Lines of Defence/Layers of Protection Analysis in the COMAH Context

Prepared by **Amey VECTRA Limited**
for the Health and Safety Executive

Lines of Defence/Layers of Protection Analysis in the COMAH Context

Andrew Franks
Amey VECTRA Limited
Europa House
310 Europa Boulevard
Gemini Business Park
Westbrook
Warrington
WA5 7YQ

A Safety Report submitted under the Control of Major Accidents Regulations 1999 (COMAH) should demonstrate that the risks arising from major hazards at the establishment are as low as reasonably practicable (ALARP). In many cases this demonstration will rely on some form of risk assessment. This report considers a number of risk assessment techniques using the Line of Defence / Layer of Protection concept and their usefulness in the COMAH context.

Summary descriptions of several methods (LOPA, TRAM, AVRIM2 and PLANOP) have been prepared. The usefulness of the methods in the context of demonstrating ALARP in COMAH safety reports has been evaluated. Of the techniques considered, it is concluded that LOPA (Layer of Protection Analysis) is potentially a useful tool in performing risk assessments for COMAH purposes.

This report and the work it describes were funded by the Health and Safety Executive. Its contents, including any opinions and/or conclusions expressed, are those of the author alone and do not necessarily reflect HSE policy.

CONTENTS

SUMMARY

A Safety Report submitted under the Control of Major Accidents Regulations 1999 (COMAH) should demonstrate that the risks arising from major hazards at the establishment are as low as reasonably practicable (ALARP). In many cases this demonstration will rely on some form of risk assessment. This report considers a number of risk assessment techniques using the Line of Defence / Layer of Protection concept and their usefulness in the COMAH context.

Summary descriptions of several methods (LOPA, TRAM, AVRIM2 and PLANOP) have been prepared. The usefulness of the methods in the context of demonstrating ALARP in COMAH safety reports has been evaluated. Of the techniques considered, it is concluded that LOPA (Layer of Protection Analysis) is potentially a useful tool in performing risk assessments for COMAH purposes.

TRAM and AVRIM2 were designed as safety report assessment or site audit tools and, in their current form, are not suitable for use as risk assessment tools. However, AVRIM2 in particular contains much information (in the form of checklists, matrices and generic fault trees) that might be useful in constructing a qualitative demonstration of ALARP.

The PLANOP approach may be useful in circumstances where a purely qualitative approach is justified, although at present there is insufficient information available on the method to perform a detailed evaluation.

SCRAM has been designed as a tool for prioritising accident scenarios for more detailed assessment and, at its present stage of development, is not suitable for use as a risk assessment method.

Safety Barrier Diagrams provide a useful, graphical representation of system failure logic and the role of the various layers of protection (barriers) in place. However, as it is currently formulated, the method avoids any explicit calculation of risk. Therefore, barrier diagrams could be used in circumstances where a qualitative approach was justified, but would not be appropriate in situations where use of a semi-quantitative or quantitative approach was demanded.

GLOSSARY

ALARP	As low as Reasonably Practicable
AVRIM2	Dutch safety report assessment tool
BPCS	Basic Process Control System
CCPS	Center for Chemical Process Safety
COMAH	Control of Major Accident Hazards Regulations 1999
DCS	Distributed Control System
E/E/PES	Electrical / Electronic / Programmable Electronic Safety Related System
ERRF	External Risk Reduction Factor
EUC	Equipment Under Control
HAZOP	Hazard and Operability Study
HSE	Health and Safety Executive
IEC	International Electrotechnical Commission
IPL	Independent Protective Layer
LOC	Loss of Containment
LOD	Line of Defence
LOP	Layer of Protection
LOPA	Layer of Protection Analysis
OT	Other Technology
PFD	Probability of Failure on Demand
PLANOP	Protective Layer Analysis and Optimisation
PLC	Programmable Logic Controller
PPE	Personal Protective Equipment
QRA	Quantitative Risk Assessment
SCRAM	Short Cut Risk Assessment Method
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
TRAM	Technical Risk Audit Method

1. INTRODUCTION

1.1 BACKGROUND

A Safety Report submitted under the Control of Major Accidents Regulations 1999 (COMAH) should demonstrate that the risks arising from major hazards at the establishment are as low as reasonably practicable (ALARP). In many cases this demonstration will rely on some form of risk assessment. This report considers a number of risk assessment techniques using the Line of Defence / Layer of Protection concept and their usefulness in the COMAH context.

Following this introduction, the remaining sections of this report are set out as follows:

- Section 2 describes the Layer of Protection Analysis technique (LOPA);
- Section 3 considers the Technical Risk Audit Method (TRAM);
- Section 4 summarises aspects of the AVRIM2 method developed in the Netherlands;
- Section 5 describes the Protection Layer Analysis and Optimisation (PLANOP) tool;
- Section 6 provides information on the Short Cut Risk Assessment Method (SCRAM);
- Section 7 discusses Safety Barrier Diagrams;
- Section 8 evaluates the usefulness of these techniques in the context of COMAH; and
- Section 9 summarises the conclusions of the evaluation.

References are listed in Section 10.

1.2 THE CONTROL OF MAJOR ACCIDENT HAZARDS REGULATIONS 1999

The EC Directive 96/82/EC (the so-called Seveso II Directive) has been implemented in Great Britain as the Control of Major Accident Hazards Regulations (1999), known as COMAH [1]. Application of the Regulations depends on the quantities of dangerous substances present (or likely to be present) at an establishment. Two levels (or ‘tiers’) of duty are specified within the Regulations, corresponding to two different quantities (or thresholds) of dangerous substances. Sites exceeding the higher, ‘upper tier’ thresholds are subject to more onerous requirements than those that only qualify as ‘lower tier’.

The Regulations contain a general duty (Reg. 4), which is applicable to both lower tier and upper tier establishments:

“Every operator shall take all measures necessary to prevent major accidents and limit their consequences to persons and the environment.”

HSE have provided the following interpretation of this general duty:

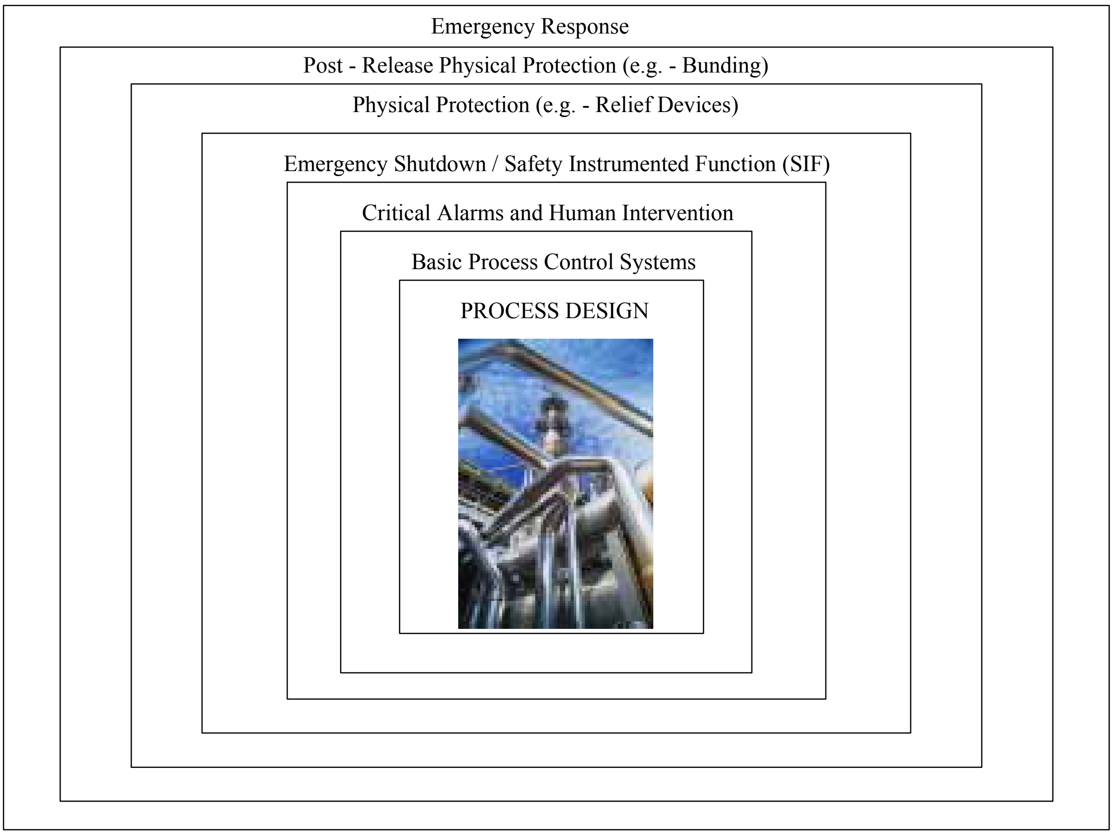
“By requiring measures both for prevention and mitigation, the wording of the duty recognises that risk cannot be completely eliminated. This in turn implies that there must be some proportionality between the risk and the measures taken to control the risk.” [1]

Amongst the duties placed on upper tier sites is the requirement to produce a Safety Report. One of the purposes of the Safety Report is to provide a demonstration that the measures for prevention and mitigation employed by the establishment result in a level of risk that is as low as reasonably practicable (ALARP).

1.3 LINES OF DEFENCE / LAYERS OF PROTECTION

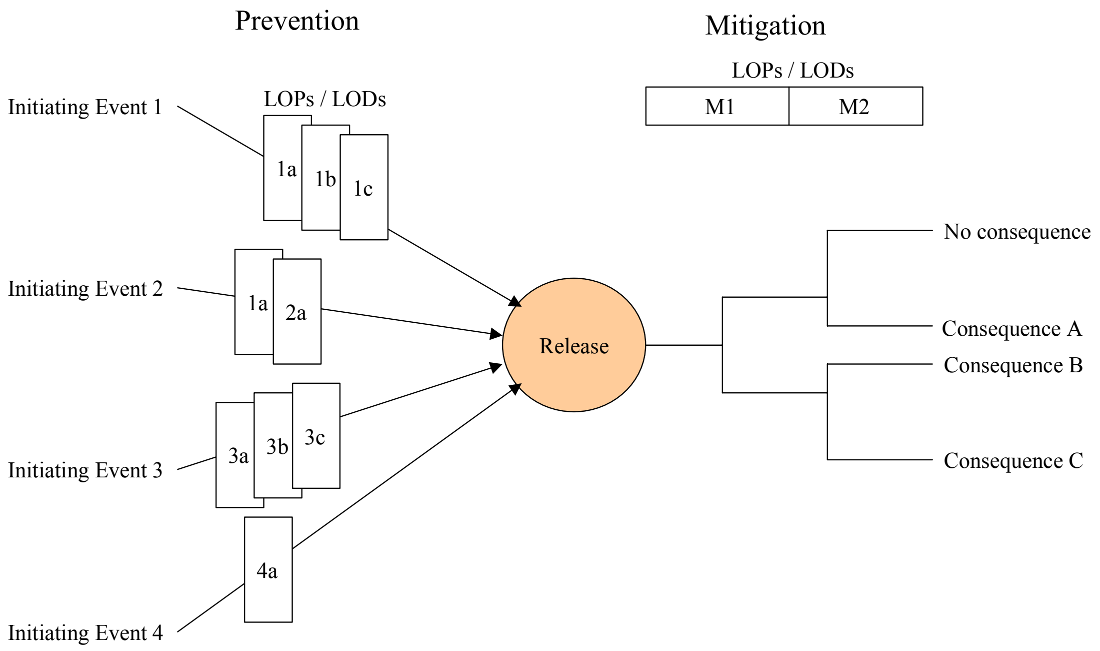
The various measures for prevention and mitigation of major accidents may be thought of as ‘lines of defence’ (LODs) or ‘layers of protection’ (LOPs). These lines or layers serve to either prevent an initiating event (such as loss of cooling or overcharging of a material to a reactor, for example) from developing into an incident (typically a release of a dangerous substance), or to mitigate the consequences of an incident once it occurs. This is illustrated in Figure 1.1 below.

Figure 1.1 Lines of Defence


Emergency Response
Post - Release Physical Protection (e.g. - Bunding)
Physical Protection (e.g. - Relief Devices)
Emergency Shutdown / Safety Instrumented Function (SIF)
Critical Alarms and Human Intervention
Basic Process Control Systems
PROCESS DESIGN

The relationship between initiating events, LODs or LOPs, releases and consequences is shown in Figure 1.2.

Figure 1.2 Initiating Events, LODs / LOPS, Releases and Consequences



Diagrams such as that shown in Figure 1.2 are known as 'bow-ties'. With reference to the diagram, there are several important points to note:

- A release can result from a number of different initiating events. Although four initiating events are shown in Figure 1.2, in reality there can be many more.
- The LOPs / LODs preventing an initiating event from giving rise to a release may differ from initiating event to initiating event. For example, the LOPs / LODs associated with Initiating Event 1 differ from those for Initiating Event 3.
- Conversely, some LOPs / LODs may be common to more than one initiating event. For example, LOP /LOD 1a is shown as being common to both Initiating Events 1 and 2.
- A release can give rise to a range of consequences, depending on the success or failure of the mitigation layers.

Subsequent sections of this report describe various methods for analysing LODs or LOPs, as reported in the technical literature. The usefulness of these methods in the COMAH context has been evaluated and the findings are detailed in Section 8. In most cases the methodologies reviewed are semi-quantitative in nature and therefore the review has focussed on their usefulness where such an approach is justified for the purposes of COMAH.

2. LAYER OF PROTECTION ANALYSIS (LOPA)

The Layer of Protection Analysis (LOPA) technique is described in detail in The American Institute of Chemical Engineers Center for Chemical Process Safety (CCPS) publication on the subject [2]. An overview of the technique is presented here. For more information the reader is referred to the CCPS publication, which contains a number of worked examples and extensive references.

2.1 BACKGROUND

LOPA is one of a number of techniques developed in response to a requirement within the process industry to be able to assess the adequacy of the layers of protection provided for an activity. Initially this was driven by industry codes of practice or guidance and latterly by the development of international standards such as IEC61508 [3] and IEC61511 [4].

In outline, IEC61508 is a standard for managing the functional safety of Electrical / Electronic / Programmable Electronic Safety Related Systems (E/E/PES). The standard is generic and can be applied to any safety related application in any industry sector. The process industry sector specific standard, IEC61511, is under development. A description of the practical application of the standard in the process industry has been presented by Charnock [5].

The standard uses a ‘safety lifecycle’ concept (from concept design, through hazard and risk analysis, specification, implementation, operation and maintenance to decommissioning) to address the steps to achieving functional safety in a systematic and auditable manner.

