TRAM: TECHNICAL RISK AUDIT METHODOLOGY FOR COMAH SITES

Patrick J. Naylor
Hazardous Installations Division, Health & Safety Executive, Bootle, L20 3RA, UK.
Dr.Tom Maddison
Hazardous Installations Division, Health & Safety Executive, Bootle, L20 3RA, UK.
Richard Stansfield
AEA Technology, Abingdon, Oxfordshire, OX14 3DB, UK

TRAM is defined, and explained as an audit methodology consistent and coherent with the principles of the widely-accepted International Electrotechnical Commission (IEC) standard IEC 61508 (electronic safeguarding systems)[1]. It is proposed that these principles can be applied beyond instrumented protection systems, encompassing a range of engineered and physical "Lines of Defence". The conceptual basis for the TRAM methodology is described, and this is placed in the context of other audit methodologies. Finally, its strength as both an assessment and inspection tool, to be used by HSE inspectors for COMAH sites, is described.

Keywords: risk assessment, safety report, line of defence, safety integrity level.

INTRODUCTION

With the realisation of the Control of Major Accident Hazard (COMAH)[7] regulations 1999, the Health and Safety Executive's (HSE) Hazardous Installations Division (HID) have regulatory responsibility for approximately 9000 sites covered by the regulations, of which some 300 are "top-tier" sites. These sites were formerly covered by the preceding Control of Industrial Major Accident Hazard Regulations 1984 (CIMAH)[6]. Apart from the *inspection* activity associated with such a number, there is the necessary *assessment* of safety report submissions from the sites covered by the regulations – all to be undertaken by the HSE/HID. This represents a significant resource "challenge". Coupled with this problem is the new charging regime within which the HSE now operates in addressing the above workload: this invokes a requirement for the HSE to be consistent in its attention to its "customers", in terms of both the attention paid to sites and companies, and judgements made as a result of inspection or assessment activity. There is therefore a requirement for a consistent, resource-efficient methodology to address these needs, to which end the HSE – in conjunction with AEA Technology – devised the Technical Risk Audit Methodology (TRAM).

SUMMARY OF METHODOLOGY

TRAM is a technique for the approximate estimation of both risk, and associated risk reduction measures, for given process sites/plant. The methodology is targeted principally at the assessment of existing operational installations and initially addressed the assessment of Liquid Petroleum Gas (LPG) Installations[2].

The technique requires hazard scenarios to be synthesised in event-tree format. This is to identify those risk reduction measures that feature at given nodes of the event tree, whose successful action at that node would result in a "safe" outcome from it (Figure 1). These risk reduction measures are termed "Lines of Defence" (or "LOD"). TRAM is realised as a computer modelling package whose algorithm requires fault sequence frequency data and end event consequence data to be input, from which a computed estimate is derived for the number of LODs *required* to reduce the risks of the scenario to a tolerable level. The auditor must then provide input in terms of technical judgement as a result of assessment or inspection activity, expressed in terms of quantified "attributes" associated with the various LODs that are relevant to the scenario being studied. Therefore, in the context of TRAM, audit is defined as encompassing both assessment and inspection activities.

In very basic terms: where the number of LODs already in place for the scenario in question exceed those estimated as necessary by TRAM, risks may be judged to have been reduced to ALARP (As Low As Reasonably Practicable). Conversely, if the estimated number of LODs falls short of that number required, further (and more detailed) consideration may be deemed necessary: e.g. full QRA (Quantitative Risk Assessment).

EARLIER WORK

Previous work undertaken on the application of TRAM dealt with Liquid Petroleum Gas Installations. It developed from the application of PRS (the Pilot Risk Study Method)[2].

This work recognised the need for safety assessment techniques beyond mere inspection. However, as opposed to QRA, it called for a "semi-formal" method of risk assessment for consistency, to provide an audit trail, and to generate a history for the plant in question. It recognised that there was a need for a structured and systematic approach to safety assessment in the hazardous industries, but pointed out that – whereas there was much HSE activity in the past in terms of *management* arrangements and Safety Management Systems – HSE, as the regulator, needed to do more developing the *technical* side of the work.

