TOP LEVEL RISK STUDY – A COST EFFECTIVE QUANTIFIED RISK ASSESSMENT

R.I. Facer, J.A.S. Ashurst, and K. A. Lee
EQE International Limited, 500 Longbarn Boulevard, Birchwood, Warrington, Cheshire WA2 0XF

Probabilistic Safety Assessment (PSA) or Quantified Risk Assessment (QRA) is an internationally accepted approach to modelling the contributors to the risk from an industrial facility, plant or process. A full PSA/QRA is a time consuming and costly exercise. A Top Level Risk Study (TLRS) is a means of achieving the benefits of a QRA more quickly, for less cost, and in a form to allow much easier use and interpretation. A TLRS is based upon the combination of experience in modelling and assessing the reliability of complex systems. Risk and Safety Management are continuous processes, especially with respect to the design and implementation of loss prevention and loss control measures. These aspects generally involve a continued expenditure on the plant, and it is important that the expenditure is directed at the areas which will contribute the maximum return in the form of risk reduction. The TLRS forms a useful input to such Cost Benefit Analysis (CBA), and again this information contributes to efficient Risk and Safety Management.

Keywords: Risk assessment, CBA, safety management, option studies, risk reduction.

INTRODUCTION

The Top Level Risk Study (TLRS) is a logical, structured, approach to deriving an indication of the risk from operation of an industrial facility, with identification of dominant weaknesses, and it facilitates modelling of alternative scenarios for safety improvements and Risk Management, utilising probabilistic techniques based upon demonstrated experience based assessments of system performance and reliability.

The TLRS is an Event Tree based assessment, with the top event reliabilities being assigned on the basis of judgement and the use of a set of experience based guidelines, instead of using the normal time consuming Fault Tree approach. It is accepted that this is a more approximate approach than a full PSA/QRA, however, the results are available in a considerably shorter timescale and, experience indicates, are not significantly different.

The information provided by a TLRS includes graphical representation of accident sequences in the form of Event Trees and a quantified analysis of the risk from operation. In addition, and perhaps just as important, the methodology also provides important analysis of both the Initiating Events and the system level Top Events included in the model to allow the most significant data items and assumptions to be most carefully reviewed.

Due to the approximate nature of the assigning of data, the model is developed in such a way as to facilitate numerous sensitivity studies to be performed on both the Initiating Event and system level Top Event data, in an efficient manner. This latter feature also enables ease of modification to the models in order to investigate the relative benefits of different proposed safety improvement and Risk Management scenarios.

EQE International, whilst working for the Government of Bulgaria, embarked on the development of a risk evaluation approach which utilised the completeness and coherence elements of a PSA/QRA, but that would develop useful results in a timely manner. The result is the Top Level Risk Study, which has been successfully applied to nuclear power and nuclear-chemical plants but can easily be adapted for other facilities and processes for the assessment of environmental, safety or business interruption aspects.

METHODOLOGY

The methodology developed for the TLRS is based on the PSA/QRA methodology, but modified to result in a tool which can be used to give timely and cost efficient information for both safety and risk management and audit purposes. A prime concern throughout the development process has been that the approach must remain logical and structured to be of use to Safety and Risk Managers and regulators.

The three key features involved in the construction of a TLRS are Operational Factors/Events, Protections and Consequences. Examples of these are shown in Figure 1. Subsections for each of the three features can be considered for the appropriate industry under review.

The key steps which make up the TLRS approach are as follows:

Understanding the Plant Design

The first, and one of the most important tasks in performing any risk study is to develop a thorough understanding of the plant or facility under investigation. This should cover the system and component design, including all support requirements and arrangements, normal and post fault duty, and any associated operator actions. In addition, it is

important that operating regimes and principles, and the safety philosophy are understood.

Fault Schedule

The fault schedule development is similar to that which would be expected for a full QRA. Plant specific faults are identified and a comprehensive listing of all applicable Initiating Events compiled. Alternatively, it may be more appropriate to use a checklist/walkdown approach for identification of the potential hazards. However the listing is developed, it is then reviewed and faults may be removed on the basis of low potential consequence or acceptably low frequency, and others are bounded to give a listing of the faults which are to be carried through to the probabilistic analysis.