In essence, implementation of the standard involves, firstly, identification of the hazards associated with the Equipment Under Control (EUC) and the EUC control system. The EUC (a reactor, for example) comprises the plant item (vessel and pipework). The EUC control system is the basic process control system (BPCS, e.g. – DCS or PLC / SCADA). Protection systems relying on other technology (OT, i.e. – not E/E/PES) and External Risk Reduction Facilities (such as blast walls or bunds) are considered to the extent that they contribute to the overall risk reduction in relation to a particular hazard.

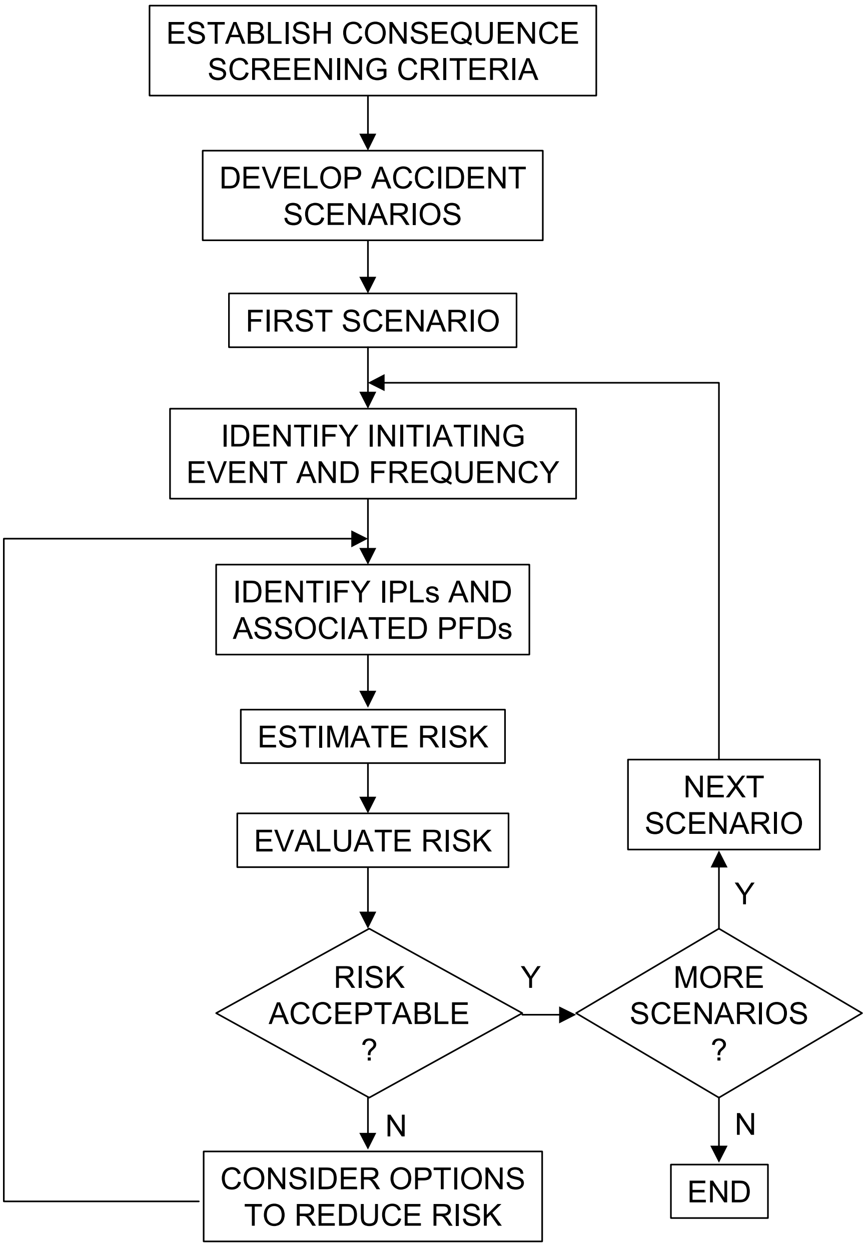
A risk analysis is then conducted, to determine the risks associated with the EUC and EUC control system. If this risk is above the upper level of tolerability then the standard requires that a so-called ‘safety function’ is put in place to reduce the risk to a tolerable level. The safety function will have an associated safety integrity requirement (e.g. – a probability of failure on demand). This is a measure of the risk reduction associated with the safety function. The risk reduction for a safety function can then be allocated between E/E/PE safety-related systems, OT safety-related systems and external risk reduction facilities. Safety functions allocated to E/E/PE safety-related systems are specified in terms of Safety Integrity Levels (SILs), where a SIL is defined in terms of a target range of failure likelihood.

Several methods for performing this risk analysis have been proposed, including LOPA. LOPA has subsequently found much broader application as a relatively simple risk assessment methodology.

2.2 THE LOPA PROCESS

The LOPA process is summarised in Figure 2.1. Each of the steps involved is described in more detail in subsequent sections.

Figure 2.1 LOPA Process


ESTABLISH CONSEQUENCE SCREENING CRITERIA
DEVELOP ACCIDENT SCENARIOS
FIRST SCENARIO
IDENTIFY INITIATING EVENT AND FREQUENCY
IDENTIFY IPLs AND ASSOCIATED PFDs
ESTIMATE RISK
EVALUATE RISK
RISK ACCEPTABLE ?
Y
N
CONSIDER OPTIONS TO REDUCE RISK
MORE SCENARIOS ?
Y
NEXT SCENARIO
N
END

2.2.1 Establish Consequence Screening Criteria

Typically LOPA is used to evaluate scenarios that have been identified in a prior hazard identification exercise using HAZOP, for example. A first step in the LOPA study is commonly to screen these scenarios, usually on the basis of consequences. In a LOPA performed for the purposes of COMAH, for example, the focus would be on major accidents to people or the environment and the analyst would seek to screen out non-major accidents.

This requires that the consequences associated with each scenario are evaluated. There are two main approaches to this:

- To characterise the consequences in terms of the quantity of material released; or

- To calculate the outcome more explicitly, for example in terms of the area corresponding to a given fatality probability, or the expected number of fatalities.

The second of these approaches would normally involve estimating the likelihood of exposed persons being present in the affected area at the time of a release.

2.2.2 Develop Accident Scenarios

In LOPA terms, a scenario comprises a single initiating event – consequence pair. With reference to Figure 1.2, a scenario constitutes a single path through the bow-tie diagram, from left to right. It is important that the scenarios to be considered are well defined prior to proceeding with the remaining steps of the analysis.

In theory the number of scenarios arising from a single hazard identification study could be very large. The diagram in Figure 1.2 represents sixteen separate scenarios (four initiating events x four consequences) around a single release case. In reality however, it may be possible to reduce the number of scenarios that need to be analysed in detail. With reference to Figure 1.2, for example, one of the outcomes is ‘No Consequence’, hence the number of scenarios can immediately be reduced from sixteen to twelve. Application of consequence screening as described above may eliminate further scenarios. It is also possible that some scenarios may be amenable to analysis using simpler, qualitative techniques, whilst other, particularly complex or significant scenarios may require more sophisticated study using quantitative risk analysis (QRA).

2.2.3 Identify Initiating Events and Frequencies

Within a given scenario, the initiating event must lead to the consequence, given failure of the all of the protective layers. The CCPS publication defines three general types of initiating event, as shown in Table 2.1.

Table 2.1 Types of Initiating Event

Initiating Event Type	Examples
External Events	High winds Seismic event Flooding Lightning Fires or explosions in adjacent plant Third party interference Vehicle impact
Equipment Failures	BPCS component failure Software failure / crash Utility failure Vessel / piping failure due to wear, fatigue or corrosion Vessel / piping failure caused by design, specification or manufacturing defects Vessel / piping failure caused by overpressure or underpressure Vibration-induced failure (e.g. – in rotating equipment) Failures caused by inadequate maintenance / repair Failures resulting from temperature extremes Failures resulting from flow surge or hydraulic hammer Failures resulting from internal explosions, decompositions or other uncontrolled reactions
Human Failures	Failure to execute steps of a task properly, in the proper sequence or omitting steps Failure to observe or respond appropriately to conditions or other prompts by the system or process

Initiating events are distinct from root or underlying causes. In general, root or underlying causes create latent weaknesses in the safety system. When a challenge arises or a demand is made on the system, these weaknesses give rise to an initiating event. For example:

- 'Inadequate operator training' is not an initiating event, but is a potential underlying cause of an initiating event of the 'human failure' type.
- 'Inadequate test and inspection' is not an initiating event, but is a potential underlying cause of an initiating event of the 'equipment failure' type.

However, an understanding of the root or underlying causes can be useful when attempting to assign a frequency to the initiating event.

In certain, complex scenarios it may also be necessary to give consideration to enabling events or conditions. Enabling events or conditions are factors that are neither failures nor protective layers. These factors or conditions do not directly cause the scenario, but must be present in order for the scenario to proceed. For example, a scenario may involve failure of a delivery hose during delivery of a dangerous substance due to the tanker being driven away whilst still connected. In order for this scenario to be realised, a delivery must be taking place. The initiating event is therefore a combination of a delivery taking place (an enabling condition) and a human failure in attempting to drive away whilst still connected.

Initiating event frequencies may be obtained from public domain sources [6-10], company data or through the use of simple fault or event trees. The data should be appropriate to the industry or operation under consideration.

LOPA is intended to be a simplified approach giving order-of-magnitude risk estimates. A high degree of accuracy in the failure data is therefore not warranted. In the case of a particularly complex or significant scenario, it may be more appropriate to utilise more sophisticated techniques such as detailed fault tree analysis and/or QRA.

Where enabling conditions or factors are present, initiating event frequencies must be modified to take this into account. In general the initiating event frequency is given by either:

Enabling condition frequency x Failure probability

Or

Enabling condition probability x Failure frequency

When the consequences of the scenario are expressed as a likelihood of fatality or an expected number of fatalities, then the frequency must be modified to account for factors such as the probability of personnel being present in the affected area, the probability of fatality given exposure to the material or harmful effect and, in the case of flammable releases, the probability of ignition. This adjustment may be made to either the initiating frequency or in the calculation of the overall scenario frequency (see section 2.3 below).

2.2.4 Identify Independent Protective Layers (IPLs) and Associated Probability of Failure on Demand (PFD)

Within the LOPA methodology the concept of the Independent Protective Layer (IPL) is well defined and important. The CCPS publication gives the following definition:

"An IPL is a device, system or action which 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. The effectiveness and independence of an IPL must be auditable."

Hence, in order to qualify as an IPL, a device, system or action must satisfy the following constraints. It must be:

- Effective in preventing the consequence when it functions as designed;
- Independent of the initiating event and the components of any other IPL already claimed for the same scenario; and
- Auditable – that is, the assumed effectiveness in terms of consequence prevention and the probability of failure on demand (PFD) must be capable of validation in some manner.

Hence all IPLs are safeguards, but not all safeguards would qualify as IPLs. The CCPS publication gives further, detailed guidance on how to determine whether a safeguard constitutes an IPL for a given scenario [2, Chapter 6]. One important consideration is the possibility of common mode failures, which may not only constitute initiating events, but may also serve to disable certain safeguards. Table 2.2 is reproduced from reference [2] and shows examples of safeguards that are not usually considered IPLs.

Table 2.2 Examples of Safeguards Not Normally Considered IPLs

Safeguard	Comment
Training & Certification	These factors may be considered in assessing the PFD for operator action but are not – of themselves – IPLs.
Procedures	These factors may be considered in assessing the PFD for operator action but are not – of themselves – IPLs.
Normal Testing and Inspection	These activities are assumed to be in place for all hazard evaluations and forms the basis for judgement to determine PFD. Normal testing and inspection affects the PFD of certain IPLs. Lengthening the testing and inspection intervals may increase the PFD of an IPL
Maintenance	These activities are assumed to be in place for all hazard evaluations and forms the basis for judgement to determine PFD. Maintenance affects the PFD of certain IPLs.
Communications	It is a basic assumption that adequate communications exist in a facility. Poor communication affects the PFD of certain IPLs.
Signs	Signs by themselves are not IPLs. Signs may be unclear, obscured, ignored etc. Signs may affect the PFDs of certain IPLs.
Fire Protection	Active fire protection is often not considered as an IPL as it is post event for most scenarios and its availability and effectiveness may be affected by the fire / explosion which it is intended to contain. However, if a company can demonstrate that it meets the requirements of an IPL for a given scenario it may be used (e.g., if an activating system such as plastic piping or frangible switches are used). *Note*: Fire protection is a mitigation IPL as it attempts to prevent a larger consequence subsequent to an event that has already occurred. Fireproof insulation can be used as an IPL for some scenarios provided that it meets the requirements of API and corporate standards.
Requirement that Information is Available and Understood	This is a basic requirement.

Note: Poor performance in the areas discussed in this table may affect the process safety of the whole plant and thus may affect many assumptions made in the LOPA process.

CCPS also gives guidance on assigning an appropriate PFD for various IPL types, together with tables of examples. Values are typically quoted as orders of magnitude.

An important point to note is the difference between IPLs that prevent a scenario from occurring and IPLs that mitigate the consequences of a scenario.

Most preventive IPLs, if they work successfully, simply stop a scenario from developing any further. However, mitigation IPLs, if they operate successfully, do not usually stop the consequences of a scenario altogether, but give rise to consequences of a reduced magnitude. Within LOPA, the less severe consequences would need to be considered as part of a separate scenario.

2.3 RISK ESTIMATION

In general the frequency with which the consequence of the scenario is realised is given by:

$$f_i^C = f_i^I . \prod_{j=1}^{J} PFD_{ij}$$

Where

f_i^C = Frequency of the consequence C associated with the scenario

f_i^I = Frequency of the initiating event i that gives rise to consequence C

PFD_{ij} = Probability of failure on demand for the jth IPL that protects against consequence C for initiating event i.

This equation is valid for low demand situations, that is, where the frequency of the initiating event (f_i^I) is less than twice the test frequency for the first IPL. When the demand exceeds this frequency, the frequency of the consequence or the frequency of demand upon the next IPL in the sequence is given by:

2 x (IPL test frequency, per year) x (IPL PFD)

The extent to which this calculation needs to be modified depends upon the consequences of interest as determined at the outset of the study (see section 2.2.1).

If the consequences of interest are fatalities, then the quantity calculated is an individual risk. For releases of flammable materials the calculation becomes:

$$IR_{i,flammable} = f_i^I . \left(\prod_{j=1}^{J} PFD_{i,j} \right) p_{ignition} . p_{present} . p_{fatality}$$

Where:

$IR_{i,flammable}$ = Individual risk from flammable effect (yr^{-1})

$p_{ignition}$ = Probability of ignition of flammable release

$p_{present}$ = Probability that individual is present when event occurs

$p_{fatality}$ = Probability that individual is killed given exposure to the event

Where a release is significantly influenced by weather conditions, a weather probability may also have to be applied. Similarly, where a release is directional in nature, a probability of the release being directed towards the individual may also have to be applied.

