assumed to decay rapidly at the edge of he cloud. The expected overpressures within Zone B are 5–25 kPa (see RR718 for further information on overpressures). Within Zone B occupants of buildings that are not designed for potential overpressures are more vulnerable than those in the open air. |
| C | r > 400m | Within Zone C the probability of fatality of a typical population can be assumed to be zero. The probability of fatality for members of a sensitive population can be assumed to be low. |




b. People onsite and offsite within the relevant hazard zones should be considered as being at risk. People within onsite buildings such as control rooms or offices that fall within the hazards zones as described above should be considered at risk unless the buildings are sufficiently blast-rated.
c. The base case should be "normal night time occupancy". Populations just beyond the 250m, e.g. a school or old people's home, should also be considered

ENVIRONMENTAL CONSEQUENCES

This paper also considers the environmental risks associated with a storage tank overflow.

## RISK TOLERANCE CRITERIA

Risk tolerance criteria can be defined for human risk and for environmental risk on the basis of existing guidance.

a. Scenario-based safety risk assessment, where the realistic potential number of fatalities is compared to the risk matrix detailed in Table 2 or an equivalent
b. Scenario-based environmental risk assessment. This type of analysis may be used to determine whether good practice measures (such as those in the COMAH Containment Policy)[3] are reasonably practicable for existing establishments, or whether the existing operations are ALARP.

SCENARIO-BASED SAFETY RISK ASSESSMENT

LOPA, like most risk assessment tools, is suitable for this type of risk assessment, using the following approach:

1. Determine the realistic potential consequence due to the hazardous scenario (in this case the number of fatalities due to an explosion following an overflow from a specific tank);
2. Estimate the likelihood of the scenario; and
3. Locate the consequence and likelihood on the following (or similar) risk matrix (Table 2).

Table 2 is based on the Health and Safety Executive Semi-Permanent Circular "Guidance on 'as low as reasonably practicable' (ALARP) decisions in control of major accident hazards (COMAH)", SPC/Permissioning/12[4]

This assessment should be repeated for each "in-scope" tank in turn. Where there is a large number of "in scope" tanks (for example 10 or more) the aggregate risk from all of the tanks should be considered.

SCENARIO-BASED ENVIRONMENTAL RISK ASSESSMENT

There are currently no published environmental risk criteria for the UK with the same status as those for safety in "Reducing Risks, Protecting People". However, information on tolerability of environmental risk has also been produced

**Table 2.** Risk matrix for scenario-based safety assessments

| Likelihood of 'n' fatalities from a tank explosion per tank per year | Risk Tolerability | | |
|---|---|---|---|
| **$10^{-4}$/yr – $10^{-5}$/yr** | Tolerable if ALARP | Tolerable if ALARP | Tolerable if ALARP |
| **$10^{-5}$/yr – $10^{-6}$/yr** | Broadly acceptable | Tolerable if ALARP | Tolerable if ALARP |
| **$10^{-6}$/yr – $10^{-7}$/yr** | Broadly acceptable | Broadly acceptable | Tolerable if ALARP |
| **$10^{-7}$/yr – $10^{-8}$/yr** | Broadly acceptable | Broadly acceptable | Broadly acceptable |
| **Fatalities (n)** | **1** | **2–10** | **11–50** |

for options assessment in section 3.7 of "IPPC H1: Integrated Pollution Prevention and Control (IPPC) and Environmental Assessment and Appraisal of BAT", Version 6 July 2003[5] (see Table 3a). Operating companies seeking to demonstrate compliance with the COMAH Regulations should adopt an approach consistent with the information provided in Table 3 and with that in their COMAH Safety Reports and PPC Permit applications.

Categories from Table 3 have been aligned to COMAH terminology as follows, "Acceptable if frequency less than" equates" to the "Broadly Acceptable region" "Acceptable if Reduced as Reasonably Practical and frequency between" equates" to the "Tolerable if ALARP region" "Unacceptable if frequency above" equates to the "Intolerable region"

Note that the issue of Environmental Risk tolerability data remains in discussion. For example, the tolerability criteria are now stated by the Environment Agency to be for the whole establishment.

## INITIATING EVENTS

### IDENTIFYING INITIATING EVENTS

Potential causes of tank overflow should be considered in each of the following categories:

Equipment Failures

For example failures of level measurement systems (gauges, radar devices, suspended weights), valves and other components; also failures of site services and infrastructure (e.g. loss of power, utilities, communications).

Human Failures

In particular errors in executing the steps of the filling operation in the proper sequence or omitting steps; and failures to observe or respond appropriately to conditions or other prompts. Possible errors may include but are not limited to:

- Incorrect calculations of the ullage in a tank (leading to an overestimate of how much material can be safely transferred into the tank);
- Incorrect verification of dips or incorrect calibration of level instrumentation;
- Incorrect routing of the transfer (sending material to the wrong tank);
- Incorrect calculation of filling time or incorrect setting of stop gauges;
- Failure to stop the transfer at the correct time (e.g. missing or ignoring the stop gauge and/or succeeding alarms).