The TLRS is an Event Tree based approach which takes each of the identified and bounded Initiating Events and models the potential accident sequences which may follow, taking into account the success and failure of the safety systems and operator actions provided to mitigate against the consequences of the fault. The TLRS approach leads to a very fast run time which enables numerous Initiating Events to be included in the model. In order to model these sequences it is first necessary to identify what the requirements are to protect against each of the faults and the levels of protection required, e.g. fire detection, equipment protection or management control.

The study will address each of the Safety Functions appropriate for the facility, e.g. for a chemical plant such considerations are: inventory, Emergency Shutdown (ESD), pressure relief systems, etc., and the success criteria will be based on existing performance analysis. For process plant it may be more appropriate to adopt a checklist/walkdown approach to confirm the mitigating features which exist, e.g. fire detection and suppression systems. This latter approach is generally more appropriate when considering hazards, either internal or natural, and in practice the review of a process will involve a combination of both approaches.

System Dependencies

The Event Trees forming the model will generally only be detailed to a system level, and as such it is important that the interactions between the systems are thoroughly understood. This should include any support requirements. It may also be appropriate to investigate the relative locations of equipment in order that the potential vulnerabilities to environmental effects and hazards can be addressed.

The approach adopted is to use a dependency matrix which identifies all of the support systems required for each of the operating systems to function correctly. It is important that each support system is also identified as an operating system so that any

second or higher order dependencies are identified. Any redundancy in supplying the support services should be identified.

The environmental dependencies are assessed in a similar manner by splitting the plant into separate regions, generally divided by some physical feature, and identifying which regions of the plant each system passes through, or is located in. This is performed for both operating and support systems.

Consequence Categories

To quantify the Event Trees used to model accident scenarios, it is necessary to define a set of consequence categories to which each sequence end state can be assigned. In general the consequence categories will be based on the functional degradation of the plant. The specific categories will depend on the specific facility under investigation, and may relate to safety issues, loss of toxic material, or business interruption and commercial impact.

The number of end states is dependent on many factors, including the specific facility, the level of detail of any transient analysis, and the purpose for which the risk study is being performed. It may be appropriate that only two consequence categories are defined, namely success or failure, however, it is generally found that a number of categories are better since they can be used to reflect the relative seriousness of sequences. In addition, they can assist in distinguishing between availability versus safety issues, and beyond design basis conditions for which some protection exists versus major accidents. For example four consequence categories were used in a TLRS for a nuclear facility, these being:

A. Equipment damage or operational delay. An availability issue, but of very limited hazard.
B. A contained release for which protection exists.
C. Minor release of inventory. A release for which some protection exists.
D. Major release of inventory. A major safety issue.

Event Tree Analysis

The possible accident sequences arising following each of the initiating events are modelled using the standard Event Tree approach of investigating the success and failure of systems provided to operate to protect against the Initiating Event, and assigning a consequence category to each end state. Due to the manner in which the data is assigned to the Top Events (see later), it is necessary that the Top Events are at a system level or, where not possible, at functional sub-system level. It is normal to treat the operator as a system for this purpose.

It is at this stage that the dependency and location matrices are used to ensure that systems are not modelled where they must be considered to have already been made unavailable due to failure of a support system or supply, and that the failure of a necessary support system is represented in a failure of the system.

Figure 2 shows an Event Tree model with Initiating Event A, Protection Factors 1, 2 and 3, and Consequence Categories A-D. The Consequence Categories are assigned once the effect of the failure of Protection Factors 1-3 have been studied and understood.

Setting Up the Model

A TLRS looks at the model under review as a series of systems, which are assigned unreliabilities as follows. The model can easily be adapted to represent an industrial facility or a management plan for a business.

The approach for modelling hazards is slightly different from that for investigating intrinsic plant faults, and it varies further for internal and external hazards.

For internal hazards, such as fire and flood, the possible locations of the hazard are identified and each treated as a separate initiating event. The different locations are defined as those with hazard barriers, or equivalent, separation. It should be noted that where there is significant distance between equipment that may be considered to be acceptably segregated.

For each hazard location, the impact on the plant and the success or failure of mitigating equipment, both detection and suppression, are investigated in a similar manner to that described above for intrinsic plant faults. The consequence categories assigned are generally the same as those used for the intrinsic plant faults.

