THE DEVELOPMENT OF SITE-SPECIFIC FAILURE RATES FOR USE IN RISK ASSESSMENTS OF MAJOR HAZARD SITES

Martin Anderson
Health and Safety Laboratory, Broad Lane, Sheffield, S3 7HQ[1]
John Gould
Health and Safety Executive, MHAU, Bootle, L20 3RA

The paper describes a research project in progress at the Health and Safety Laboratory (HSL) for the Major Hazards Assessment Unit (MHAU) of the UK Health and Safety Executive. It summarises the development of a quantified fault tree analysis of a guillotine failure during the transfer of chlorine from bulk storage to a road tanker, at a hypothetical 'best practice' reference site. The research aims to produce a methodology to develop site-specific failure rates for use in a quantified risk assessment at major hazard sites.

Keywords: Major hazard, risk assessment, tanker transfer, failure rates.

INTRODUCTION

RISKAT and Generic Data

MHAU provides advice to local authorities on land-planning proposals for the siting of new major hazard plant and for the development of housing, etc., in the vicinity of existing major hazard installations. HSL and MHAU have collaborated over the past 10 years in the development of a range of computerised Quantified Risk Assessment (QRA) tools, RISKAT[2], to inform such land-use planning advice.

The RISKAT suite of programs draw heavily on generic failure rate data. In this context, generic data is derived mainly from historical and some theoretical data. The values contain elements of engineering judgement and caution. A single or 'generic' value is taken to be representative of this data. These generic failure rates are incorporated into the numerical estimation of individual risks from a particular installation. Generic failure rates, being derived from historical and theoretical data, include all causes of failure and should thus reflect 'average' conditions or standards.

No Such Thing As An 'Average' Plant

Even identical plants can, however, be operated, maintained and managed to varying standards. Some plants, therefore, may warrant a failure rate different from the generic value to reflect site specific conditions. These differences will invariably have an impact on the risk

1 HSL is an agency of the Health and Safety Executive
2 See Hurst et al., (1) for details of RISKAT

level. Concern has thus been raised about the use of generic failure rates for differing plants and standards, in terms of construction, operation, maintenance and management systems, for example.

Recent research has suggested that standards at plants may vary by an order of magnitude either side of this average value. For example, it is described in Hurst et al. (2) that failure rate data is lognormally distributed so that generic failure rates correspond to a plant of 'average' safety performance. The suggestion that failure data may vary by about an order of magnitude either side of this generic value to reflect above- and below-average safety performance was based on data collected on pipework failures and also information collected under RIDDOR[3] which showed a ±1 order of variance in loss of containment dangerous occurrences reported by companies to the HSE.

This proposal is supported elsewhere. Taylor (4) found that incident rates for similar equipment could vary by a factor of over 100 depending upon maintenance and inspection practices. Joschek (quoted in Taylor, 4) reported that accident rates for one international company varied by a factor of 60 across it sites worldwide. Additionally, Technica assessors using the MANAGER technique[4] noted a range of three orders of magnitude for accident frequency between inherently good plants and unsafe plants. This equates to a possible maximum difference between two identical plants of a factor of 1000.

Tanker Transfer Operations

Transfer of hazardous materials is an obvious area where variations in plant and operating procedures could make a marked difference to the failure rate, which in turn have a significant effect on the calculated risk levels. Tanker transfer operations are a particular concern as it has been determined that they form a significant contribution to the risk of a release (for example, see Purdy 5).

The general consensus is that these operations offer the greatest potential for release because they involve a temporary connection between road tankers and storage vessels, which inherently carries more risk. Every day hundreds of these transfer operations take place throughout the UK. Materials that may be transferred include flammables (e.g. LPG, oxygen), toxics (e.g. ammonia, chlorine) and acids (e.g. hydrochloric, sulphuric).

RESEARCH AIMS

The objectives of this project are to identify and assess the key factors that contribute to the generic failure rate for tanker transfers with the aim of developing a site-specific methodology for the assessment of this particular operation to include a consideration of engineering reliability, human factors and organisational issues.