External Events

For example:

- Changes in the filling rate due to changing operations on other tanks or due to changes within a wider pipeline network;
- Failure to terminate filling at the source (remote refinery, terminal or ship) on request from the receiving terminal.

One systematic way of identifying initiating events is to prepare a Demand Tree.

## SPECIAL CONSIDERATIONS

### Failures of the Basic Process Control System (BPCS) as Initiating Events

The term "Basic Process Control Function" (BPCF) was developed to differentiate between the **functional** requirement for process control (what needs to be done) and the **delivery** of the functional requirement through the Basic Process Control System. The terminology is intentionally analogous to the terms "Safety Instrumented Function" and "Safety Instrumented System". Although the definitions in BS EN 61511[6] are not always explicit in this area, the authors considered that a BPCS can include either a fully automated control system or a system that relies on one or more people to carry out part of the BPCF. The BPCS is considered to comprise all the arrangements required to effect normal control of the working level in the storage tank, including operational controls, alarms through the BPCS and the associated operator response. For the purposes of the LOPA and the type of scenario under consideration, the BPCS would typically include several of the following:

- A level sensor on the tank;
- Field data marshalling and communications systems;
- Input/output cards;
- Central processing units (logic controller, processing cards, power supplies and visual displays);

**Table 3a.** Heading and introduction from Section 3.7 in "IPPC H1: Integrated Pollution Prevention and Control (IPPC) and Environmental Assessment and Appraisal of BAT", Version 6 July 2003.[5]

| Category | | Definitions |
|---|---|---|
| 6 | Catastrophic | • Major airborne release with serious offsite effects<br>• Site shutdown<br>• Serious contamination of groundwater or watercourse with extensive loss of aquatic life |
| 5 | Major | • Evacuation of local populace<br>• Temporary disabling and hospitalisation<br>• Serious toxic effect on beneficial or protected species<br>• Widespread but not persistent damage to land<br>• Significant fish kill over 5 mile range |
| 4 | Severe | • Hospital treatment required<br>• Public warning and off-site emergency plan invoked<br>• Hazardous substance releases into water course with $\frac{1}{2}$ mile effect |
| 3 | Significant | • Severe and sustained nuisance, e.g. strong offensive odours or noise disturbance<br>• Major breach of Permitted emissions limits with possibility of prosecution<br>• Numerous public complaints |
| 2 | Noticeable | • Noticeable nuisance off-site e.g. discernible odours<br>• Minor breach of Permitted emission limits, but no environmental harm<br>• One or two complaints from the public |
| 1 | Minor | • Nuisance on site only (no off-site effects)<br>• No outside complaint |

**Table 3.** Risk matrix for environmental risk

| | Category | Acceptable if frequency less than | Acceptable if Reduced as Reasonably Practical and frequency between | Unacceptable if frequency above |
|---|---|---|---|---|
| 6 | Catastrophic | $10^{-6}$ per year | $10^{-4}$ to $10^{-6}$ per year | $10^{-4}$ per year |
| 5 | Major | $10^{-6}$ per year | $10^{-4}$ to $10^{-6}$ per year | $10^{-4}$ per year |
| 4 | Severe | $10^{-6}$ per year | $10^{-2}$ to $10^{-6}$ per year | $10^{-2}$ per year |
| 3 | Significant | $10^{-4}$ per year | $10^{-1}$ to $10^{-4}$ per year | $10^{-1}$ per year |
| 2 | Noticeable | $10^{-2}$ per year | $\sim 10^{+1}$ to $10^{-2}$ per year | $\sim 10^{+1}$ per year |
| 1 | Minor | All shown as acceptable | – | – |

- Operators and other workers required to perform the normal control function required to control the level of the storage tank;
- Communication arrangements between operators if more than one operator is required to carry out the control function;
- Final elements (which may be a remotely or locally operated valve or pump)

BS EN 61511 sets a limit on the dangerous failure rate of a BPCS (which does not conform to IEC 61511) of no lower than 1E-5/hr. This limit is set to distinguish systems designed and managed in accordance with BS EN 61511 from those that are not.

The performance claimed for the BPCS should be justified, if possible by reference to actual performance data.

- In the first, and most conservative, approach no credit is taken for any component of the BPCS as a protection layer if the initiating event also involves the BPCS. The failures involving the BPCS may be lumped into a single initiating event or may be separately identified. This approach is consistent with simple applications of LOPA. This approach fully meets the requirements of BS EN 61511.
- The second approach is to allow a single layer of protection to be implemented where there is sharing of components between the BPCS as an initiator and the BPCS as a layer of protection. Where credit for such a

layer is claimed, the risk reduction factor is limited to 10 and the analysis must demonstrate that there is sufficient independence between the initiating event and the protection layer. This approach meets the requirements of BS EN 61511 providing all the associated caveats are applied and adequate demonstrations are made.