In the case of toxic releases, the equation is:

$$IR_{i,toxic} = f_i^I . \left(\prod_{j=1}^{J} PFD_{i,j} \right) . p_{present} . p_{fatality}$$

Where:

$IR_{i,\ toxic}$ = Individual risk from toxic effect (yr^{-1})

If the consequences of interest are numbers of fatalities, then the quantity calculated is an expected number of fatalities per year for the scenario. The expected number of fatalities per year is also termed the Potential Loss of Life (PLL). The corresponding equations are:

$$PLL_{i,flammable} = IR_{i,flammable}.n_{present}$$

And

$$PLL_{i,toxic} = IR_{i,toxic}.n_{present}$$

Where

$PLL_{i,flammable}$	=	Potential loss of life from flammable event (fatalities.yr^{-1}).
$PLL_{i,toxic}$	=	Potential loss of life from toxic event (fatalities.yr^{-1}).
$n_{present}$	=	Number of persons present and exposed to the event.

Note that this method of calculating PLL assumes that exposed individuals are located relatively close together. Where exposed individuals are distributed over a wide area, a different approach to the calculation of PLL may be required.

In order to calculate the individual risk to a specific exposed person at a given location, it is necessary to sum the risk contributions from each of the scenarios with the potential to affect the individual of interest.

As an alternative to performing the calculations described above, the various parameters may be combined within a matrix or decision table. Typically the table or matrix also embodies the risk criteria for decision making. An example is shown in Figure 2.2, which is extracted from an earlier CCPS reference [11].

Figure 2.2 Decision Table – Safety Integrity Level for Safety Instrumented Function

Number of IPLs

Total number of Independent Protection Layers including the Safety Instrumented Function being classified.

Notes 4, 6

3	NOTE 5	NOTE 5	NOTE 5	NOTE 5	NOTE 5	NOTE 5	NOTE 5	SIL 1	SIL 1
2	NOTE 5	NOTE 5	SIL 1	NOTE 5	SIL 1	SIL 2	SIL 1	SIL 2	SIL 3 NOTE 2
1	SIL 1	SIL 1	SIL 2	SIL 1	SIL 1	SIL 3	SIL 3 NOTE 2	SIL 3 NOTE 2	SIL 3 NOTE 1
	Low	Mod	High	Low	Mod	High	Low	Mod	High
	Event Frequency			Event Frequency			Event Frequency		
	Note 3			Note 3			Note 3		
	Minor			Serious			Extensive		

Consequence Severity

NOTE 6

Notes:

1. One SIL3 SIF does not provide sufficient risk reduction at this risk level. Additional modifications are required.
2. One SIL3 SIF may not provide sufficient risk reduction at this risk level. Additional PHA reviews are required.
3. Event Frequency – Initiating Event Frequency – Frequency that the consequence occurs without any of the IPLs in service (i.e. – frequency of the demand).
4. Event Frequency and Total Number of IPLs are defined as part of the LOPA work.
5. SIF IPL is probably not needed.
6. The Consequence Severity categories and the Initiating Event Frequency categories should be calibrated with the company’s risk criteria.

These tables or matrices usually contain the number of IPLs or the number of IPL credits as one of the parameters. The CCPS publication gives the following definition of an IPL credit:

1 IPL credit is equivalent to a PFD of 1 x 10^{-2}

On this basis, the CCPS book also provides example look-up tables of different IPLs, the associated PFD and the number of IPL credits the IPL attracts.

A further alternative is to present frequencies and probabilities in the form of logarithms. Hence an initiating event frequency of 1 x 10^{-2} yr^{-1} becomes 2 and a PFD of 1 x 10^{-2} becomes 2. If this approach is used, the logarithm is rounded to the nearest integer. Some analysts use a conservative approach of rounding downwards to the next integer (so that 2 x 10^{-2} becomes 1). The calculation becomes:

$$F_i^C = F_i^I + \sum_{j=1}^{J} P_{ij}^{'}$$

Where

F_i^C = the frequency exponent of consequence C of scenario i.

F_i^I = the absolute value of the log of the frequency of initiating event i.

$P_{ij}{}'$ = the absolute value of the log of the PFD of the jth IPL that protects against scenario i.

2.4 EVALUATION OF RISK

The risk may be evaluated by comparing risk reduction options for the same scenario with one another, or by comparing the calculated risk with risk criteria. The CCPS publication gives four basic categories of criteria:

- Criteria that place risk characterisations per scenario in matrices, with parameters of frequency and consequence as guides.
- Criteria that specify a maximum allowable risk (e.g. risk of fatality or financial loss) per scenario.
- Criteria that specify a minimum number of IPLs (or IPL credits) for any specific scenario.
- Criteria that specify a maximum cumulative risk for a process or geographical area.

Following this comparison, a judgement must be made as to whether further action is necessary. Possible actions may include the application of additional IPLs, or a more fundamental change in design to make the process inherently safer (by reducing scenario frequency or consequence, or by eliminating the scenario altogether).

It should be noted that, for the purposes of COMAH, any criteria used in the risk assessment process will need to be consistent with those published by HSE [14].

3. THE TECHNICAL RISK AUDIT METHOD (TRAM)

The Technical Risk Audit Method (TRAM) [12, 13] was developed as a risk based auditing and inspection tool by the UK Health and Safety Executive (HSE) for application at major hazard sites falling within the scope of the COMAH Regulations.

The underlying approach within TRAM is broadly similar to that employed by LOPA, in that scenarios are defined and the associated protective measures (termed Lines of Defence or LODs within TRAM, as opposed to IPLs within LOPA) ascertained. The methodology is implemented as a software package. Information on fault sequences, initiating event frequency, scenario consequences and failure probabilities is input by the analyst. The software determines the number of LODs required to reduce the risks from the scenario to a tolerable level.

Where the number of LODs in place for the scenario under analysis exceeds those predicted as necessary by TRAM, it is assumed that risks may be judged to be ALARP. Conversely, if a requirement for additional LODs is indicated by TRAM, further, more detailed consideration (using QRA, for example) may be necessary.

The TRAM methodology is described in more detail in the sections below.

3.1 LOD RATING

Within TRAM, a LOD rating of 1 is assigned to a measure with a PFD of 1×10^{-1}. That is:

$$\mathrm{LOD}_{\mathrm{TRAM}} = -\log_{10}(p)$$

Where:

$\mathrm{LOD}_{\mathrm{TRAM}}$ = LOD rating.
p = PFD for measure for which LOD rating is required.

Note that this differs from the definition of an IPL credit within LOPA (an IPL credit of 1 equates to a PFD of 1×10^{-2}).

Within TRAM, the protective layer or LOD is more broadly defined than an IPL in LOPA. A LOD has to be independent of other LODs in the fault sequence and of the initiating event, as does an IPL in LOPA. However, a LOD may be a physical condition such as natural heat dispersion or cold weather conditions, whereas these factors would not be considered IPLs in LOPA, not meeting the ‘effectiveness’ or ‘auditable’ criteria.

3.2 FREQUENCY CLASS

Frequency Class F_i is obtained from the initiating event frequency by:

$$F_i = -\log_{10}(f_i^I)$$

3.3 CONSEQUENCE CATEGORY

Within TRAM, the Consequence Category for a scenario must be selected with care, since the Consequence Category incorporates the risk acceptability criteria. This is done to enable the use of a simple numerical process in order to judge acceptability. An explanation is presented below.

The acceptability of individual risk can be determined by summing the individual risk contributions from all of the relevant fault sequences and comparing it with an acceptability criterion value, α_{worker}:

$$IR_{worker} = \sum_{i} f_i^I \prod_{j=1}^{J} PFD_{ij} < \alpha_{worker}$$

Where
IR_{worker} = Individual risk to exposed workers (yr^{-1})

Note that the summation is performed only over those fault sequences with fatal consequences.

A consequence category, C_i, can then be defined such that the following expression, when fulfilled, indicates acceptability:

$$C_i = -\log_{10}\left(\frac{\alpha_{worker}}{m}\right)$$

To relate C_i to α_{worker} it is necessary to estimate the number of fault sequences which can give rise to a worker fatality. If this number is m, then the Consequence Category is given by:

C_i = $-\log_{10}(\alpha_{worker}/m)$

For example, if an acceptable worker risk is $10^{-3}yr^{-1}$ and it is assumed that there are typically 10 such fault sequences contributing to the risk, then in this case m is 10 and α_{worker} is 10^{-3}, leading to a Consequence Category of 4.

With the Consequence Category defined in this way, then the risk from each individual fault sequence will be acceptable if the following condition is satisfied:

$F_i + \Sigma LOD_i - C_i >$ 0

The second term in this equation is the Required LOD Rating, $LOD_{required}$. By rearranging:

$F_i + LOD_{required} \geq$ C_i

A similar equation may be derived on the basis of a consideration of societal (group) risk.

Hence the Consequence Category to be assigned to a given scenario depends on the criterion to be applied. In order to provide guidance, a standard set of Consequence Categories is provided within TRAM, based on a logarithmic scale running from 1 (minor economic consequences) to 6 and beyond (multiple fatalities), and designed to be consistent with published HSE risk criteria [14]. These Categories are shown in Table 3.1.

Table 3.1 TRAM Consequence Categories

Consequence Category	Description
>7	Catastrophic Accident: gross disruption, large numbers of fatalities, extensive media coverage, Public Enquiry, impacts on regulatory framework and law.
>6	Major Accident: significant off-site disruption, many dead and injured, main feature of national news, results in Public Enquiry and prosecutions.
>5	Significant Accident: some off-site disruption, small numbers of dead / many injured, features in national news, legal actions, investigations and compensation claims.
>4	Small Scale Accident: disruption local to site, fatalities limited to workers involved in accident, few serious injuries, mentioned in local news, investigation and compensation claims.
>3	Minor Accident: limited to a small part of the site, injuries / lost time accident, no media coverage, site / company investigation only.
<=3	Limited Accident of low consequence.

3.4 EXCESS LOD RATING

The Excess LOD Rating is used as a measure of the acceptability of the risk from individual scenarios. The Excess LOD Rating is the difference between the required LOD rating for acceptability ($LOD_{required}$, as described above) and the LOD rating of the measures actually present, as determined from the data provided by the assessor concerning the LODs available:

$$LOD_{excess} \quad = \quad LOD_{available} - LOD_{required}$$

In order to be acceptable, LOD_{excess} should have a positive value. Within the TRAM tool, scenarios may be ranked according to LOD_{excess}. Scenarios where LOD_{excess} was less than a small positive value (1, for example) would require further investigation.

4. AVRIM2

AVRIM2 [15, 16] is an assessment and inspection tool developed for the Dutch Labour Inspectorate. The tool is currently used for the assessment of on-site safety reports (Arbeidsveiligheidsrapporten or AVRs) for major hazard sites submitted to the regulator under the requirements of the Seveso II Directive.

The Lines of Defence concept sits at the core of AVRIM2. The tool allows the assessment and inspection of the LODs in place to prevent loss of containment of hazardous materials and of the systems by which a site operator monitors and improves the effectiveness of those LODs. It is this link between the technical measures (the LODs) and the safety management system that distinguishes AVRIM2 from LOPA or TRAM. Poor safety management is seen as a potential 'common cause' failure mode that could result in the failure of a number of LODs.

The tool comprises a number of modules, which assist an inspector in conducting the assessment:

- An Initiating Event Matrix;
- Generic Fault Trees;
- A Benchmark Risk Matrix;
- An Organisational Typing Tool; and
- A Management Control and Monitoring Loop.

Each of these modules is described below.

4.1 INITIATING EVENT MATRIX

The Initiating Event Matrix assists the inspector in determining whether a safety report has considered all of the initiating events relevant to the site in question. The matrix is displayed in Figure 4.1. Direct causes are listed across the top of the matrix and containment types or activities are listed down the left hand side. Each direct cause – containment type combination represents an initiating event (corrosion of pipe, for example). By identifying the relevant containment types / activities present on the site, the inspector may determine the relevant initiating events and compare this list with the safety report contents.

Figure 4.1 AVRIM2 Initiating Event Matrix

Activities	Containment (release points)	Direct Causes of Loss of Containment								
		Corrosion	Erosion	External Loading	Impact	Pressure (High / Low)	Vibration	Temperature (High / Low)	Wrong Equipment / Location	Operator Error
Storage										
	Atmospheric tanks									
	Pressure vessels									
Transfer										
	Pumps									
	Compressors									
	Pipework									
	Ductwork									
Sampling										
	Sampling points									
	Sample									
	Container									
Processing										
	Pumps									
	Compressors									
	Heat exchangers									
	Pipework									
	Pressure vessels									
	Atmospheric tanks:									
	- On ship									
	- On barge									
	- On rail car									
	- On road tanker									
	Loading arms									
	Hoses									
	Pipework									
	Pumps									
	Compressors									

Activities	Containment (release points)	Direct Causes of Loss of Containment								
		Corrosion	Erosion	External Loading	Impact	Pressure (High / Low)	Vibration	Temperature (High / Low)	Wrong Equipment / Location	Operator Error
Designed Release Points										
	Relief valves									
	Explosion panels									
	Drain points									
	Bursting discs									
	Vents									
Special Cases										
	Domino (other sites)									
	Aircraft impact									
	Terrorism / vandalism									
General										
	Flanges									
	Instruments									
	Valve									
	Gaskets									
	Bellows									
	Expansion joints									
	Coolant systems									
	Heating systems									
	Inert systems									
	Air systems									
	Water systems									

4.2 GENERIC FAULT TREES

AVRIM2 contains generic fault trees corresponding to each of the direct causes displayed in the Initiating Event Matrix. In addition, Generic Fault Trees are presented for the cause ‘Exceeds Containment Limit’. The purpose of the fault trees is to assist an inspector in determining whether all relevant, possible scenarios leading to loss of containment have been considered within a safety report. In AVRIM2 terms, a scenario is represented by a minimal cut set (a unique combination of base events necessary and sufficient to lead to the top event) from one of the generic fault trees. These scenarios can in turn be used to determine where a site operator should have LODs in place.

The LODs themselves are linked to base events within the Generic Fault Trees via ‘Checklist Lines of Defence’. These checklists provide a suggested list of the components of a LODs system relevant to the base event.

Four types of LOD are defined:

- Physical LODs which prevent failure of the physical containment itself;
- Process instrumentation and control LODs which prevent failure of the measurement and / or control of the process;
- Barrier LODs which prevent failure of the containment through a protective device or system which diverts material or energy when there is a demand on the containment system; and
- Work system LODs which prevent events that may place demands on physical systems.

The authors state that a system of LODs providing ‘defence-in-depth’ should possess the following components:

- Physical containment;
- Automatic shutdown / shut-off for deviations;
- Physical barriers for diverting mass or energy so that containment limits are not exceeded;
- Systems of work, including response procedures should a deviation occur;
- Protection of personnel against exposure; and
- Emergency preparedness.