The initial development of an audit technology was therefore framed in terms of the work on LPG installations, where the risk reduction methods vary from site to site, but where the safety of such plant depends upon the preventative and mitigation methods. The general approach, as a forerunner to TRAM, involved the use of frequency/consequence analysis and an initial identification of discrete Lines of Defence and their classification (using a simple Frequency/Consequence matrix). Coupled with this was a LOD assessment, describing LODs as "active", "passive" or "physical" systems. An "active" system is defined as on that requires an external power source for its successful operation, as opposed to a passive system that does not (e.g. a mechanical relief valve), with a physical system being typically one where the defence system may be as simple as natural heat dispersion or cold weather conditions.
The numerical scheme in PRS defined a LOD Rating of 1 for a protection system with failure probability P of 10^{-2}, i.e.

$$LOD_{PRS} = -\frac{1}{2} Log_{10}\left(P\right) \qquad 1$$

The initial results of using this manual technique of LOD assessment showed much promise on the LPG subject matter, achieving a high level of consistency in the LOD assessment of the installations concerned. Although generating consistent results for the installations under study, the field trials were limited to a single type of installation. It was not possible for diverse plant to be assessed, nor was it possible for diverse assessments of the same plant to be undertaken. The consistency achieved therefore was only between installations of the same type and the frequency and consequence classification was not rooted in numerical analysis. Because of this, it was necessary to develop TRAM as a numerical model. It has been described in the past as a "semi-quantitative" form of risk assessment, but it is perhaps more apt to describe it as a method of "approximation".

METHODOLOGY

TRAM has been modified from the original PRS in terms of the definition of a LOD, which aligns it with IEC61508[1] (see equation 17 and Table 3). This modifies equation 1 above such that TRAM redefines a LOD rating as being 1 for a system with failure probability 10^{-1}, i.e.

$$L.O.D._{TRAM} = -Log_{10}(P) \qquad 2$$

In addition, whereas PRS used a frequency/consequence matrix when evaluating the acceptability of LODs, TRAM redefined the Consequence Category of a final fault sequence outcome as being a number in the range from 1 (no safety consequences) to 7 (catastrophic accident involving multiple deaths). In practice, considering only the safety and environmental consequences, the range used is 3-7, as per Table 2.

FREQUENCY CLASS

In TRAM, the Frequency Class of fault sequence i is defined according to:

$$F_i = -\mathrm{Log}_{10}(f_i) \qquad 3$$

where f_i is the initiating event frequency. PRS originally used a "look-up" table (Table 1), however the changes implemented in TRAM did not alter this aspect of the concept, only the *implementation* of the concept in the computerised model.

The main change from PRS to TRAM, however, was the introduction of a generic risk model based on event trees. In the PRS method, the user (HSE inspector) was required to analyse any fault sequence based on his knowledge of the plant and process. By using a generic risk model, greater consistency is introduced by TRAM allowing the direction of inspection resources towards risk dominant plants.

When using the computerised version of TRAM, the user concentrates on evaluating the effectiveness of the plant's safety systems. Based on a combination of judgement and quantification, a LOD Rating is derived for each safety system. In addition, plant data is used to derive the Frequency Class and Consequence Category for the various fault sequences. Once these data are entered, TRAM calculates the risk dominant fault sequences and hence total risk in terms of Individual Risk Per Annum (IRPA) for the operating scenario under study. The use of a generic risk model reduces considerably the work required and ensures that all applications of the method use the same assumptions regarding application of LODs to scenarios.

Table 1 Frequency Classes

Absolute frequency f_i	Frequency class F_i (= $-\log_{10}f_i$)
1×10^{-1}	1
1×10^{-2}	2
1×10^{-3}	3
1×10^{-4}	4
1×10^{-5}	5
1×10^{-6}	6
1×10^{-7}	7

RISK ANALYSIS BASIS

The risk, R_i, due to event i is related to its consequence and frequency of occurrence (Table 1) as follows:

$$R_i = f_i \; c_i \; P_i \qquad 4$$

where f_i is the initiating event frequency (occurrences per year) of fault sequence i, and P_i is the probability of this event developing into a major accident of consequence c_i.
This risk may be individual risk (risk to a worker on the plant) or a contributor to societal risk, depending on how c_i is defined. For individual risk, c_i would be the probability of death of an individual worker (IRPA); for societal risk, c_i would be a measure of the *total* number of deaths expected for this fault sequence. In both cases, the total risk is obtained by summing the contributions from all applicable fault sequences. The societal risk is usually expressed as the total frequency of faults leading to similar consequences.

Assuming that "protection" systems act *independently* of each other, the probability of an initiating event developing into a major accident is given by:

$$P_i = \prod_{j=1}^{n} P_{i,j} \qquad 5$$

where $P_{i,j}$ is the failure probability of defence system j in fault sequence i. These protection systems can be physical systems (whether "active", "passive" or physical – as previously defined), natural processes or managerial controls which either help prevent the initiating event developing into a major accident or mitigate its consequences.