For natural hazards of sufficiently greater magnitude, it is generally the case that they will result in some impact on the plant requiring it to be shutdown, e.g. a seismic event or extreme wind is generally assumed to result in a loss of off-site electrical supply. The approach to modelling the plant response to such hazards is therefore to identify what consequential Initiating Events could be considered to have occurred, and model these in a similar manner to that described for the intrinsic plant faults, but taking into account any potential impact on the mitigating equipment by the natural hazard. The impact on the plant equipment will be assessed using equipment fragility (probability of failure as a direct consequence of the hazard), either plant specific if available, or based on generic information. Again, the same consequence categories will be used for the sequence end states.

Fault Frequency and Top Event Data

The assigning of data to the Initiating Events follows the traditional approach based on available operational experience data, historical and world data for equivalent plant.

Assigning data to the Top Event is done using judgement and a set of guidelines. The guidelines used will be specific to the plant or facility being modelled, but will ensure that a consistent approach is adopted to the assigning of data. This is important to ensure that the results of the importance studies can be used to identify dominant weaknesses. For each facility there is one set of guidelines for the systems based Top Events and another for the operator based Top Events.

One of the factors on which the rules for the system based Top Events will be based is its function and any redundancy in the system to achieve this, e.g. the number of trains and any spare capacity. It will also be necessary to take account of the separation of any redundant items, system locations, i.e. the potential for the system to be affected by the initiating event or another safety system failure. The diversity between redundant equipment and system may also be represented in the event tree and taken into account.

The control philosophy of the system and the control logic and any associated instrumentation will have an effect on system reliability, for instance the number of signals required, or the majority voting logic may be taken into account.

Other important factors may be the level of maintenance and inspection, the design and manufacturing criteria, safety culture at the plant and the work control procedures, etc.

The rules applied to deriving the operator reliability are more simple and are generally based on a combination of the time available for the action, the indications available and the procedures governing the action. A band of data may be appropriate to allow for modelling of any administrative improvements, e.g. improved housekeeping, procedural development, training, etc.

The structure of the Top level Study is such that the effect of each of these rules and their application can be investigated by performing sensitivity studies on the model. This is discussed further below.

Evaluation of Risks

The purpose of the evaluation phase of the TLRS is to calculate the total predicted frequency of each of the pre-defined consequence categories. EQE use either a proprietary event tree code, or an in-house code which is tailored to provide extensive importance analyses and model manipulation capabilities.

The Outputs from the TLRS

The evaluation of the TLRS gives a numerical indication of the actual risk from each of the identified Initiating Events and the total frequency of any of the consequence categories. Although important and useful, this is by no means the extent of the information available from the TLRS. The importance analyses will give an indication as to the dominant contributors to the different consequence categories either as weaknesses in the protection (Top Events) or the major vulnerabilities of the design (Initiating Event). Top Events can also be grouped together for analysis. This information is important to identify which areas require special attention and should be the subject of loss prevention exercises. This information helps to prioritise improvement activities or can be used to justify that changes in some areas will make little impact upon either the risk or other consequences.

The model is easy to modify and manipulate which enables numerous sensitivity studies to be performed and therefore allows the effect of the data approximations to be investigated and provides some confidence in the results. It also makes it eminently suitable as a decision making tool for assessing the relative benefits of proposed modifications to the plant.

Figure 3 shows one of the outputs of the Event Trees analysis as a bar chart, detailing the frequency of risk for each of the consequence categories A-D.

The Advantages of the TLRS

The main advantage of the TLRS over a full PSA/QRA approach is the time and cost. The timescales enable safety improvements and Risk Management decisions and actions to be taken at an earlier time and therefore enables risk reduction in the short term. The low costs make the TLRS an affordable tool and available to all parties, including the designers, the safety managers, the operators, the regulators/licensers, risk managers, investors, insurers and brokers.

The TLRS does not compromise the requirement for a logical approach in reducing the timescales and as such proves very useful in removing any pre-conceived ideas as to which are the major contributors to the risk. The importance analyses provide great insight into this area.

The ease of changing data and the model facilitates numerous modification options to be investigated, and as such can form an invaluable tool in the execution of Cost Benefit Analysis or option studies. Although the data is derived on a approximate basis, the ease of changing the data also enables investigation into the sensitivity to the data used, and provides some confidence as the acceptability of the approach.