Furthermore, a hierarchy for LODs is presented. In order of preference, this is:

1. Eliminate hazard.
2. Reduce level of hazard (inventory reduction / substitution).
3. Contain / control hazard by physical means.
4. Contain / control hazard by systems of work.
5. Protect personnel against exposure:
    a) Personnel not present within effect distance.
    b) Measures that protect a group (strengthen building).
    c) Measures that protect an individual (PPE).
6. Emergency preparedness should controls fail.

In summary, the inspector is required to carry out the following checks:

- That all relevant scenarios have been identified and their LODs specified;

- That the system of LODs prevents and/or protects against all of the failure events within the scenario;
- That the system of LODs has all of the relevant preventive and protective components of a defence-in-depth system;
- That missing LODs have been identified by the operator; and
- That there is a plan for dealing with identified weaknesses.

4.3 RISK MATRIX

Under the Dutch regime, operators are also required to evaluate the risk associated with the various major accident scenarios that have been identified, and to compare the results with risk criteria. The operator develops the risk criteria used.

Typically operators will use a semi-quantitative approach to this risk assessment. In order to give guidance to inspectors when considering the risk assessments within safety reports, a 'benchmark' risk matrix is provided within AVRIM 2. The matrix is shown in Figure 4.2. The corresponding Consequence Severity and Likelihood categories are defined in Table 4.1.

Figure 4.2 AVRIM2 Risk Matrix

Likelihood of Loss of Containment	**Consequence Severity**				
	5 **Severe**	**4** **Major**	**3** **Serious**	**2** **Minor**	**1** **Negligible**
5 Very High	X	X	X	X	O
4 High	X	X	X	O	O
3 Average	X	X	O	O	=
2 Low	X	O	O	=	=
1 Very Low	O	O	=	=	=

KEY	
X	Unacceptably high risk. Company should reduce by prevention / protection.
O	High risk. Company should address cost-benefits of further risk reduction. Inspector should verify that procedures and controls are in place.
=	Acceptable. No action required.

Table 4.1 AVRIM2 Risk Matrix Category Definitions

	Likelihood Scale	**Consequence Scale**
1	Very low. Failure never heard of in the industry. Almost impossible on the installation. <10^{-4} per year.	Negligible. Minor impact on personnel, no loss of production time, <f 10,000 cost.
2	Low. Failure heard of in the industry. Remote, but possible on the installation. <10^{-3} per year.	Minor. Medical treatment for personnel, minor damage, short loss of production time, <f 100,000 cost.
3	Average. Failure has occurred in the company as a whole. Occasional, could occur some time on the installation. <10^{-2} per year.	Serious. Serious injury to personnel (LTI), limited damage, partial shutdown, <f 500,000 cost.
4	High. Failure happens several times a year in the whole company. Possibility of isolated incidents on the installation. <10^{-1} per year.	Major. Permanent injury / health effect, major damage, production stop, <f 1,000,000 cost.
5	Very high. Failure happens several times a year at the installation. Could be repeated incidents on the installation. >10^{-1} per year.	Severe. One or more fatalities, large scale damage, long term production stoppage, >f 1,000,000 cost.

Note: Costs are presented in Dutch Guilders (f).

4.4 ORGANISATIONAL TYPING TOOL

AVRIM2 contains a tool for organisational profiling of a company. This profile then enables a prediction of the possible strengths and weaknesses within the company safety management system to be made. The tool is based on the findings of a structured investigation into inspectors' knowledge and perception of Dutch companies that have to provide a safety report. This investigation also allowed the development of correlations between aspects of an organisation's profile and possible strengths and weaknesses within the safety management system.

4.5 MANAGEMENT CONTROL AND MONITORING LOOP

The Control and Monitoring Loop within AVRIM2 provides inspectors with a model to assist them in evaluation of an operator's safety management system. As mentioned previously, deficiencies within the safety management system are seen as potentially giving rise to common mode failures within the LODs.

The Control and Monitoring Loop is illustrated in Figure 4.3. The management system is seen as acting within a system climate, and acting upon the plant containment systems and personnel. The left hand side of the diagram represents the Control side of the loop, i.e. – the control of human decisions and actions that have an impact on the LODs. The right hand side of the diagram shows the Monitoring side of the loop, i.e. – the monitoring of the performance of the LODs and correction of deviation from required standards, and the improvement of those standards.

Analysis of loss of containment accidents [17] has shown that management could have prevented or corrected deviations that originated from:

- Design
- Construction
- Operation
- Maintenance

The relevant management prevention or recovery measures have been grouped into four key areas:

- Hazard review
- Checking and supervision of tasks
- Routine inspection and testing
- Human factors review

The combination of these areas with the four life cycle phases gives a set of areas for consideration, as shown in Table 4.2. Each life cycle phase is represented by a control and monitoring loop. A more detailed explanation of each component of the loop is provided in [15].

Figure 4.3 AVRIM2 Control and Monitoring Loop

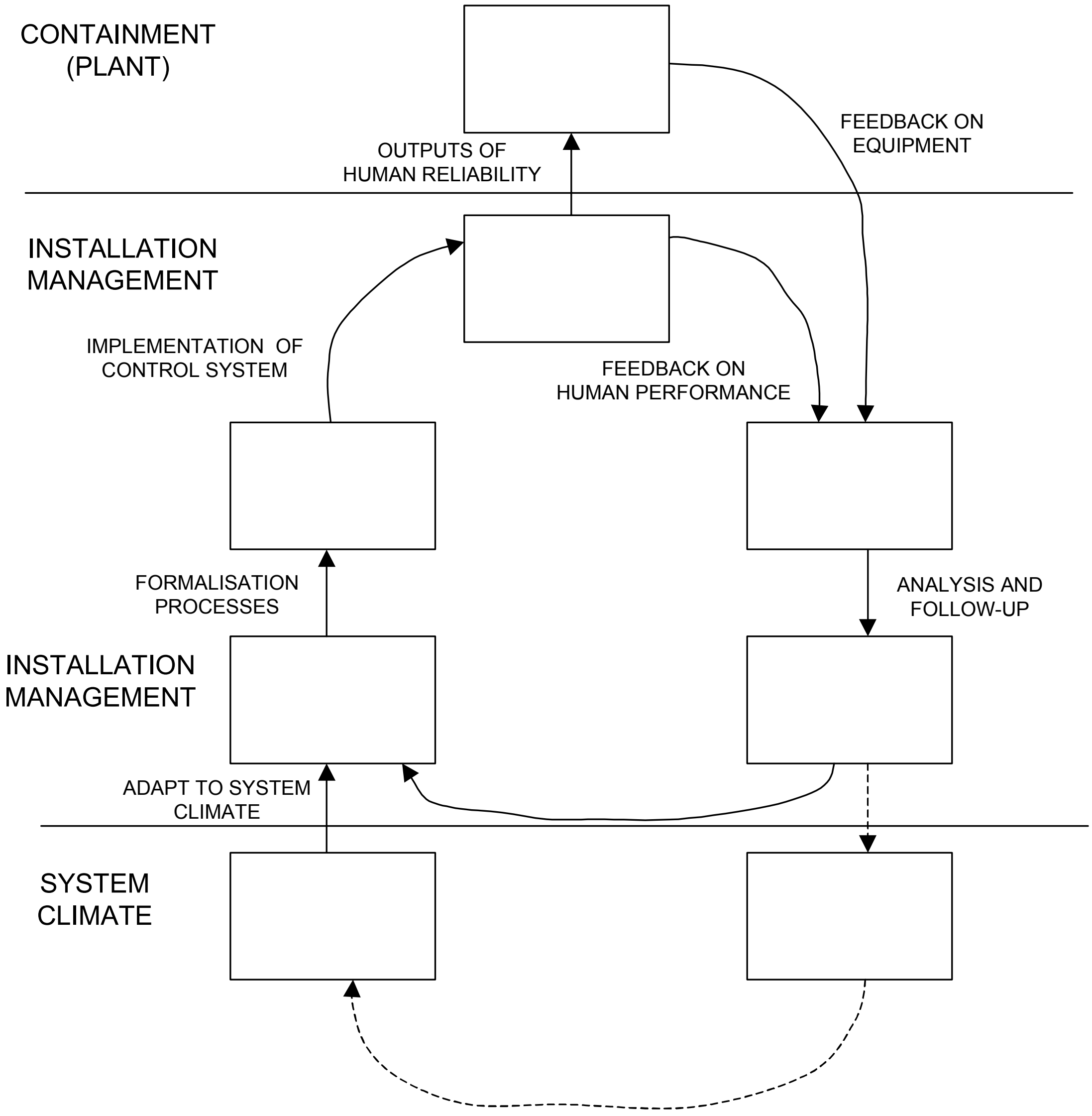


Table 4.2 Summary of Management Areas Considered within AVRIM2

	HAZARD REVIEW	CHECKING AND SUPERVISION	ROUTINE INSPECTION AND TESTING	HUMAN FACTORS REVIEW
DESIGN	Design and mods standards, codes, hazard analysis / safety studies and follow-up.			
CONSTRUCTION		Checking and supervision that construction of LODs is to spec.		
MAINTENANCE	Evaluation of maintenance errors in the hazard analysis / safety study.	The supervision of maintenance tasks and checking of completed activities to ensure safe / correct for relevant LOD related tasks.	Routine testing and inspection of LOD equipment to determine if OK, and maintenance follow-up as required.	Identification that possibilities for maintenance error are minimised in maintaining LODs though appropriate ergonomics, task design and training.
OPERATION	Evaluation of operational errors in the hazard analysis / safety study.	Supervision and checking of operational tasks for relevant LODs.		Identification that possibilities for operational error are minimised in maintaining LODs though appropriate ergonomics, task design and training.

4.5.1 Technical – Management Links

A recent development within AVRIM2 [16] has been the introduction of explicit links between the LODs associated with the Generic Fault Tree base events and the safety management system. The link is via management themes. Each of the four control and monitoring loops has associated with it a number of key management themes, which relate to the design, construction, maintenance or operation of the LOD. For example, the base event 'Not Replaced with Like' is linked to the Maintenance life cycle and the following management themes:

- Standards for maintenance;
- Inspection and testing;
- Control of conflicts between safety and production;
- Human factors in error management of maintenance, inspection and testing; and
- Supervision and checking of maintenance, inspection and testing tasks.

5. PLANOP

PLANOP (Protection Layer Analysis and Optimisation) [18] is a tool developed by the Chemical Risks Directorate of the Belgian Ministry of Labour for the qualitative analysis of the protective layers at a process plant. The tool is recommended for progressive implementation throughout the design process, although it may also be used to study existing installations. It is essentially a tool for collection, organisation and analysis of information concerning process risks, in order to support decisions on the implementation of safety measures.

5.1 THE PLANOP RISK MODEL

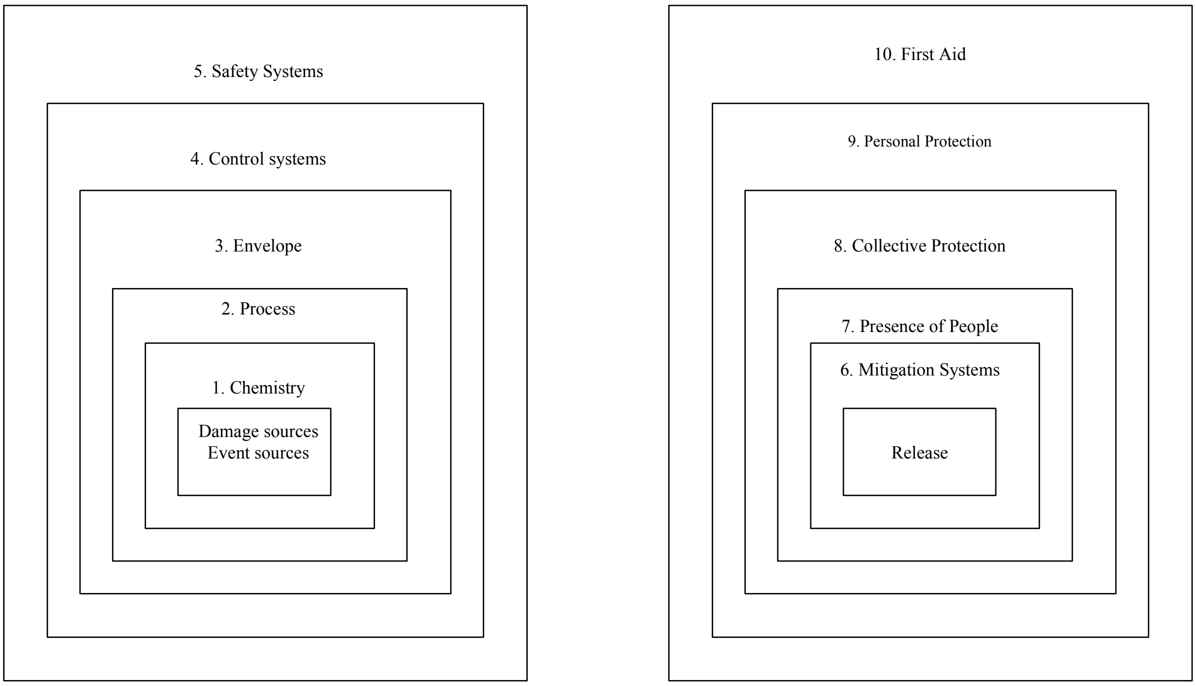
The PLANOP methodology distinguishes between 'damage sources' and 'event sources'. 'Damage sources' are the fundamental reason for the presence of a hazard and fall into two categories: hazardous materials and reactions.

'Event sources' are types of causes of loss of containment. Four general LOC types are defined:

- Failure of the containment envelope due to excessive forces;
- Failure of the containment envelope due to impairment;
- Accidental opening of the envelope due to human intervention; and
- Releases via process openings in the containment envelope.

PLANOP also uses a defined set of protection layers, as shown in Figure 5.1. These layers are divided into two groups: prevention (pre-release) layers and mitigation (post-release) layers. The layers are presented in order of their preference, thus encouraging the analyst to consider inherently safer approaches as a matter of priority. Emergency planning is considered outside the scope of PLANOP.

Figure 5.1 PLANOP Protection Layers



In conjunction with this, a set of risk reduction strategies is presented for each of the event and damage sources and for both preventive and mitigating types of layer. These strategies are shown in Table 5.1 for preventive layers and Table 5.2 for mitigation layers.