CONSEQUENCE CATEGORY

The acceptability of risk is established by comparing it with criteria. In TRAM, the acceptability criteria are included in the definition of the Consequence Category such that a simple numerical process may be used to judge acceptability.

Societal Risk is usually represented as an f-N curve, which relates the total frequency (f) of a major accident to the number of fatalities (N). To be acceptable, the sum of the frequencies of major accidents leading to between N and 10 x N fatalities should be less than a chosen criterion, α_N which depends on N, i.e.

$$f_{\text{N to 10 N fatalities}} = \sum_{\text{Faults with N to 10N fatalities}} f_i \prod_{j=1}^{n} P_{i,j} < \alpha_N \qquad 6$$

A Consequence Category, C_i can be defined such that the following expression, when true, indicates acceptability:

$$f_i \prod_{j=1}^{n} P_{i,j} < 10^{-C_i} \qquad 7$$

To relate C_i to α_N it is necessary to estimate the number of fault sequences which can give rise to between N and 10 x N fatalities. If this number is m, then the Consequence Category is given as

$$C_i = -Log_{10}\left(\frac{\alpha_N}{m}\right) \qquad 8$$

As an example, suppose that faults leading to between 1 and 10 fatalities are “acceptable” if the frequency of occurrence is less than 10^{-6}/year, and that there are typically ten such fault sequences. In this case, m is 10 and α_N equals 10^{-6}, leading to a Consequence Category of 7 for each of the fault sequences. If the Consequence Category is defined in this way, then each individual fault sequence will be acceptable if the following expression, derived from equation 6, is true:

$$F_i + \sum_{j=i}^{n} LOD_i - C_i > 0 \qquad 9$$

where F_i is the Frequency “Class”. The second term in this equation is called the Required (or “Derived”) LOD Rating and for acceptability it is required that:

$$F_i + LOD_{\mathrm{Re}quired} \geq C_i \qquad 10$$

The Consequence Category can also be defined in terms of the risk posed to individual workers. The acceptability of the individual worker risk can be established by evaluating the total frequency of all fault sequences which lead to deaths and comparing it with an acceptability criterion. For a situation where the risk is taken as “acceptable” (offset by the economic benefit associated with the risk) an “acceptable” level of risk may be 10^{-4}/year risk of death, while 10^{-3}/year would be at the limit of tolerability[3].

In TRAM, the level of risk is established by summing the frequency of occurrence of all fault sequences which could lead to a worker fatality i.e.

$$R_{Wor\,\mathrm{ker}} = \sum_{All\, i\, where\, c_i > c_{fatal}} f_i \prod_{j=1}^{n} P_{i,j} < \alpha_{Wor\,\mathrm{ker}} \qquad 11$$

A Consequence Category is defined in a similar way as before, i.e.:

$$C_i = -Log_{10}\left(\frac{\alpha_{Wor\,\mathrm{ker}}}{m}\right) \qquad 12$$

where m is the number of fault sequences which could lead to a worker fatality. As an example, if an acceptable worker risk is 10^{-3}/year, then, for 10 fault sequences which could lead to a fatality, the Consequence Category, C_i, would be 4 and each fault sequence would be acceptable if:

$$F_i + \sum_{j=i}^{n} LOD_i - C_i > 0 \qquad 13$$

SELECTION OF CONSEQUENCE CATEGORY

The above analysis shows that care must be taken in the definition of the Consequence Category as it incorporates the acceptability criterion whilst depending on the number of fault sequences. In addition, because at least two acceptability criteria can be used (based on worker risk and on societal risk) the definition is not necessarily unique. In order to circumvent these problems, a standard definition of Consequence Category is provided in TRAM, based on a logarithmic scale running from 1 (minor economic consequences) to 6 and beyond (multiple deaths). The definition covers both individual risk and societal risk and is broadly consistent with HSE guidelines on tolerability of risk (TOR)[3] .

The scale is logarithmic so, for example, a Consequence Category 6 accident is considered to be ten times more severe than a Consequence Category 5 accident. For major accidents leading to multiple fatalities, a suitable acceptability criterion may be that the summed frequency is less than 10^{-6}/year. If there were typically 10 such fault sequences, each fault sequence would be allocated a Consequence Category of 7 and the Available LODs are checked to ensure that equation 10 is satisfied.