Figure 4 shows the results obtained from a sensitivity study, compared to the original TLRS analysis and the saving that can be made by carrying out specific modifications to the plant or business model..

The TLRS also forms the perfect basis from which a full scale PSA/QRA can be developed if that is the requirement. The TLRS has the advantage that it has the same structure as a PSA/QRA and as such the full PSA/QRA could be developed in a staged manner over a period of time, whilst maintaining a risk model which is available to be used throughout the full PSA/QRA development process.

The TLRS has been used in a comparison with a full approximately million pound PSA/QRA. The difference in the results was small (less than a factor 2) although the TLRS cost less than £50,000 for the equivalent study.

System Failure Probabilities

Empirical evidence suggests that the failure probability of a system, or groups of components, is dependent on a number of factors, i.e.

- *the minimum level of redundancy within the system;*
- the separation/segregation between similar components;
- the Control & Instrumentation logic;
- the maintenance practices followed; and
- the plant safety culture.

Furthermore, the evidence would suggest that the failure probability of a system cannot be reduced below a minimum value which is related to the level of redundancy provided within the system.

Given the above, the TLRS assumes that the unavailability of a system, or other groups of components, can be estimated on the following basis:

Basic System Failure Probability * Degradation Factors.

The basic system failure probability of a system, or a group of components is dependent on a number of factors, i.e.

- Commonality/separation/segregation.

This factor accounts for the affects on the system failure probability of the number of:

a) passive component failures required to fail the system;
b) separate locations of groups of similar components, i.e. the number of location in which failure needs to occur to fail all of the components; and

c) segregated areas of groups of similar components, i.e. the number of segregated areas in which failure needs to occur to fail all of the components.

- Control & Instrumentation logic.

This factor accounts for those aspects of the Control & Instrumentation, etc., that are not modelled explicitly within the TLRS. Factors considered are the minimum number of:

a) Control & Instrumentation sensors, transmission or voting logic failures required to fail the system; or
b) control actions which may prevent the system operating correctly.

- Maintenance practices.

This category addresses the impact of the maintenance practices that are followed, that is whether a regulatory approved maintenance, testing and inspection regime is followed or not.

- Safety Culture.

This category address the impact of the general attitude of the plant staff towards safety and equipment availability.

The appropriate degradation factor is determined by taking into account the safety culture, the minimum number of active component failures required to fail the system. It should be noted that, although where more than one aspect appears to apply, only the highest single degradation factor is applied for each of the above four categories.

Operator Actions

Following several faults, or fault sequences, the operator is required to perform certain actions in order to either maintain the continued operation of a safety system, or to prevent further deterioration. For a satisfactory assessment of the risk of operation, the likelihood that the operator fails to carry out the claimed actions must be estimated.

In the TLRS, the probability that the operator fails to perform a claimed action in good time is estimated depending on the time taken to take action. As an example of a particular application the categories can be split into:

Operator action within an hour. *If* it is necessary to initiate a safety system, or stop the fault from the control room or at a point local to plant; or to take action to prevent further deterioration;

Operator action in greater than one hour. In order to re-establish equipment starting procedures, or system which can be manually commissioned.

Operator action after 8 hours. Following common practice, an operator reliability of a further order of magnitude is claimed due the change of shift.

Operator action after 24 hours. Another order of magnitude is claimed due the multiple change in shifts and the availability of other advisory personnel.

It is assumed that all the claimed actions are effectively backed by the appropriate procedures. Furthermore, it is assumed that these procedures are reinforced by appropriate training.

TLRS IN SUMMARY

The benefits in time and cost when carrying out a TLRS are particularly of use in the identification of dominant weaknesses within the plant or business model, where the consequences may be significant either in terms of safety to workers, or loss of market share and business interruption. Follow-up sensitivity analysis can then be carried out to look at the ways in which the risk could be realistically reduced by modifying specific areas of weakness within the plant or model. This would enable the expenditure to be directed towards areas of the plant where the effect on risk reduction would be the most effective.