ESTIMATING INITIATING EVENT FREQUENCIES

- Where the initiating event is caused by the failure of an item of equipment, the failure rate per year (in hours/year) may be derived from the failure-to-danger rate of the equipment item.
- Where the initiating event is caused by the failure of a person to carry out a task correctly and in a timely manner, the initiating event frequency is calculated as the product of the number of times the task is carried out in a year and the Human Error Probability (HEP) for the task. In this case, the time at risk is already included in the number of times the task is carried out in a year and no further factor should be applied.
- Where the initiating event is taken to be the failure of a BPCS control loop (when it does not conform to BS EN 61511), the minimum frequency which can be claimed is 1E-05 dangerous failures per hour.
- It is important that where probabilities or frequencies are assigned numerical values, these values are supported by evidence.

## ENABLING EVENTS / CONDITIONS

Enabling events and conditions are factors which are neither failures nor protection layers but which must be present or active for the initiating event to be able to lead to the consequence. Examples may include:

- The number of tank-filling operations carried out in a year (which may change as commercial circumstances change);
- The proportion of tank fills which are carried out where the batch size is capable of causing the tank to overflow (it may be that the tank under review normally runs at a very low level and would not normally be able to be filled to the point of overflow by typical batch sizes);
- The tank operating mode (if the tank is on a fill-and-draw operating mode so that the level is more or less static);

**Crosschecking** may qualify for inclusion in the risk assessment:

Tank-filling operations may include a number of cross-checking activities as part of the operation. These may include checks before the transfer starts (eg routing valve line-up, tank dips, available ullage) and periodic checks during the filling operation (eg to confirm the filling rate).

Cross-checks may be represented in the LOPA as factors which modify the initiating event frequency For example, if the initiating event 'Wrong tank line up' where a flow is misdirected is considered, the frequency of misrouting may be adjusted if a suitably rigorous cross-check is carried out. Cross-checks can provide an opportunity to detect and respond to an error condition and may be considered as part of a prevention layer.

Credit for such activities can only be taken if general rules such as effectiveness, independence, 'testability and auditability' are complied with.

## PROTECTION LAYERS

The LOPA methodology relies on the identification of **Protection Layers**, and in specifying protection layers it is important that all the rules for a protection layer are met. A valid protection layer needs to be:

- Effective in preventing the consequence;
  - A protection layer must be **effective**. This requires that the layer has a minimum functionality that includes at least:
    - A means of detection of the impending hazardous condition,
    - A means of determining what needs to be done, and finally
    - A means of taking effective and timely action which brings the hazardous condition under control. and
  - Independent of any other protection layer or initiating event; and
  - Capable of being functionally tested:
    - Whole loop testing (sensor, logic solver, final control element)
    - Complete operator action where required to respond to a detected process deviation. This includes the deviation sensing element, the receipt and understanding by the operator and his action to stop the scenario from developing further; and
  - Auditable:
    - Sufficient record of reliability for failure frequencies and protection layer testing results.

THE BASIC PROCESS CONTROL SYSTEM AS A PROTECTION LAYER

It may be possible to take credit for the BPCS as a protection layer if sufficient independence can be demonstrated between the required functionality of the BPCS in the protection layer and any other protection layer or the initiating event. Clauses 9.4 and 9.5 of BS EN 61511-1 and BS EN 61511-2 present the requirements on the BPCS when used as a protection layer.

RESPONSE TO ALARMS

The BSTG Final Report required operators of gasoline storage tanks to review and where necessary revise the settings of the level alarms on their gasoline storage tanks in accordance with a prescribed methodology. Where the alarm settings meet the requirements of the BSTG Final

Report[7], it is considered legitimate to consider operator response to a high level alarm under suitable conditions. As with other protection layers, the alarm itself is only part of the protection layer. The full protection layer needs to include the alarm, the operator, the machine-operator interface, any communications systems (if communications between operators is required to deliver the required alarm function) and a final element such as a block valve.

SAFETY INSTRUMENTED SYSTEMS

In LOPA studies, the normal convention is that the need for Safety Instrumented Systems (SIS) is determined when all other protection layers have been considered. If an existing SIS complies with BS EN 61511 then a reliability performance consistent with the SIL-rating of the SIS and its design and operation can be claimed.