Similarly, for faults leading to a worker fatality, an individual risk (IRPA) of 10^{-3}/year is at the limit of acceptability, based on TOR[3] guidelines. If there are 10 such fault sequences leading to a single fatality, each would be assigned a Consequence Category of 4 and the LODs checked to ensure equation 10 is satisfied. On this scale (which, on the basis of the above discussion, includes an acceptability criterion) major accidents leading to multiple deaths would have a Consequence Category of 7 and a fire or VCE (Vapour Cloud Explosion) leading to a lower number of deaths would have a Consequence Category of 6. A small fire involving (e.g.) a limited quantity of Liquid Petroleum Gase (LPG), with possibly one worker fatality, would have a Consequence Category of 4 on this basis.

Table 2: Consequence Categories for TRAM

Conseqence Category	**Descriptor**
> 7	**Catastrophic Accident**: gross disruption; large numbers of dead; very newsworthy; Public Enquiry; impacts on regulatory framework &/ law.
> 6	**Major accident**: significant off-site disruption; many dead and injured; main feature of national news; results in public enquiry &/ 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; dead 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; not mentioned in news; site/company investigation only.
>= 3	**Limited accident** of low consequence.

LINES OF DEFENCE

The concept of Line of Defence is used as the key measure in assessing the margin of acceptability by which protective systems "outweigh" the risks against which they are designed to act.

A number of alternative measures can be used to decide whether risk from individual fault sequences or from all fault sequences is acceptable. One measure of the acceptability of the defence systems in a particular fault sequence can be obtained by looking at the difference between the LOD Rating required to give acceptability and the LOD Rating actually available. This is termed the "Excess LOD Rating" and is defined as follows:

$$LOD_{Excess} = LOD_{Available} - LOD_{Re\,quired} \qquad 14$$

To be acceptable, LOD_{Excess} should be <u>positive</u>, i.e.

$$\text{For all fault sequences i,} \quad LOD_{Excess} > 0 \qquad 15$$

In TRAM, fault sequences may be ranked by LOD_{Excess} and fault sequences where LOD_{Excess} is negative or less than a small positive number (e.g. 1) indicate further investigation.

ACCIDENT FREQUENCY

The accident frequency due to fault sequence i is given by:

$$f_{Major\ Accident} = 10^{-(C_i+LOD_{Excess})} = 10^{-(F_i+LOD_{Available})} \qquad 16$$

THE TRAM RISK MODEL

TRAM is a form of event tree modelling whereby the decision point – or node – in the event tree is represented by a Line Of Defence (LOD), whose failure at that point defines the event. It deals with fault trees of systems whose failure leads to the true critical initial event, by incorporating them into a multi-branch event tree structure by transposition[4]. This facilitates the coding required for the modelling of a given process scenario in TRAM.

The concept of an attribute of a LOD is an important one. Effectively, any given protection system may have a number of components or features, which together describe the LOD, and each of which may be assessed for effectiveness. "Derived LOD rating" is the term given to the LOD *requirement*, generated by the methodology, prior to its assessment and/or inspection, as required by the TRAM audit. In effect, it is the calculated value that the LOD should have, in order for it to be an effective means of protection in the given application. The term "derived" means that it is computed/calculated as a result of the frequency and consequence data input into the software model. Similarly, the "Assessed LOD rating" is the quantification given to the LOD as a result of data gathered by the auditor, whether by inspection or assessment. This is a separately computed value, which then provides a comparison with the derived LOD value previously computed.

The TRAM Risk Model therefore comprises the following components:

- **Frequency Classes** of initiating Events, derived from plant/generic data - e.g. release rates - originally obtained in the earlier work on LPG facilities.
- **Scenario Types**, which bring together a number of initiating events which lead to similar consequences.
- **Lines of Defence (LODs)**, which represent safety features on the plant designed to prevent a major accident developing from the initiating event, or mitigate the consequences of a major accident should it develop. (*LODs are quantified using information collected during the audit).*
- **Consequence Categories,** which provide a means of classifying a major accident based on its possible consequences.
- **Event trees**, which link the above components and represent fault sequences leading from an initiating event to major accidents.

This risk model is based on a classical hazard escalation model as per Figure 1.

PRACTICAL AUDIT METHOD

1. Once the boundary of the process is defined, it may be described from the *available* information in the (COMAH) safety report and the event tree may be derived incorporating all fault sequences. At this stage, the key initiating events and ultimate scenarios may be identified from the material available, together with the applicable LODs. The LODs so identified are then tabulated.
2. Once the above information is collated from the written submission, the process scenario is configured in the TRAM software package. Each branch of the event tree for each of the applicable "fault paths" is entered into the database as individual records; frequency classes (Table 1) are assigned to initiating events (from empirical data available); and consequence categories are inferred from the selection shown in Table 2.
3. Whether by report assessment or site inspection (or both - as appropriate), the fault sequences of the event tree are traced through by the auditor, examining each of the designated LODs at each stage, and selecting the most appropriate attribute to describe it, using the descriptors provided from a proforma, in conjunction with the auditor's own engineering judgement.
4. Once the raw-data is gathered as described above, it is entered into the TRAM model against the LOD and LOD-attribute fields. The excess LOD calculation is performed by the computer model along with residual risk, expressed as IRPA.
5. The results may be interpreted and compared with acceptability criteria.