Table 5.1 Risk Reduction Strategies for Preventive Protection Layers

Risk reduction strategies towards damage sources (substances and reactions)	
Chemistry	Eliminate or replace hazardous substances. Use them in a different form. Find alternative, less hazardous reaction routes or reaction conditions.
Process	Reduce inventory by passive measures (e.g. – reduce storage capacity). Select a less hazardous reactor type (e.g. – plug flow vs batch reactor). Avoid undesired reactions by passive measures (e.g. – process layout).
Envelope	Not applicable.
Control Systems / Safety Systems	Reduce inventory by active measures (e.g. – stock control, high level interlock on tank).
Risk reduction strategies towards force producing phenomena (type 1 event sources)	
Chemistry	Avoid force producing phenomena or limit their force producing capacity by the selection of substances or reaction routes.
Process	Avoid force producing phenomena or limit their force producing capacity by passive measures (e.g. – limit the delivery pressure on a pump).
Envelope	Increase the resistance to the forces produced (e.g. – make a pressure vessel resistant to the highest pressure the phenomenon can generate).
Control Systems / Safety Systems	Prevent force producing phenomena or limit the forces produced by active measures (e.g. – control / safety systems on a batch reactor to prevent an exotherm).
Risk reduction strategies towards envelope impairing phenomena (type 2 event sources)	
Chemistry	Avoid envelope impairing phenomena or limit their envelope impairing capacity by the selection of substances or reaction routes.
Process	Avoid envelope impairing phenomena or limit their envelope impairing capacity by passive measures (e.g. – limit flowrate to reduce erosion).
Envelope	Increase the resistance to the impairing effect (e.g. – material selection).
Control Systems / Safety Systems	Prevent envelope impairing phenomena or limit their impairing capacity by active measures (e.g. – control concentration to avoid corrosion).
Risk reduction strategies towards human interventions (type 3 event sources)	
Chemistry	Not applicable.
Process	Avoid human interventions involving the opening of the containment envelope.
Envelope	Provide resistance to inadvertent opening, (e.g. – avoid valves that can be opened by accidental contact).
Control Systems / Safety Systems	Prevent the opening of the installation before hazardous materials are removed.
Risk reduction strategies towards process openings (type 4 event sources)	
Chemistry	Not applicable.
Process	Avoid process openings to atmosphere or limit the size of the opening.
Envelope	Not applicable.
Control Systems / Safety Systems	Take active measures to avoid breakthrough of hazardous substances (e.g. – control and safety systems on absorbent circulation in a scrubber).

Table 5.2 Risk Reduction Strategies for Mitigating Protective Layers

Mitigation Systems	Limit the released quantities (e.g. – shut-off valves), prevent the spreading of the released quantities (e.g. – bunds), prevent ignition of flammable materials, fight fire.
Presence of People	Avoid or limit presence of people, keep people at a safe distance.
Collective Protection	Protect people by collective measures (e.g. – reinforced buildings, safe havens)
Personal Protection	Use of personal protective equipment.
First Aid	Provide means for giving first aid (e.g. – safety showers).

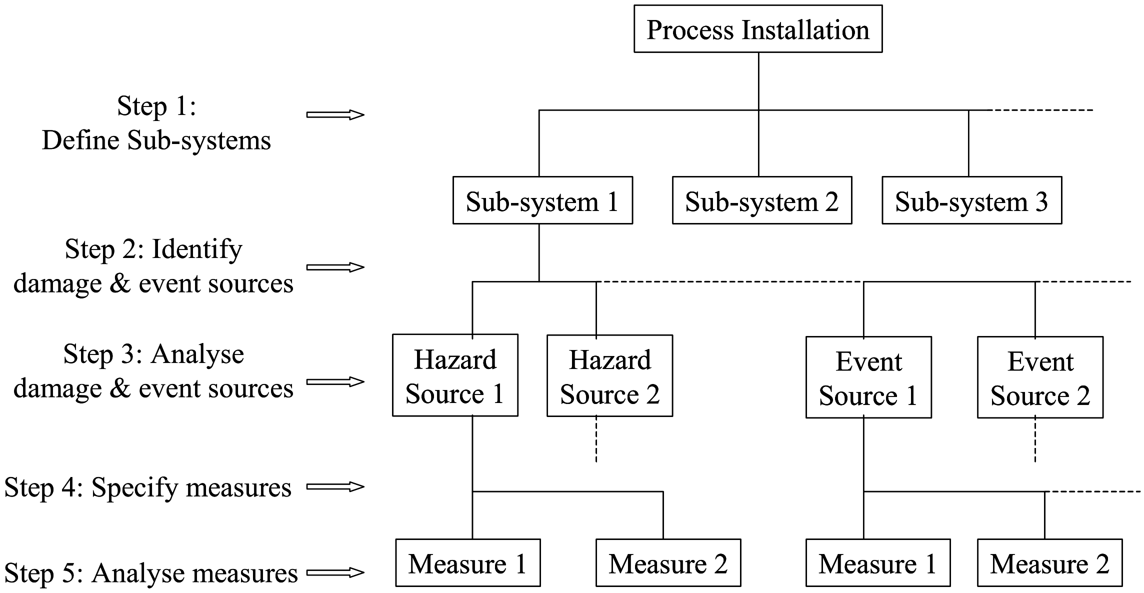
5.2 IMPLEMENTATION OF PLANOP

Implementation of PLANOP involves populating the data structure shown in Figure 5.2. This process involves five steps:

1. Definition of sub-systems.
2. Identification of damage and event sources.
3. Analysis of damage and event sources.
4. Specification of risk reduction measures.
5. Analysis of risk reduction measures.

Each of these steps is described in subsequent sections.

Figure 5.2 PLANOP Data Structure



5.2.1 Step 1: Definition of Sub-Systems

The extent to which the plant is broken down into sub-systems at this stage will determine the level of detail achieved in subsequent steps. The authors recommend that each equipment item (vessel, heat exchanger, column etc.) is treated as a sub-system, but ensuring that the complete plant is addressed.

5.2.2 Step 2: Identification of Damage and Event Sources

In the case of damage sources, identification is assisted by a Substance Identification Question List, whilst identification of reactions is assisted by generation of an Interaction Matrix, which includes all of the substances present within the sub-system. A distinction is made between substances and reactions present under normal conditions and those present under abnormal conditions.

Identification of event sources is facilitated by an extensive checklist.

5.2.3 Step 3: Analysis of Damage and Event Sources

Analysis of event sources is performed through the completion of template data sheets, which provide a checklist for substance or reaction properties and a means of recording those properties.

Essentially analysis of event sources involves identifying event causes and the possible consequences of the resulting loss of containment. This is achieved by the completion of simple ‘cause trees’ and ‘consequence trees’. These trees are less complex than fault or event trees. Typical cause trees are provided within the PLANOP tool.

5.2.4 Step 4: Specification of Risk Reduction Measures

This step involves identification of risk reduction measures for each of the damage and event sources identified. The analyst is assisted in this by the risk reduction strategies presented above, and by a ‘Measure Suggestion List’ that is given for each of the event sources in the Event Source Checklist. The Measure Suggestion List contains a list of possible measures classified according to the type of protection layer as illustrated in Figure 5.1.

5.2.5 Step 5: Analysis of Risk Reduction Measures

The purpose of this step is to identify means by which the reliability and / or effectiveness of the measures proposed can be jeopardised. This analysis can result in a more detailed specification of the risk reduction measure in order to prevent failure or impairment of effectiveness. This is supported within the tool by question list for different component types (relief valves, measuring devices, etc.).

6. THE SHORT-CUT RISK ASSESSMENT METHOD (SCRAM)

The Short-Cut Risk Assessment Method (SCRAM) [19] has been proposed as a means of prioritising accident scenarios for more detailed analysis (using QRA, for example).

SCRAM may be applied following a HAZOP or other hazard identification exercise. Accident scenarios are characterised according to a model of accident progression developed by Wells et al [20] and illustrated in Figure 6.1 and Table 6.1.

Figure 6.1 Development of a Process Incident [19]

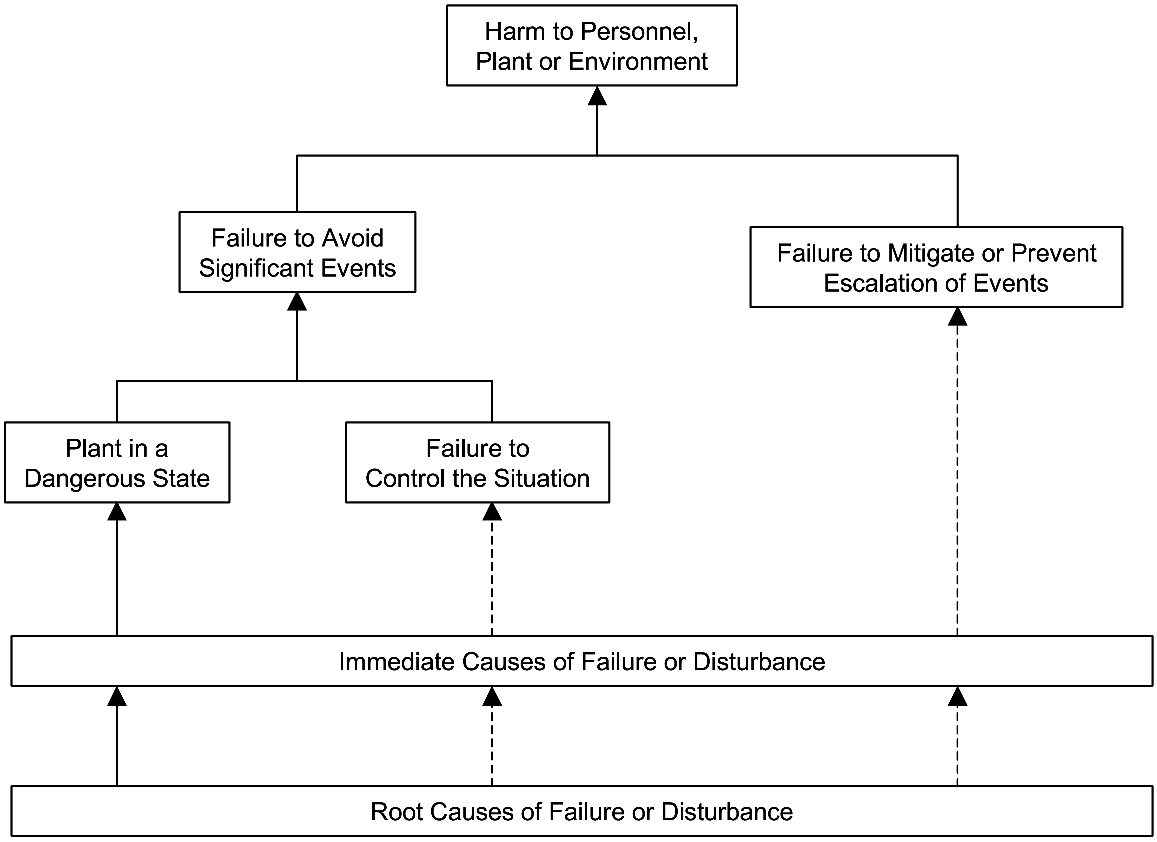

Harm to Personnel, Plant or Environment
Failure to Avoid Significant Events
Failure to Mitigate or Prevent Escalation of Events
Plant in a Dangerous State
Failure to Control the Situation
Immediate Causes of Failure or Disturbance
Root Causes of Failure or Disturbance

Table 6.1 General Process Incident Scenario [19]

DAMAGE AND HARM Consequences from appreciable to catastrophic Minor consequences or near miss	
FURTHER ESCALATION Post-incident damage Further dispersion on ground Further dispersion in air Damage by chemicals Damage by missiles or impact Damage by fire or explosions	FAILURE TO PREVENT FURTHER ESCALATION Inadequate post-incident response Failure of public response Failure of off-site emergency response Failure of on-site emergency response
ESCALATION OF EVENTS Damage and harm on escalation Escalation by fire or explosion Ignition of flammable mixture Dispersion of chemicals	FAILURE TO MITIGATE OR PREVENT ESCALATION Failure of emergency response to prevent escalation Failure of emergency response to mitigate effects
SIGNIFICANT RELEASE OF MATERIAL Release of material causes damage / harm Release creates hazard or hazardous condition	FAILURE TO RECOVER SITUATION AFTER RELEASE Release fails to disperse safely Accumulation after release Release fails to attenuate Immediate emergency response inadequate Inadequate protection / passive protection
RELEASE OF MATERIAL Rupture of plant with release Discharge of process material	FAILURE TO RECOVER SITUATION BEFORE RELEASE Operator action fails Control systems fail to recover situation
DANGEROUS DISTURBANCE OF PLANT Disturbance ultimately exceeding critical defect or deterioration in construction Flow through abnormal opening to atmosphere Change in planned discharge or vent	INADEQUATE EMERGENCY CONTROL OR ACTION Emergency control system fails to correct
HAZARDOUS DISTURBANCE OF PLANT Hazardous trend in operation conditions Construction defective or deteriorated in service Abnormal opening in equipment Change in planned discharge or vent	INADEQUATE EMERGENCY CONTROL OR ACTION Normal control systems fail to correct the situation Operators fail to correct the situation Maintenance fails to correct the situation
IMMEDIATE CAUSES OF FAILURE OR DISTURBANCE Action by plant personnel inadequate Defects directly cause loss of plant integrity Plant or equipment inadequate or inoperable Control system or emergency control inadequate Change from design intent Environmental and external causes of disturbance	ROOT CAUSES OF FAILURE DISTURBANCE Site and plant facilities Operator performance Information systems and procedures Management performance Resource provision Organisation and management systems System climate External systems

For each scenario, the analysis is completed using a Risk Evaluation Sheet, an example of which is shown in Table 6.2 (from reference [19]).

Table 6.2 Example Risk Evaluation Sheet

Risk Evaluation Sheet		Date: 01-01-93 Page: 1 of 4		
Project: TOMHID Plant: Hydrogen Unit: Methanator Section	Reference: GLW Location: Sheffield Equipment: Preheat	**PRIORITY FOR QRA**		
Fixed bed reactor converting oxides of carbon & water to H_2 & CH_4		S	L	P
CONSEQUENCES OF ESCALATION	Fire escalate to pipe rack and C plant	4	-6	C
FAILURE TO PREVENT FURTHER ESCALATION	Failure to avoid domino due to lack of time and ineffective fire-fighting		P=0.01	
CONSEQUENCES OF SIGNIFICANT EVENT	Torch fire on section of plant	3	-4	B
FAILURE TO MITIGATE OR AVOID ESCALATION	Failure to avoid ignition: self ignites as release is hot AND release not attenuated in 15 minutes	3	P=1	
SIGNIFICANT EVENT	Release through overtemperature	F=E-4		
FAILURE TO RECOVER THE SITUATION	Operator fails to stop all plant flows (1)	P=0.1		
DANGEROUS DISTURBANCE	Overtemperature in reactor	F=E-3		

INADEQUATE EMERGENCY CONTROL	Failure of operator to stop flow
	Failure of shutdown system
		P=0.1
		P=0.05		

HAZARDOUS DISTURBANCE	High temperature in the reactor	F=0.1		
INADEQUATE CONTROL	Operator fails to reduce trend on CO_2 alarm or TAH or PAH	P=0.1		

IMMEDIATE CAUSES	High CO_2 in stream from absorber
	Impurities: sneak path on start-up line
		F=1
		F=E-2		

RECOMMENDATIONS, COMMENTS, OR ACTIONS F for Frequency P for Probability S = Severity L = Likelihood P = Priority E-2 signifies 10^{-2}	(1) The operator can increase the probability of a release by incorrect action and special supervision is required on any Methanator problem 1. Do not depressurise on high temperature unless sure of no flow 2. Operator needs to be alerted by several alarms 3. Check if start-up line needed if heat exchange circuit modified 4. Improve adsorber design to enhance reliability 5. Public not affected by domino escalation 6. Business damage would be extensive if spread too complex			

An accident is considered to progress from its immediate causes to one of several outcomes, depending on whether or not mitigation is possible or whether escalation occurs. The consequences of the outcomes are assigned to a severity category (S). The severity categories and corresponding acceptable frequencies provided by the authors are displayed in Table 6.3.