Using information available from a particular site in this manner will produce a site-specific failure rate which may vary either side of the generic value. The use of such a site-specific failure rate has the potential to improve the site-specificity and transparency of a

3 Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (3)

4 Management-safey-systems-assessment Guidelines in the Evaluation of Risk (Pitblado et al., 6)

QRA. In addition, an understanding of the major contributors to the generic failure rate enables risk reduction strategies to be more efficient, in that resources can be targeted at the principal contributing factors.

It is also intended that the research will produce a methodology as to how site factors may be included in the assessment of other operations besides tanker transfers.

LITERATURE REVIEW

The project commenced with a literature search to identify relevant references. These were then reviewed along with the results of a search of tanker transfer incidents. Several important themes were drawn out of this review, as follows:

- It was confirmed that transfer operations form a significant contribution to the overall risk from an installation (one reference quotes 95% at distances of up to 500 metres).
- Failure incident causes were found to be described by a small group of direct and underlying causal factors and their percentage contributions can be calculated from incident databases.
- The frequency of failure incidents can vary by at least an order of magnitude either side of a generic or 'average' value.
- The role of human factors during transfer operations is considered paramount.
- Numerous improvements to transfer operations have been identified that have the potential to significantly reduce the risk of a loss of containment; the vast majority of failures being theoretically prevented by management systems that control underlying causes.

TASK ANALYSIS

Several visits were made to major hazard installations in order to observe tanker transfer operations, both from storage to road tanker and vice-versa. During these visits, operators and managers were interviewed; relevant documentation gathered and a video made of the transfer. It became apparent that the variation between the transfer of different substances meant that they could not all be accommodated in a single model within the project timescale. It was therefore decided that only the transfer of chlorine (a highly toxic liquid) would be modelled at this stage.

From the information gathered on the site visits, two reference sites were described and a Hierarchical Task Analysis (HTA) provided for the transfer procedure. HTA is a technique which describes the operations necessary in order to achieve a particular system goal. Each operation is further broken down into sub-operations until redescription is unnecessary, according to the requirements of the analysis. Plans are also described, which state exactly when operations and sub-operations should be performed to achieve the system goal or sub-goal[5].

Briefly, upon arrival of a tanker on site, the transfer operation involves a series of four main tasks:

[5] See Kirwan and Ainsworth (7) for a detailed description of Hierarchical Task Analysis

· Pre-transfer checks. This involves checking documents, positioning the tanker in the filling bay and securing the vehicle by means of barriers and/or interlocks on brakes. The volume of liquid in both the tanker and the storage tank are checked to ensure that overfilling cannot occur. Valves on both vessels are checked for leaks.

· Connection of hoses/loading arms. This stage involves connecting transfer hoses to the tanker and to the site according to a predetermined procedure. The connections are then vented and tested for leaks. Visual/audible weight alarms may then be set and checked.

· Transfer of liquid/vapour from tanker to site (or vice versa). The valves are then opened to begin the transfer and vessel weights are checked to ensure that the process is progressing satisfactorily. The operator checks the receiving vessel periodically. When the required amount has been transferred the valves are closed (again, in a specific order).

· Uncoupling of the hoses/loading arms. The hoses can then be uncoupled and stored according to procedure. The valves are then checked for leaks and the tanker dome secured. The tanker weight will then be rechecked and documentation completed.

Each of these tasks can be further broken down into their components - note that the transfer process varies in detail according to the substance to be transferred. The complete operation takes about 2 hours and at a producing site there may be several loading operations every day.

HUMAN ERROR ANALYSIS

The above task analysis provided a thorough understanding of the operation and formed the basis of a Human Error Analysis. The technique employed, decompositional task analysis, identifies potential human errors at each stage in the process, the possible consequences of each error and any factors which may influence performance on this task (referred to as 'Performance Shaping Factors' {PSFs}), such as training, experience and time pressure. Examples of human errors identified included:

· inadequate coupling of the transfer hoses
· omission of the pressure drop test before commencing transfer
· driving away with the hoses attached
· failure to wear personal protective equipment.