RELATIONSHIP TO IEC 61508

The IEC61508 standard[1] describes the use of safety-related systems to provide an appropriate level of "functional safety": that is to say, the contribution to overall safety by correct performance of the safety-related systems.

This concept is of fundamental importance, since it describes the two key requirements that have to be specified before analysis of the protection system may be made: that the safety-related system performs the safety functions that have been specified; and that the safety functions be performed with the degree of confidence appropriate to the application, so that the overall safety (risk reduction) is achieved.

The second of these key requirements introduces the concept of Safety Integrity Level (SIL), which describes the performance of a safety system in terms of its probability of failure on demand, and attaches discrete levels (SILs) to systems ranging from 1 (lowest) to 4 (highest). Once a SIL has been determined for a particular safeguarding protection system, it forms the basis of requirements for the safety integrity requirement. Often the application will indicate the SIL of the system to be specified. Conversely, if a Safeguarding System has a SIL assigned to it, it (theoretically) will have the same integrity characteristics irrespective of the application.

RISK GRAPH APPROACH

In order to more fully understand the link between TRAM and IEC61508[1], it is relevant to understand the derivation of the Safety Integrity Level concept, which is based on Risk Assessment Principles.

The Risk Graph provides a frequency/consequence basis for the assignation of Safety Integrity Levels – in effect, it is a *qualitative* method of deriving a *quantified* SIL. However, the IEC61508[1] standard is based, not on the consequence of failure, but on the amount of risk reduction which it is intended to achieve. The protected plant or machinery is termed the "Equipment Under Control" (EUC). As can be seen, it follows the risk matrix (frequency versus consequence) mapping principle, as shown in Figure 2.

As can be seen from the Table 3, the definition of SIL is linked to the Probability of Failure on Demand (PFD) of the Safeguarding/Protection system acting as specified. However, the SILs are somewhat different depending on the protection context. With machinery, which is constantly in use, there is a continuous demand-rate on a safety system (e.g. a machine guarding/interlock system) and so SIL is linked to probability of dangerous failure *per hour* (PF/h). However, the EUC is the process plant of a Hazardous Installation for the purposes of this paper, where there is only a periodic demand on chemical plant protection systems (e.g. emergency shutdown systems), and so the SIL – in this context – is linked to probability of failure *per demand* (PFD). This is shown in the Table 3 under *low-demand* and *high-demand* modes respectively.

The LOD concept in TRAM is linked logically to that of SIL in IEC61508[1] as a direct result of the strategic change made from the earlier Pilot Risk Study work, where it was recognised that IEC61508 was becoming a widely promulgated, and widely used standard. It was important that – if TRAM was to become an acceptable methodology to both the regulator and industry – it did not conflict with this standard in any way. To this end, the numerical definition of a Line of Defence was changed to the following:

$$\text{L.O.D.} \quad = \quad -\text{Log}_{10}\,(\text{P.F.D.}) \qquad 17$$

And therefore,

$$\text{L.O.D. } (n\ldots n+1) \quad \equiv \quad \text{S.I.L. } (n). \qquad 18$$

as shown in Table 3.

Table 3 SIL/LOD/PFD Relationship

Safety Integrity Level (SIL)	Equivalent LOD "Rating"	PFD Range (Low Demand Mode)	**PF/h Range (High Demand Mode)*
4	4-5	$10^{-5}\ldots10^{-4}$	*$10^{-9}\ldots10^{-8}$*
3	3-4	$10^{-4}\ldots10^{-3}$	*$10^{-8}\ldots10^{-7}$*
2	2-3	$10^{-3}\ldots10^{-2}$	*$10^{-7}\ldots10^{-6}$*
1	1-2	$10^{-2}\ldots10^{-1}$	*$10^{-6}\ldots10^{-5}$*

(The shaded high demand mode of operation is not applicable to the subject of this study).

As can be seen, both LOD and SIL are expressions of probability of failure on demand (PFD). However, whereas SILs are discrete *integer* values, LODs may have a *continuous* value within the ranges shown. This is an important distinction.