Frequencies of outcomes are developed by assigning a frequency to the immediate cause(s), then applying probabilities of failure for each of the opportunities to control or prevent the accident from developing. The various failures to prevent or control may be thought of as failures of LOPs / LODs. Frequencies are estimated to the nearest order of magnitude. The Likelihood (L) is then the logarithm of the frequency.

Table 6.3 SCRAM Example Severity Categories

Severity	Title	Description	Acceptable Frequency (yr^{-1})
5	Catastrophic	Catastrophic damage and severe clean-up costs On-site: Loss of normal occupancy > 3 months Off-site: Loss of normal occupancy > 1 month Severe national pressure to shut down Three or more fatalities of plant personnel Fatality of member of public or at least five injuries Damage to SSSI or historic building Severe permanent or long-term environmental damage in a significant area of land	10^{-5}
4	Severe	Severe damage and major clean-up Major effect on business with loss of occupancy up to 3 months Possible damage to public property Single fatality or injuries to more than five personnel A 1 in 10 chance of a public fatality Short-term environmental damage over a significant area of land Severe media reaction	10^{-4}
3	Major	Major damage and minor clean-up Minor effect on business but no loss of building occupancy Injuries to a maximum of five plant personnel with a 1 in 10 chance of fatality Some hospitalisation of public Short-term environmental damage to water, land, flora or fauna Considerable media reaction	10^{-3}
2	Appreciable	Appreciable damage to plant No effect on business Reportable near miss incident under CIMAH (sic) Injury to plant personnel Minor annoyance to public	10^{-2}
1	Minor	Near-miss incident with significant quantity released Minor damage to plant No effect on business Possible injury to plant personnel No effect on public, possible smell	10^{-1}

A risk parameter is determined from:

Risk = L + S

The example severity categories in Table 6.3 are constructed to give a target risk parameter of zero. Prioritisation of accident outcomes is performed according to severity and risk, as shown in Table 6.4.

Table 6.4 SCRAM Prioritisation Table

Severity Category	**Value of Risk**			
	-2	**-1**	**0**	**1**
1	None	None	None	C
2	None	None	C	B
3	None	C	B	A/B
4	C	B/C	B	A
5	B	B/C	A	A

Key:
A – Immediate attention needed
B – Further study probably required
C – Further study may be necessary

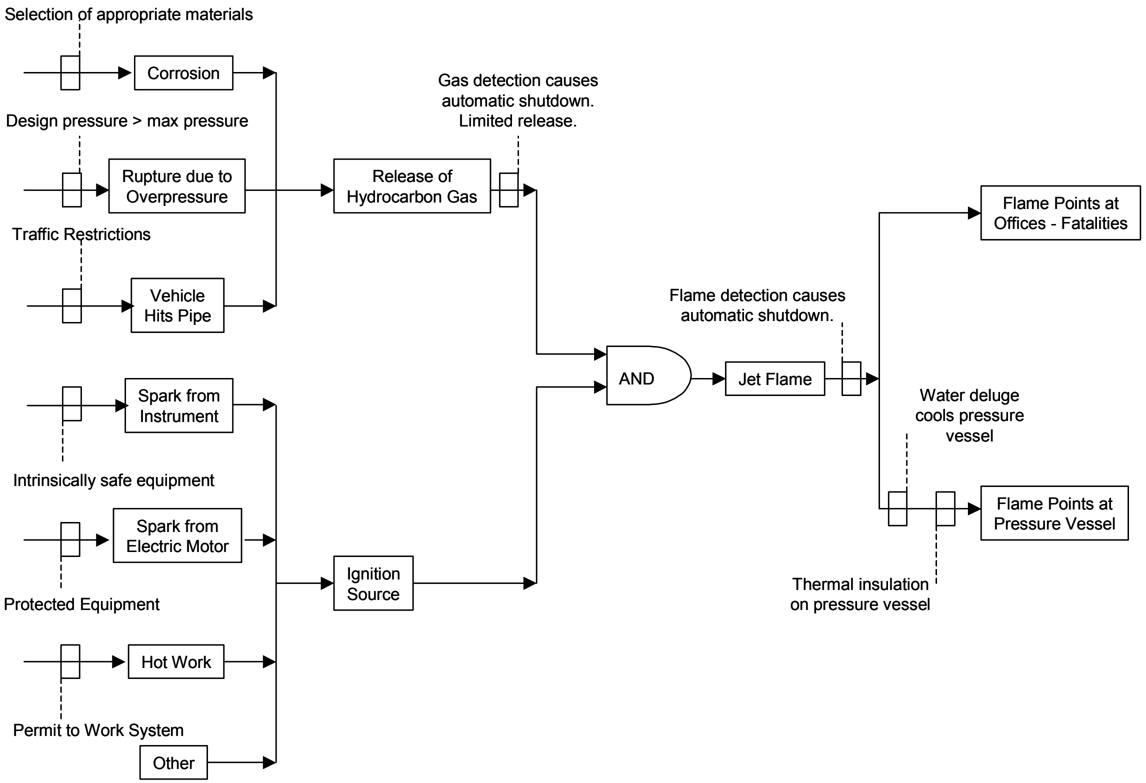
7. SAFETY BARRIER DIAGRAMS

A basic barrier diagram is shown in Figure 7.1. Typically the diagram is constructed on the basis of knowledge of the system failure logic obtained during a HAZOP or other hazard identification study. Safety barriers (LOPs or LODs) are shown as rectangles on the lines between causes and consequences. In overall form the diagram is similar to the bow-tie diagram illustrated in Figure 1.2. The barriers on the left hand side of the diagram are preventive; those on the right hand side provide mitigation.

Barriers may be full or partial. A full barrier completely prevents a cause from developing into a consequence, unless it fails to operate. A partial barrier may not fully prevent a cause from generating a consequence, even if it operates as it should, an example being an alarm. Different symbols are used to indicate full and partial barriers, as shown in Figure 7.2.

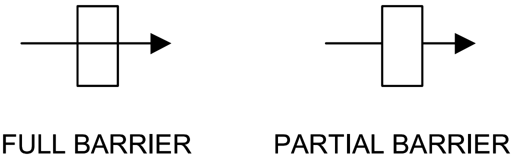
In addition barriers may be classed as passive (such as a bund or fire wall), active (such as a trip system) or circumstantial (such as wind direction).

Figure 7.1 Basic Safety Barrier Diagram



Selection of appropriate materials
Corrosion
Design pressure > max pressure
Rupture due to Overpressure
Traffic Restrictions
Vehicle Hits Pipe
Gas detection causes automatic shutdown. Limited release.
Release of Hydrocarbon Gas
Spark from Instrument
Intrinsically safe equipment
Spark from Electric Motor
Protected Equipment
Ignition Source
Hot Work
Permit to Work System
Other
AND
Flame detection causes automatic shutdown.
Jet Flame
Flame Points at Offices - Fatalities
Water deluge cools pressure vessel
Flame Points at Pressure Vessel
Thermal insulation on pressure vessel

Figure 7.2 Barrier Types



Having constructed the diagram, the initiating events on the far left hand side of the diagram are assigned to a frequency category (F) and the consequences on the far right of the diagram are assigned to a consequence category (C). The frequency and consequence categories used are shown in Table 7.1 and Table 7.2 respectively.

Table 7.1 Barrier Diagram Frequency Categories

Category F	**Description**
6	**Frequent Event** Twice or more a week
5	**Normal Event** A few times per year
4	**Unusual Event** Less than once a year
3	**Rare Event** Less than once in 100 years
2	**Very Rare Event** Less than once in 10000 years
1	**Extremely Rare Event** Less than once in a million years
X	**Frequency Cannot be Estimated** e.g. – Sabotage, terrorism

Table 7.2 Barrier Diagram Consequence Categories

Category C	**Description**
0	**No Consequences** No danger or disturbance
1	**Insignificant Consequences** Minor disturbance
2	**Noticeable Consequences** Production disturbed
3	**Significant Consequences** Injuries on site, damage to equipment
4	**Serious Consequences** Fatalities on site
5	**Major Accident** Fatalities on and off site

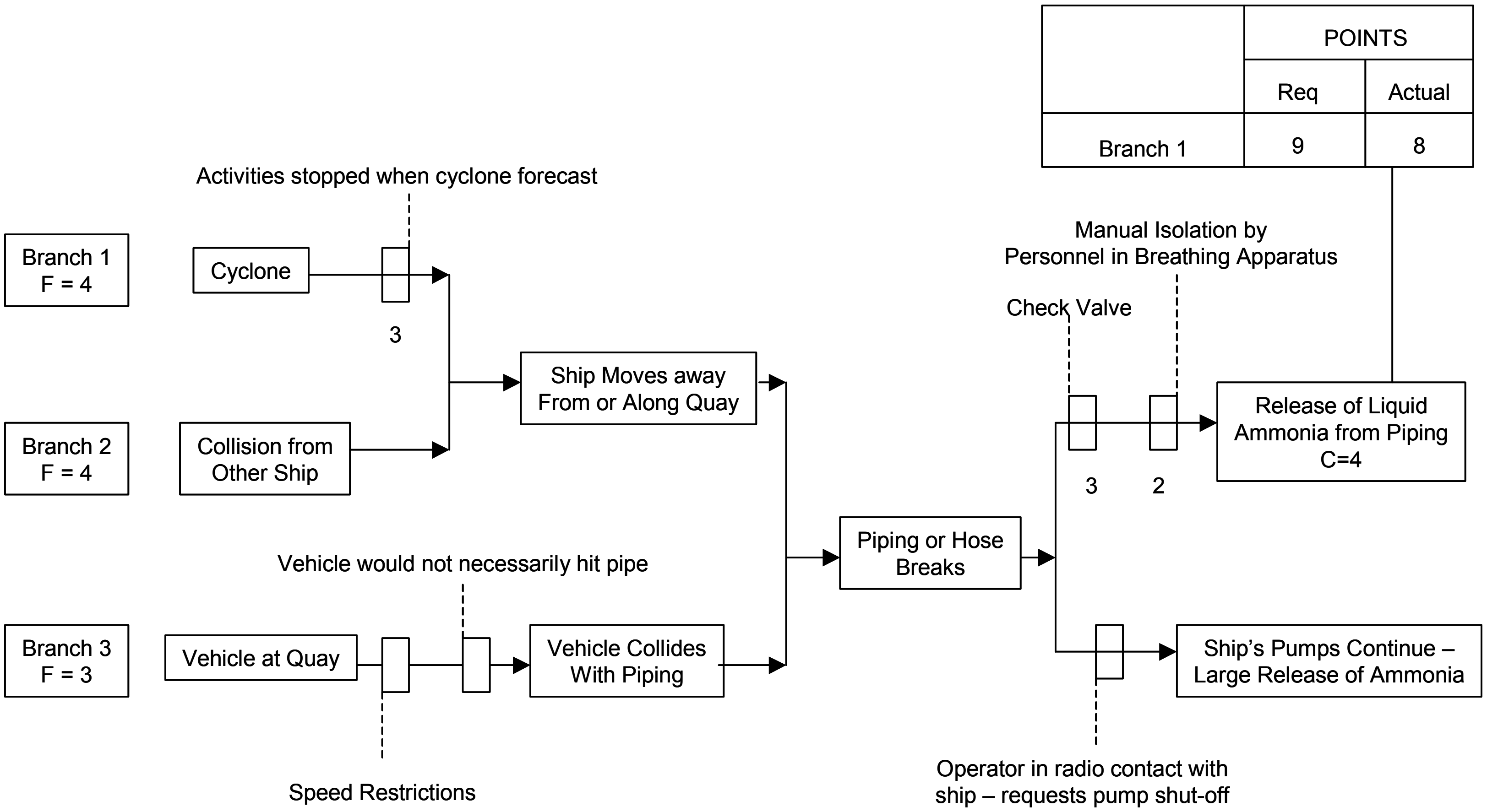
Each barrier on the diagram is then assigned an appropriate number of ‘Barrier Points’. The concept is similar to that of the IPL credit in LOPA or the LOD rating in TRAM. In Barrier Diagrams, 1 Barrier Point corresponds to a PFD of $10^{-½}$. Typical Barrier Point values are displayed in Table 7.3.

Table 7.3 Typical Barrier Point Values

Barrier	Application / Comments	Points
Fire wall	Prevents the spread of fire to other areas for at least 60 minutes	10
Bunded enclosure	Pond can hold the largest volume that could be released	8
Water reservoir	Enough water to meet fire fighting needs in the event of the largest release	6
Rupture disc	Releases pressure to atmosphere	6
Safety relief valve	Releases pressure to atmosphere	6
Alarm with trip	Trip initiates effective safety measure	6
Emergency Shutdown (ESD) valve	Closes automatically, part of a failsafe installation	4
Alarm with manual intervention	Alarm warns an operator in a permanently manned control room who then initiates effective safety measures	4
Regular inspection	100% inspection carried out by authorised person under strict quality control. Interval between inspection appropriate to the specific equipment	4
Non-return valve	Allows flow in one direction only in pipe	2

Each path (from initiating event on the left to consequence on the right) is then assessed separately, to determine whether sufficient barrier points are in place to prevent the initiating event giving rise to the consequence. The number of barrier points in place is obtained by summing the barrier points for each barrier along the path. This is compared with the required number of barrier points to determine whether further action is necessary. This process is illustrated in Figure 7.3. The number of barrier points required is a function of initiating event Frequency (F) and the Severity of the consequences (S), as shown in the risk matrix in Table 7.4. The author states that this matrix has been benchmarked against the F-N curve risk criteria used in the Netherlands.