Other Safety Related Protection Systems

Where relevant may be considered .It is possible to argue that some other protection layers can be considered so long as they meet the requirement for a protection layer set out in the Process Safety Leadership Group Final Report 'Fuel Storage Sites'[8]

## MITIGATION LAYERS

Mitigation Layers are Protection Layers representing **intentional** design or operational measures which become effective once primary containment has been lost. Examples include overflow detection, bunding, fire protection and emergency response.

## CONDITIONAL MODIFIERS (CM)

A Conditional Modifier is a factor which may influence the frequency of a scenario proceeding to the full consequence. For example, it could be assumed that a tank can overflow only when material is transferred into it, either deliberately or in error. If such transfers occur for only part of the time, a Conditional Modifier can be used to allow for this.

The same principles of independence, effectiveness and auditability which apply to protection layers also apply to conditional modifiers. It is important to make sure that the conditional modifier, as defined in the LOPA, is effective in its own right in preventing the consequence without relying on the performance of another conditional modifier or protection layer.

CM 1 – PROBABILITY OF CALM AND STABLE WEATHER

The basis of this report is that the development of a large vapour cloud with the kind of compositional homogeneity that is believed to have existed at Buncefield required low wind speed and stable atmospheric conditions.

CM 2 – PROBABILITY OF IGNITION OF A LARGE FLAMMABLE CLOUD

This conditional modifier represents the probability that the ignition of the vapour cloud from a storage tank overflow is delayed until it is sufficiently large to cause a widespread impact. Alternative outcomes are an earlier ignition that causes a localised flash fire, or safe dispersal of the cloud without ignition.

CM 3 – PROBABILITY OF EXPLOSION AFTER IGNITION

Factors such as ambient temperature; cloud size, shape, and homogeneity; topography; congestion (including that from vegetation); droplet size; fuel properties; and weather conditions may have a significant effect on the probability of an explosion compared to a fire.

This conditional modifier is intended to represent such factors. Research currently being carried out by the Health and Safety Laboratory, when complete, will add more precision to determining this Conditional Modifier.

CM 4 – PROBABILITY THAT A PERSON IS PRESENT WITHIN THE HAZARD ZONE

This conditional modifier can be used to represent the probability that the normal pattern of work or living of a person means that they are only present in the hazardous area at the time of a tank overflow for part of the time. Obviously for a large event like an explosion, this is likely to tend towards 100%.

CM 5 – PROBABILITY OF FATALITY

This conditional modifier may only be used if a single value can be specified for the hazardous scenario.

CM6 – PROBABILITY OF THE ENVIRONMENTAL CONSEQUENCE

This conditional modifier is included to account for any factors additional to those considered elsewhere in the LOPA (for example seasonal factors, if not implicitly included in other factors within the LOPA) that may influence whether the hazardous scenario can cause the defined environmental consequence.

## COMPLETING THE STUDY OF THE SCENARIO SET (CASE)

The process is repeated for the other studies needed where a given hazardous event can be caused by two or more initiating events. It must be remembered that the resulting predicted frequency of the unmitigated hazardous event is aggregated over all relevant initiating events.

It is important that a **sensitivity analysis** should be carried out to explore the sensitivity of the predicted risk levels to the assumptions made.

## CONCLUDING REMARKS

For the full story please go to appendix 2 in : http://www.hse.gov.uk/comah/buncefield/fuel-storage-sites.pdf

## REFERENCES


1. 'Reducing Risks, Protecting People'· (U.K. Health and Safety Executive) http://www.hse.gov.uk/risk/theory/r2p2.pdf
2. HSE Research Report RR718. The Buncefield Explosion Mechanism Phase 1 and 2 http://news.hse.gov.uk/2009/06/25/rr718-buncefield-explosion-mechanism-phase-1-volumes-1-and-2/
3. COMAH Containment Policy U.K. Environment Agency. http://www.environment-agency.gov.uk/static/documents/Business/containmentpolicy_1961223.pdf
4. Health and Safety Executive Semi-Permanent Circular "Guidance on 'as low as reasonably practicable' (ALARP) decisions in control of major accident hazards (COMAH)", SPC/Permissioning www.hse.gov.uk/comah/circular/perm12.htm
5. Integrated Pollution Prevention and Control (IPPC) and Environmental Assessment and Appraisal of BAT", Version 6 July 2003 (U.K. Environment Agency) www.ni-environment.gov.uk/ippc_h1.pdf
6. BS EN 61511 BS EN 61511-2:2004 (British Standards Institute) Functional safety. Safety instrumented systems for the process industry sector. Guidelines for the application of IEC 61511-1 shop.bsigroup.com/en/ProductDetail/?pid.
7. BSTG Final Report (Health and Safety Executive) www.hse.gov.uk/comah/buncefield/bstgfinalreport.pdf
8. Process Safety Leadership Group Final Report 'Fuel Storage Sites' http://www.hse.gov.uk/comah/buncefield/fuel-storage-sites.pdf