CONTROL SYSTEMS IN TRAM

In the area of Control Systems, TRAM considers Instrument-based Protection Systems as "active" risk-reduction measures, (as opposed to "passive" - e.g. fire/blast walls). Such Instrument/Control systems are often the most safety critical element in the defence hierarchy, particularly in instances where the system acts in the absence of inherent safety in the process plant. Furthermore, the complexity of such systems and their associated failure modes requires a sound audit methodology capable of being configured within TRAM. However, as a rule of thumb, the SIL4 level of system integrity is beyond that which is normally found or proposed in the chemical process industries for instrument-based protection systems.

OTHER AUDIT METHODOLOGIES

In order to understand the particular application of TRAM as an audit method, it is important to place it in the context of other audit techniques found in industry. This section briefly describes those methods that are targeted at the same work area as TRAM.

AVRIM[8] – THE DUTCH EXPERIENCE

AVRIM2 is a safety report and site inspection methodology commissioned and implemented by the Dutch Ministry of Social Affairs and Employment[8]. It is targeted at "major hazard installations", broadly comparable to those UK onshore petrochemical installations covered by COMAH. It was designed as a tool to support the activities of the Labour Inspectorate of this Ministry, to provide a uniform and complete approach to address the issues of risk.

It is principally focused on the assessment and inspection issues of those controls which a company has to prevent *loss of containment* of hazardous materials, and to those systems by which a company monitors and improves the effectiveness of such controls. There is an emphasis on safety aspects of the *design*, and on risk *management* systems.

As with COMAH, it originates from the Seveso II directive, and therefore as an audit methodology it too follows the principles of ISO 9000[5]in that it provides for the examination of the safety report (adequacy) and the verification that the measures cited in the report are applied in practice (compliance).

As with TRAM, the AVRIM2 methodology has models to capture the generic causes of failure, based on a risk-matrix/ranking approach. It further proposes the use of a number of generic fault trees to describe the pathways to the given risk event. AVRIM 2 also uses the concept of "Line of Defence", but with a different meaning: it is not a "unit" of risk reduction, as with TRAM; but a management system or control in place to act against the hazard. It is – unlike TRAM – currently confined to the hazards of loss of containment.

The central model of AVRIM is the "control and monitoring loop", and defines the chief lines of defence of a company as being the design, construction, operation and maintenance of its installation. It does not generate a *quantified* outcome in a similar manner to TRAM , it rather considers each defence on its own merits, as being *qualitatively* sufficient or not.

HS(G)65 – THE POPMAR MODEL[9]

The HSE set-out a Safety Management System method (HS(G)65, 1997)[9] in which it proposed an hierarchical approach to safety management, against which audit is possible at both the site and corporate level. It sub-divides a companies management into *policy, organising, planning, measurement* of effectiveness, *audit* and *review* of performance. This became known as the "POPMAR" model, and is shown in Figure 3.

It is important to state that the POPMAR model represents a *non-technical* and *qualitative* audit method. It is not a quantitative model. It deals more with the structure of an organisation and its management provisions to deal with health and safety in its broadest terms. The common ground between this non-technical methodology and that of TRAM is that it too follows the principles of ISO 9000[5], in that written procedures have to be formulated against which they can be subsequently validated by practical examination.

This guidance is useful in that it is *people* focused rather than *plant* focused, and it develops each of the stages outlined in the flowchart methodology, but it addresses the human elements - more of occupational health and procedural/cultural aspects of managing for safety - than of safety "engineering" itself. As such, it is not comparable with the TRAM method.

ENGINEERING JUDGEMENT CONSIDERATIONS

The TRAM methodology is reliant upon the input of sound engineering/technical judgement. This can be assisted by the quality of the knowledge-based tool provided by the software package in which TRAM is now realised. However, ultimately, this in turn relies upon sufficient knowledge of the Inspector/Auditor who must select, from a range of attributes applicable to a generic LOD, that which most accurately describes the protection system under examination. In addition, the auditor must be able to sensibly assign frequency classes and consequence categories to given fault sequences, and to be capable of adducing an event tree to describe the hazardous scenario from information provided by the operator.

COMAH APPLICABILITY

Having said this, TRAM is envisaged to provide an assessment/inspection (i.e.audit) format for many of the sites covered by the COMAH[7] regulations, releasing resource for the attention on major hazard, top-tier sites. The TRAM methodology, by allowing both individual excess LOD, and total fault-sequence excess LOD quantification, assists decision-making in terms of deficiency and, more specifically, *serious* deficiency as defined by COMAH.