Figure 7.3 Barrier Diagram – Use of Barrier Points



	POINTS	
	Req	Actual
Branch 1	9	8

Branch 1
F = 4
Branch 2
F = 4
Branch 3
F = 3
Cyclone
Activities stopped when cyclone forecast
3
Collision from Other Ship
Ship Moves away From or Along Quay
Vehicle at Quay
Vehicle would not necessarily hit pipe
Speed Restrictions
Vehicle Collides With Piping
Piping or Hose Breaks
Check Valve
Manual Isolation by Personnel in Breathing Apparatus
3
2
Release of Liquid Ammonia from Piping C=4
Ship's Pumps Continue – Large Release of Ammonia
Operator in radio contact with ship – requests pump shut-off

Table 7.4 Barrier Diagram Risk Matrix

Frequency	Category F	Number of Barrier Points Required				
Frequent Event - Twice a week or more	**6**	2	6	10	14	18
Normal Event – a few times a year	**5**		3	7	11	15
Unusual Event – less than once a year	**4**		1	5	9	13
Rare Event – less than once per 100 years	**3**			1	5	9
Very Rare Event – less than once per 10000 years	**2**				1	5
Extremely Rare Event – less than once per million years	**1**					1
	Category C	**1**	**2**	**3**	**4**	**5**
	Consequences	**Insignificant Consequences**	**Noticeable Consequences**	**Significant Consequences**	**Serious On-Site Consequences**	**Major Accident**

8. USEFULNESS IN THE COMAH CONTEXT

8.1 DEMONSTRATION OF ALARP

As mentioned in Section 1, one of the purposes of the Safety Report produced under COMAH is to provide a demonstration that the measures for prevention and mitigation employed by the establishment result in a level of risk that is as low as reasonably practicable (ALARP).

The ALARP principle forms part of an overall tolerability of risk framework described by HSE [14]. The HSE framework is commonly represented by a triangle, as shown in Figure 8.1. The risk increases from the bottom point of the triangle to the top. The framework suggests that there is an upper limit to individual risk, above which the risk is regarded as unacceptable whatever the benefits. An activity or practice falling into this region would normally be ruled out unless action could be taken to reduce the risk so that it fell into one of the regions lower down the triangle. This is represented by the dark region at the top of the triangle.

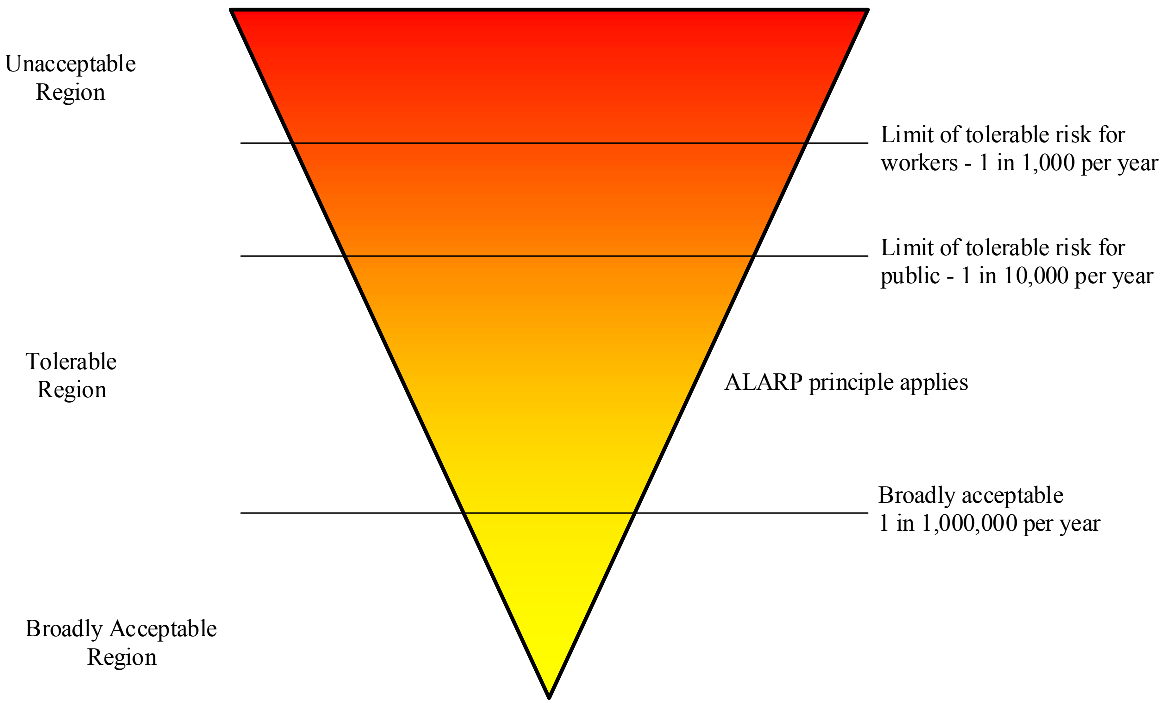
The light zone at the bottom of the triangle represents what is known as the 'broadly acceptable region'. Risks falling into this region are regarded as insignificant and adequately controlled. Further action to reduce risk would not normally be required, unless there were obvious, reasonably practicable measures available. The levels of risk within this region are comparable to those that people regard as trivial or insignificant in their daily lives.

The zone between the unacceptable and broadly acceptable regions (the middle part of the triangle) is known as the tolerable region. Within this region the risks must be controlled to a level that is as low as reasonably practicable (ALARP).

HSE have suggested that the boundaries between the different regions on the triangle are as follows:

- For workers, the boundary between the unacceptable and the tolerable region should be an individual risk of fatality of 1 in 1000 per year (1 x 10^{-3} yr^{-1}). This is based upon a consideration of the risks associated with the most hazardous work activities that society appears to tolerate.
- For members of the public, this boundary is set an order of magnitude lower at a level of individual risk of fatality of 1 in 10,000 per year (1 x 10^{-4} yr^{-1}).
- The boundary between the tolerable and the broadly acceptable regions is considered to be an individual risk of fatality of 1 in 1,000,000 per year (1 x 10^{-6} yr^{-1}). As indicated above, this represents a level of risk comparable to those that people regard as trivial or insignificant in their daily lives.

Figure 8.1 Risk Criteria Framework


Unacceptable Region
Limit of tolerable risk for workers - 1 in 1,000 per year
Limit of tolerable risk for public - 1 in 10,000 per year
Tolerable Region
ALARP principle applies
Broadly acceptable 1 in 1,000,000 per year
Broadly Acceptable Region

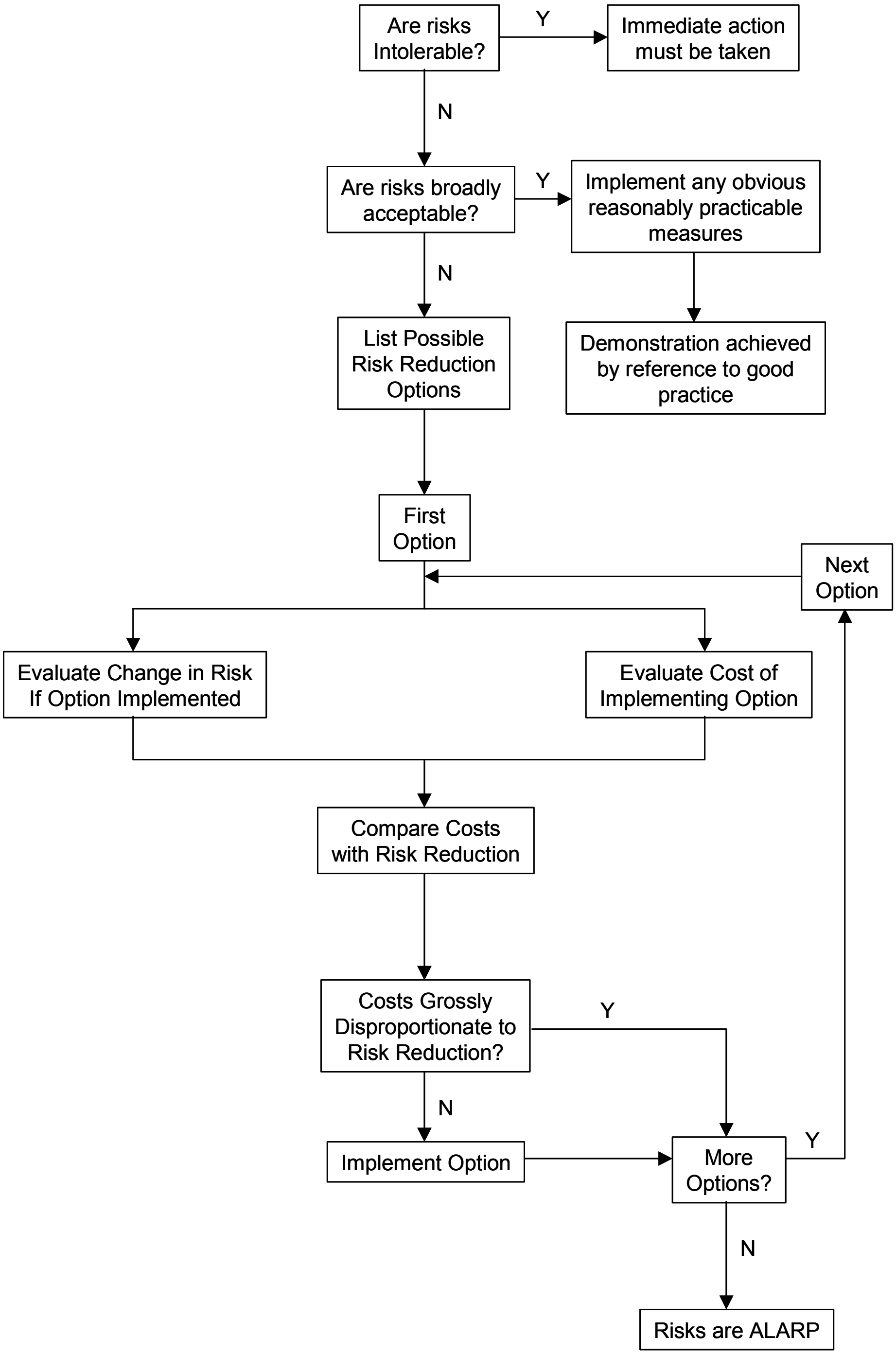
The ALARP principle requires that the cost of a measure be ‘grossly disproportionate’ to the benefits before the measure can be considered not reasonably practicable to implement. The principle is defined within relevant case law (Edwards vs the National Coal Board, [1949] 1 All ER 743):

“Reasonably Practicable” is a narrower term than “physically possible”, and implies that a computation must be made in which the quantum of risk is placed in one scale and the sacrifice involved in the measures necessary for averting the risk (whether in money, time or trouble) is placed on the other, and that, if it be shown that there is a gross disproportion between them – the risk being insignificant in relation to the sacrifice – the defendants discharge the onus upon them.”

(It should be noted that the CCPS LOPA publication [2] uses the term ALARP in a different, more general sense, to mean the risk level that is tolerable to an organisation).

The process of determining whether risks from an establishment are ALARP is outlined in Figure 8.2.

Figure 8.2 ALARP Determination Process


Are risks Intolerable?
Y
Immediate action must be taken
N
Are risks broadly acceptable?
Y
Implement any obvious reasonably practicable measures
N
Demonstration achieved by reference to good practice
List Possible Risk Reduction Options
First Option
Next Option
Evaluate Change in Risk If Option Implemented
Evaluate Cost of Implementing Option
Compare Costs with Risk Reduction
Costs Grossly Disproportionate to Risk Reduction?
Y
N
Implement Option
More Options?
Y
N
Risks are ALARP

Each of the methods described in the preceding sections has been considered for its usefulness in demonstrating that risks are ALARP in the context of a COMAH safety report. The results of these considerations are described below.

8.2 LAYER OF PROTECTION ANALYSIS (LOPA)

As a risk assessment technique, LOPA can be used to assist in the evaluation of the change in risk that would result from the implementation of a risk reduction option and so assist in the ALARP demonstration process outlined in Figure 8.2. However:

- The nature of the technique means that use of LOPA will not be appropriate in all circumstances.
- The way in which LOPA is implemented for COMAH purposes may differ from the way in which it is implemented for other purposes (such as IPF SIL level determination).

These factors are discussed in more detail below.

8.2.1 LOPA Applicability

The CCPS publication [2] observes that LOPA is one of a spectrum of risk assessment techniques, ranging from simple, qualitative, to detailed, fully quantitative methods. LOPA falls somewhere in the middle of this range, being termed a ‘simplified-quantitative’ method. In general, use of LOPA would not be appropriate when:

- A simpler, qualitative approach would suffice; or
- The scenario is too complex to be analysed using LOPA and more sophisticated quantitative methods must be employed.

In the context of COMAH, the published guidance [22] indicates that the depth and type of risk analysis will vary, but is likely to be proportionate to:

- The scale and nature of the major accident hazards presented by the establishment and the installations and activities on it;
- The risks posed by the establishment to neighbouring populations and the environment (i.e. – the extent of possible damage); and
- The complexity of the major accident hazard processes and activities, and the difficulty in deciding and justifying the adequacy of the risk control measures adopted.

Hence, for COMAH purposes, the risk assessment for a simple bulk chlorine water treatment facility well separated from any surrounding population or sensitive environmental receptors would be expected to use qualitative or semi-quantitative approaches. However, the risk assessment for a large, complex chemical manufacturing facility, handling a number of dangerous substances, located adjacent to a densely populated area and / or sensitive environmental receptors would be expected to contain a greater degree of quantification (although perhaps not full QRA).

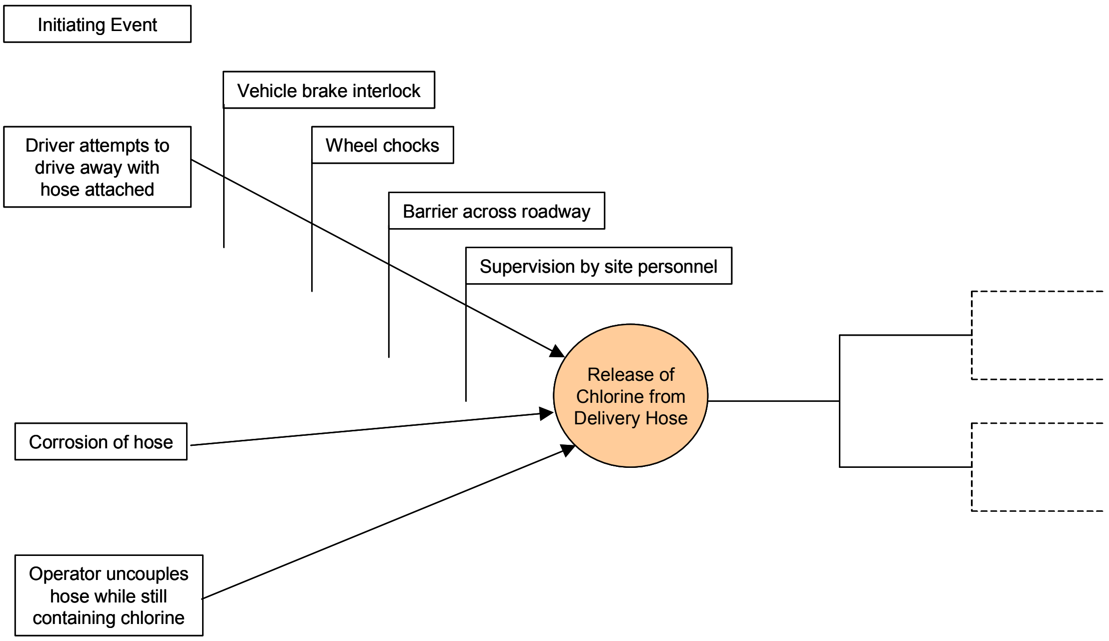
According to this principle of proportionality, the use of LOPA would be appropriate in circumstances where the use of a technique at the semi-quantified to quantified end of the spectrum was justified.