Figure 1: Construction of TLRS

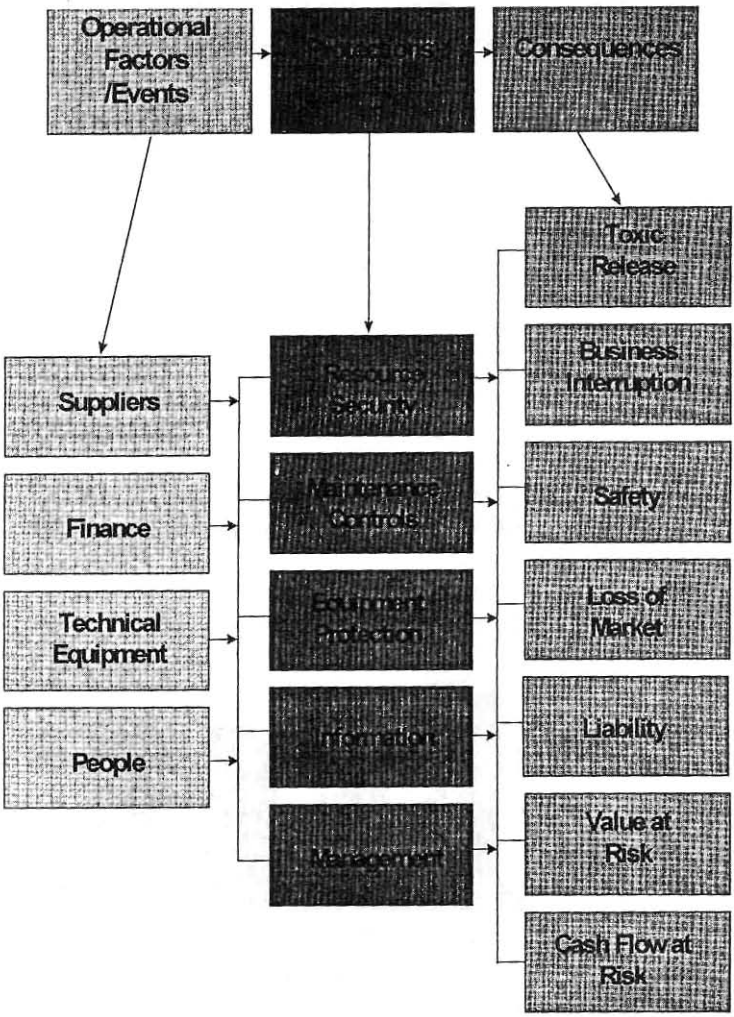

Figure 2: Event Tree Layout

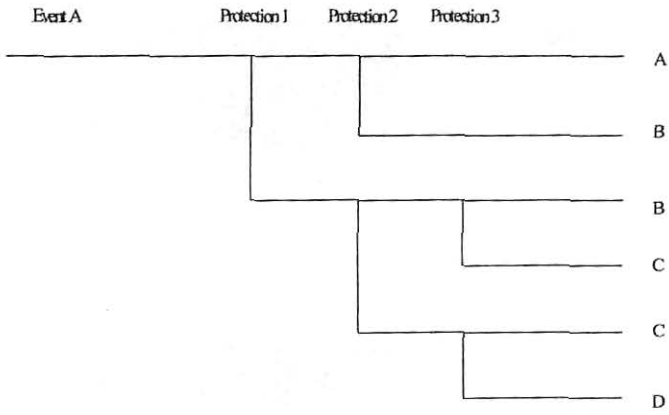

Figure 3: Quantification of Risk for Consequence Categories A-D

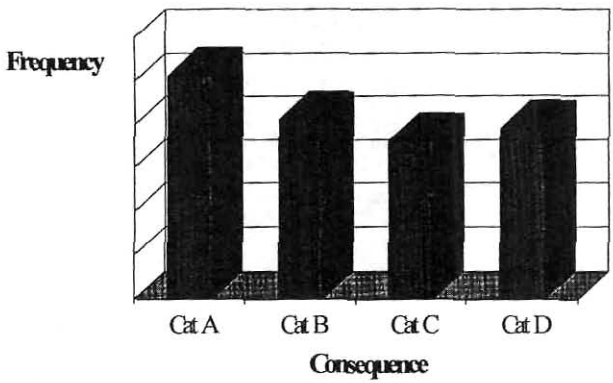

Figure 4: Cost of Improvement v Risk Cost Saving