CONCLUSIONS

The advantages of the TRAM technique are many. It is firstly a methodology which improves the efficiency of the available assessment/inspection resource, whilst retaining a formal, objective methodology for the work. It is a semi-quantitative / approximation method of risk and LOD which is not as (assessment) resource intensive as full Quantitative Risk Assessment (QRA), but may indicate where the latter is necessary. It complements (and incorporates) much of the established techniques of risk assessment such as Event Tree Analysis (ETA), Fault Tree Analysis (FTA) and Failure Mode and Effects Analysis (FMEA), whilst incorporating the principles of reliability engineering. It follows the International Standards Organisation's (ISO's) Quality model ISO 9000[5], as the audit procedure deals with both the "compliance" criteria in the assessment component, and the "adequacy" of defences in the inspection. Most of all, it provides - probably for the first time - an integrated approach to assessment and inspection, which takes account of engineering judgement against good industry practice, and provides quantification/rating for practical considerations such as plant condition, maintenance, systems of work, and training.

REFERENCES

1. IEC 61508 - *Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems*, International Electrotechnical Commission (IEC), Geneva, 1998

2. Maddison, T and Kirk, P.G. (1995)."Application of Pilot Risk Study Methods to the Safety Inspection of Industrial Plant." *Loss Prevention Bulletin* 125, 11-16.

3. “TOR” HSE (1992) . *Tolerability of Risk from Nuclear Power Stations*. HMSO (ISBN 0 11 8863681).

4. Aldersey.M.L., Lees.F.P.,Rushton.A.G.(1991). Knowledge Elicitation and Representation for Diagnostic Tasks in the Process Industries. Rugby: Institution of Chemical Engineers. Trans. I.Chem.E.

5. BS-EN-ISO 9000-1.(1994). Quality Management and Assurance standards: Guidelines for use.

6. HSE. (1984). A Guide to the control of Industrial Major Accident Hazard Regulations 1984 (CIMAH).London: HMSO. Ref. HS(R)21 rev.

7. HSE. (1999). A Guide to the Control of Major Accident Hazard Regulations 1999. Sheffield: HSE Books. Ref. L111.

8. Netherlands Ministry of Social Affairs and Employment. (1996). *Arbeids Veiligheids Rapport Inspectiemethodiek (AVRIM): AVRIM2 Handboek*. The Hague: SZW.

9. HSE (1997). *Successful Health and Safety Management*. HS(G)65. Norwich: HMSO.

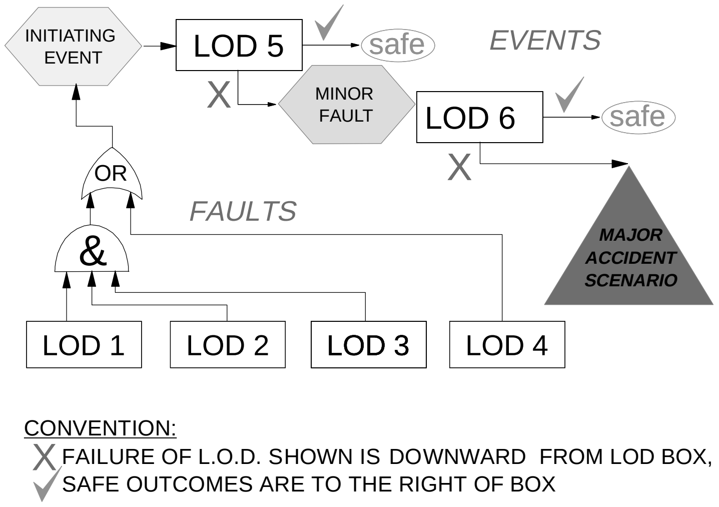
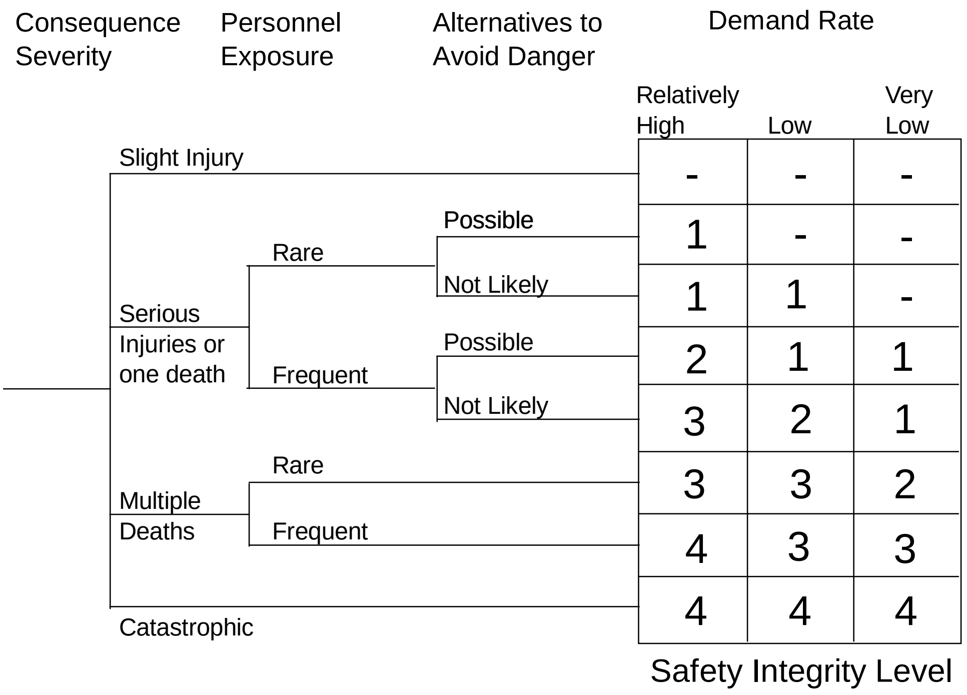