Additionally, in order for LOPA to be applied to a scenario, the scenario must possess certain features:

- There must be a well-defined initiating event that produces a demand on the protective layers;
- There must be well-defined independent protective layers (IPLs) fitting the LOPA requirements of effectiveness, independence and auditability.

Consider the example 'bow-tie' diagram shown in Figure 8.3, relating to a release of chlorine from a road tanker delivery hose. The diagram is provided for illustrative purposes only and is not intended to be comprehensive.

Figure 8.3 Example Bow-Tie Diagram


Initiating Event
Vehicle brake interlock
Driver attempts to drive away with hose attached
Wheel chocks
Barrier across roadway
Supervision by site personnel
Release of Chlorine from Delivery Hose
Corrosion of hose
Operator uncouples hose while still containing chlorine

The diagram shows an event, 'Release of Chlorine from Delivery Hose' and, on the left hand side, three potential initiating events. The scenario involving the top-most initiating event would be amenable to analysis by LOPA. The initiating event is well defined; and it is possible to identify a series of IPLs that could meet the LOPA methodology criteria.

The scenario involving the initiating event, 'Corrosion of hose', could not be analysed readily using the LOPA technique. The initiating event is not well defined since corrosion occurs over an extended period of time. Although a number of measures to prevent such an event could be identified (regular inspection, storage of the hose in an appropriate location between deliveries, appropriate materials of construction), the failure of these measures would constitute underlying causes of corrosion rather than IPLs.

The scenario involving 'Operator uncouples hose while still containing chlorine' as an initiating event may not be appropriate for analysis using LOPA. Although the initiating event is well defined, IPLs are harder to identify. Safeguards would include operator training, competence and hazard awareness. However, as with the previous scenario, failures of these safeguards represent underlying causes of the initiating event. It is suggested that scenarios displaying a strong dependence on operator action would be better addressed using human error analysis techniques.

8.2.2 Use of LOPA for COMAH

With reference to Figure 8.2, it can be seen that a demonstration that risks are ALARP comprises two main elements:

- An estimate of the overall level of risk from the establishment; and
- An assessment of whether or not further risk reduction measures are justified.

Use of LOPA may contribute to both of these elements. LOPA, perhaps in conjunction with other techniques, could be used to synthesise an estimate of the overall risk from an establishment from an analysis of the scenarios contributing to that risk.

Where appropriate, LOPA may also be used to analyse particular scenarios of interest, to determine the change in risk upon implementation of proposed risk reduction measures. In conjunction with a cost-benefit analysis, the LOPA results could be used to demonstrate ALARP.

Clearly, when used in this context, the LOPA study will need to be configured to generate outputs that are measures of individual or societal risk (or both). This process of risk estimation is outlined in Section 2.3.

In some applications, decisions of risk acceptability using LOPA are based, not on a risk estimate that is linked to the overall risk from the establishment, but on either:

- A risk criterion at the 'per scenario' level; or
- A required number of IPLs for a scenario with a given consequence level.

The use of these approaches may be problematic in the context of COMAH. Principally this is because showing that the frequency or risk associated with a given scenario is at or below a target level would not in itself constitute a demonstration of ALARP. It would still be necessary to show that the cost of implementing any further measures would be grossly disproportionate to the risk reduction achieved.

Other difficulties may arise if the 'risk per scenario' criterion is set in a generic fashion, that is, without reference to the site-specific risk profile (note that this is the approach taken in determining the TRAM consequence categories, see Section 6.3 below). This is because the criterion requires an assumption concerning the number of such scenarios that contribute to the overall risk, which may or may not be correct in a particular case. This may lead to a situation where, although the risk from each scenario is judged to be acceptable on a 'risk per scenario' basis, the summation of the contributions from all scenarios leads to a risk that is intolerable.

However, it may be possible to utilise a 'risk per scenario' criterion that has been developed on a site-specific basis. This would require an estimate of the overall risk from the establishment, together with knowledge of the number of scenarios contributing to the overall risk.

Similarly, use of a criterion expressed in terms of a required number of IPLs may also be inappropriate for COMAH purposes, in some circumstances. In effect, specifying a number of IPLs required for a given consequence level for a scenario equates to specifying a 'per scenario' risk criterion, except that now assumptions are made concerning not only the number of scenarios contributing to the overall risk, but also concerning the value of each IPL. However, this approach simplifies the LOPA process considerably. Hence LOPA, used in this way, may be appropriate when a more qualitative risk assessment approach is justified.

It should be noted that a distinction is made between the use of LOPA when implementing a standard such as IEC61508 and the use of LOPA when seeking to demonstrate ALARP in the context of COMAH. In the former situation, use of LOPA in conjunction with 'risk per scenario' or 'required numbers of IPLs for a scenario' criteria might be entirely appropriate and represent implementation of good practice. The objective of the assessment is to establish the requirement for an IPF and the appropriate SIL, for a specific item of Equipment Under Control.

However, in the context of COMAH, the operator is required to provide a demonstration of ALARP for an establishment as a whole, not just a specific EUC item. HSE documents on ALARP decisions [23] state that, where the risk from the establishment is broadly acceptable, then demonstration may be achieved by adherence to codes, standards and relevant good practice. However, where the risk from the establishment is in the 'Tolerable' region, then a case-specific ALARP demonstration is required, in which the operator should consider what more could be done to reduce the risk and whether any further measures would be reasonably practicable to implement. It is in this context that use of LOPA in conjunction with 'risk per scenario' or 'required numbers of IPLs for a scenario' criteria might be inappropriate.

8.3 TRAM

Unlike LOPA, TRAM was not developed to be a risk assessment method, but a site audit and inspection tool. The underlying methodology is essentially the same as LOPA, except that Layers of Defence in TRAM are more broadly defined than IPLs in LOPA and could include what might be determined mitigating circumstances (such as weather conditions).

One difficulty in utilising TRAM for risk assessment purposes is the amalgamation of the risk criteria with the consequence categories. Whilst this is a convenient simplifying assumption that enables the tool to operate for screening, auditing and inspection purposes, it creates difficulties when applied to risk assessment. As with the 'risk per scenario' criterion for LOPA, this simplification has required assumptions concerning the number of scenarios contributing to the overall risk from the establishment and is therefore problematic for the same reasons.

8.4 AVRIM2

Like TRAM, AVRIM2 was not developed as a risk assessment methodology, but as a tool to assist inspectors in their assessment of safety reports submitted by operators.

One of the principal features of AVRIM2 is the explicit link that has been constructed between Lines of Defence and aspects of the safety management system. This stems from a recognition that poor safety management is a potential 'common cause' failure mode which could result in a number of LODs being undermined.

In comparison, at present LOPA does not specifically address safety management issues, but could be regarded as complementary to other methods such as safety auditing and inspection. The findings of a LOPA study could be used to highlight the importance of installing, maintaining, testing and inspecting the specified layers of protection appropriately. An audit programme could then be used to verify that these activities were being performed correctly.

The creation of links to the safety management system in addition to the normal LOPA outputs might be a particularly useful development in the context of COMAH. Although this study has focussed on the risk assessment requirements of COMAH, the Regulations also place a strong emphasis on safety management systems.

8.5 PLANOP

PLANOP is a qualitative tool for the specification and / or analysis of protective layers. The method may be useful in the COMAH context, for establishments where the use of more sophisticated techniques was not justified. However, at present the description of PLANOP available in the published literature is not sufficiently comprehensive to allow a detailed evaluation.

8.6 SCRAM

SCRAM has been designed as a screening tool for prioritising accident scenarios for further analysis. Further development would be required in order to make SCRAM a risk assessment technique in its own right. At present the method only considers LOPs / LODs in very broad terms, as failures at different points during the progression of an accident.

8.7 BARRIER DIAGRAMS

The Safety Barrier Diagram method considers LOPs / LODs explicitly, as do LOPA and TRAM. The graphical presentation of initiating events, barriers and consequences is useful in allowing the analyst to understand the failure logic of a system.

From the information available, it appears that (as with LODs in TRAM) barriers are more broadly defined than IPLs in LOPA. For example ‘circumstantial barriers’ may include mitigating circumstances such as wind direction.

A barrier diagram may not be appropriate where the failure logic is complex or where there is a need to address the possibility of common mode failure, when use of a more sophisticated technique such as fault tree analysis might be appropriate.

The criteria presented for determining the number of barrier points required are similar in principle to the use of LOPA, where the required number of IPLs is specified for a given consequence level. As indicated in Section 8.2.2 above, this equates to a ‘per scenario’ risk criterion and is therefore subject to the limitations described previously.

As it is currently presented, the barrier diagram method avoids calculating risk explicitly. It would therefore be difficult to use the method in a semi-quantitative ALARP demonstration, since the benefit of introducing further risk reduction measures could not be evaluated readily, other than as an increased barrier point score. This difficulty could be overcome by amending the method to use PFDs on the diagram instead of barrier points. The frequency of a given consequence could then be obtained by multiplying the initiating event frequency by each of the barrier PFDs along the appropriate path through the diagram.

9. CONCLUSIONS

Summary descriptions of several methods (LOPA, TRAM, AVRIM2, PLANOP, SCRAM and Safety Barrier Diagrams) have been prepared. The usefulness of the methods in the context of demonstrating ALARP in COMAH safety reports has been evaluated. Of the techniques considered, it is concluded that LOPA (Layer of Protection Analysis) is potentially a useful tool in performing semi-quantitative risk assessments for COMAH purposes.

TRAM and AVRIM2 were designed as safety report assessment or site audit tools and, in their current form, are not suitable for use as risk assessment tools. However, AVRIM2 in particular contains much information (in the form of checklists, matrices and generic fault trees) that might be useful in constructing a qualitative demonstration of ALARP.

The PLANOP approach may be useful in circumstances where a purely qualitative approach is justified, although at present there is insufficient information available on the method to perform a detailed evaluation.

SCRAM has been designed as a tool for prioritising accident scenarios for more detailed assessment and, at its present stage of development, is not suitable for use as a risk assessment method.

Safety Barrier Diagrams provide a useful, graphical representation of system failure logic and the role of the various layers of protection (barriers) in place. However, as it is currently formulated, the method avoids any explicit calculation of risk. Therefore, barrier diagrams could be used in circumstances where a qualitative approach was justified, but would not be appropriate in situations where use of a semi-quantitative or quantitative approach was demanded.

10. REFERENCES

1. Health and Safety Executive (1999). 'A guide to the Control of Major Accident Hazards Regulations 1999'. HSE Books, L111.
2. CCPS, (2001). 'Layer of Protection Analysis – Simplified Process Risk Assessment'. American Institute of Chemical Engineers, New York.
3. International Electrotechnical Commission (1998). 'Functional Safety of Electrical / Electronic / Programmable Electronic Safety – related Systems, Parts 1-7'. IEC61508, IEC, Geneva.
4. International Electrotechnical Commission (2001). 'Functional Safety Instrumented Systems for the Process Industry Sector, Parts 1-3'. (Draft in Progress), IEC61511, IEC, Geneva.
5. Charnock, C (2001). 'IEC61508 – A Practical Approach to its Application in the Process Industry'. Institution of Chemical Engineers Symposium Series 148 (HAZARDS XVI), pp667-682.
6. CCPS (2000). 'Guidelines for Chemical Process Quantitative Risk Assessment, Second Edition'. American Institute of Chemical Engineers, New York.
7. CCPS (1989). 'Guidelines for Process Equipment Reliability Data'. American Institute of Chemical Engineers, New York.
8. IEEE (1984). 'ANSI/IEEE Standard 500-1994: Guide to the Collection and Presentation of Electrical, Electronic, and Sensing Component Reliability Data for Nuclear-Power Generating Stations'. IEEE Standards Association.
9. EuReData (1989). 'Reliability Data Collection and Use in Risk and Availability Assessment'. Proceedings of the 5th EuReData conference, Heidelberg, Germany, 1986.
10. Det Norske Veritas (1997). 'Offshore Reliability Data Handbook'. 3rd ed., OREDA participants, Hovik, Norway.
11. CCPS (1993). 'Guidelines for Safe Automation of Chemical Processes'. American Institute of Chemical Engineers.
12. Naylor P J, Maddison T and Stansfield R (2000). 'TRAM: Technical Risk Audit Methodology for COMAH Sites'. Hazards XV The Process, its Safety, and the Environment – Getting it Right, Manchester 2000. IChemE Symposium Series 147.
13. Roberts, I (2000). 'Application of TRAM Version 2.07 to the TOTAL LPG Storage Facility at Hauconcourt, France'. AEA Technology Report AEAT/RSMS/RD00347/R1 Issue 1.
14. Health and Safety Executive (2001). 'Reducing Risks, Protecting People HSE's decision-making process'. HSE Books, C100.
15. Bellamy, L J and Brouwer W G J (1999). 'AVRIM2, a Dutch major hazard assessment and inspection tool'. J. Hazardous Materials 65 (1999) 191-210.
16. Bellamy L J and van der Schaaf J (1999). 'Major Hazard Management: Technical – Management Links and the AVRIM2 Method'. Proceedings of the Seveso 2000 European Conference, Athens 1999.
17. Bellamy L J, Geyer T A W and Astley J A (1989). 'Evaluation of the human contribution to pipework and in-line equipment failure frequencies'. HSE Contract Research Report 15/1989.
18. Vasina, P and Van Gils E (2001). 'PLANOP: A Methodology for the Progressive Analysis and Optimisation of the Protective Layers of a Process Installation'. Loss Prevention and Safety Promotion in the Process Industries, Proceedings of the 10th International Symposium, 19-21 June 2001, Stockholm, Sweden, pp 533-544.
19. Allum, S and Wells G L (1993). 'Short-Cut Risk Assessment'. Trans IChemE, Vol 71, Part B, pp 161-168.

20. Wells, G L et al. (1992). 'Incident scenarios: their identification and evaluation'. Trans IChemE, Vol 70, Part B, pp 179-188.

21. Selig, R (2002). 'Communication of Complex Safety Issues Using Barrier Diagrams'. Fire and Blast Issues of the COMAH Safety Case, Fire and Blast Interest Group, Meeting 17 April 2002.

22. Health and Safety Executive (1999). 'Preparing Safety Reports: Control of Major Accident Hazard Regulations 1999'. HSE Books, HSG190.

23. HSE / HID (2002). 'Guidance on 'As Low As Reasonably Practicable' (ALARP) Decisions in Control of Major Accident Hazards (COMAH)'. SPC/Permissioning/12, available at: http://www.hse.gov.uk/hid/spc/perm12/index.htm .

This page is left intentionally blank