Figure 1: The TRAM Risk Model



Relatively High	Low	Very Low
-	-	-
1	-	-
1	1	-
2	1	1
3	2	1
3	3	2
4	3	3
4	4	4

Figure 2: The IEC61508 "Risk Graph" Approach

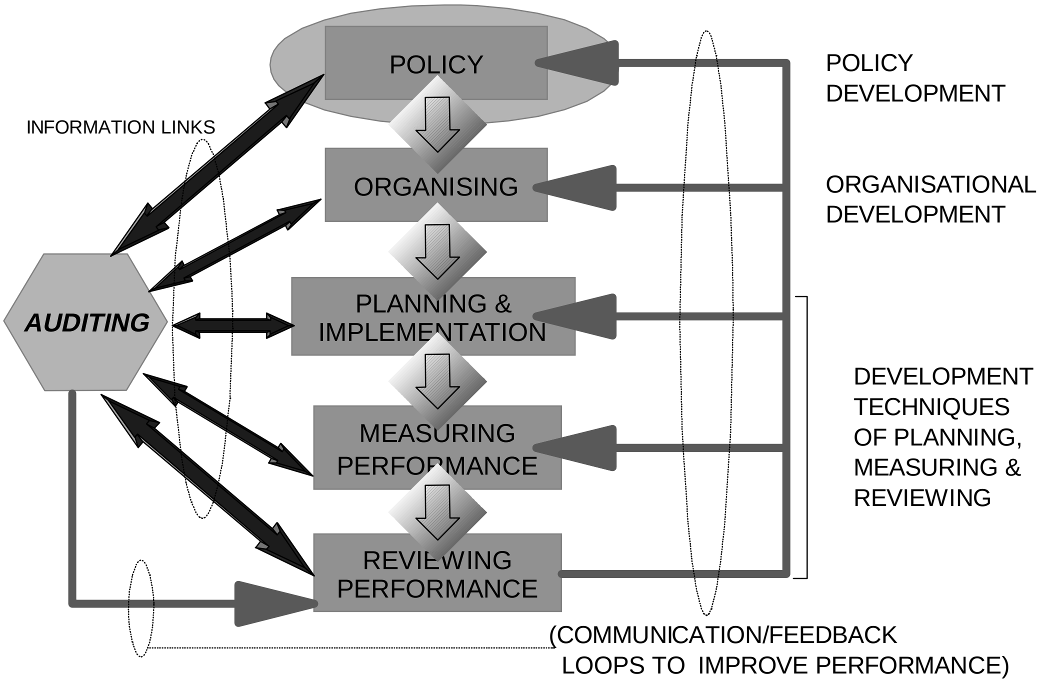

POLICY
ORGANISING
PLANNING & IMPLEMENTATION
MEASURING PERFORMANCE
REVIEWING PERFORMANCE
AUDITING
INFORMATION LINKS
POLICY DEVELOPMENT
ORGANISATIONAL DEVELOPMENT
DEVELOPMENT TECHNIQUES OF PLANNING, MEASURING & REVIEWING
(COMMUNICATION/FEEDBACK LOOPS TO IMPROVE PERFORMANCE)

Figure 3: The HS(G)65 "POPMAR" Audit Model