Various ergonomic problems were also identified in the human error analysis such as displays and controls being difficult to read, or hard to reach. The likelihood of these human errors were then estimated using Human Reliability Assessment (HRA[6]), to be fed into the quantified fault tree analysis.

[6] See Kirwan (8) for details of Human Reliability Assessment

FAILURE EVENTS

Historical experience demonstrates that guillotine failure of the hose and coupling, leading to a loss of containment incident, may occur due to one of three events:

- driver pullaway
- hose burst
- coupling failure

The failure rate utilised by MHAU in their risk assessment calculations is composed of these three failure events. These events have also been used to structure previous risk assessments of tanker transfer operations; for example, the research reported by Munley and Bardsley (9). Reeves and Prescott (10) also considered these failure events for the various stages of a chlorine transfer operation in their risk assessment of this process.

FAULT TREE ANALYSIS

In order to determine how a loss of containment of chlorine could occur during the transfer and to quantify the likelihood of this undesirable event, a fault tree has been developed. The analysis of failure events described above forms the top structure of the fault tree and each of these three branches of the tree have been further described to the level of base events[7]. Examination of the tree shows that it incorporates both hardware/engineering and human failures.

This fault tree is based upon a reference system designed to incorporate features from the best sites that were visited during the initial stages of the project and from a review of industry 'best practice'. It contains several high-integrity safety systems such as interlocked barriers, instrument air-fed actuated valves on the tanker, interlocks to tanker brakes and an emergency shutdown system. This hypothetical site can thus be seen as 'above average' in terms of safety management.

Description of Fault Trees

Pullaway. This section of the fault tree can be divided into two paths: where the tanker moves unassisted and where the tanker is moved intentionally. In both cases it is necessary for several safety systems to fail or be defeated, such as interlocked barriers/doors and brake interlocks. For the tanker to move unassisted it is also necessary for the transfer to take place on sloped or uneven ground.

At the reference site several safety systems must fail or be defeated for a guillotine failure to occur due to a pullaway incident. Actuated valves on the tanker are activated by instrument air from the site and will close isolating the tanker if this line is separated during the pullaway incident. (Thus this line should thus be as short as possible). Should the tanker be moved, a movement detection system will be activated and automatically isolate the tanker.

---

7 See Kirwan and Ainsworth (7) for details of the Fault Tree Analysis technique

Historical experience has led to an intentional pullaway event being considered to be the major contributor to loss of containment incidents. However, over recent years both transfer facility and tanker operators have implemented hardware and human factors improvements (such as those modelled on the fault tree) that have reduced the contribution of this type of event to such major hazard incidents.

Hose Burst. This sub-tree can also be divided logically into two main pathways: where the hose fails catastrophically (that is, 'break before leak') and where the hose fails due to the escalation of a pin-hole leak ('leak before break').

Where the hose fails catastrophically, this may be due to either a defect existing prior to the transfer operation or the hose developing a defect during the transfer, for example where a normal hose is used under abnormal operating conditions (such as overpressure).

Where the hose fails due to escalation of a pin-hole leak, it must escalate significantly in order to produce guillotine failure of the hose. There is opportunity for this leak to be detected by the pressure drop or leak tests. However, where a leak develops during the actual transfer of chlorine (that is, after the pressure drop and leak tests have been completed) detection of the leak will either be through smell (assuming that an operator is present) or the chlorine detectors.

Coupling / Connection Failure. Three sub-trees have been modelled for this event. First of all, if the hoses are inadequately connected and the transfer commenced, the inadequate connection may escalate to a total coupling failure during the transfer of chlorine, resulting in a full-bore release. For this to occur, the operator must fail to detect the inadequate connection; through failure of the pressure drop and leak tests and inspection of the coupling, or fail to act upon an inadequate connection. It is recognised that an inadequate connection may occur due to either mechanical failure (for example, corrosion) or operator error (failure to connect the hoses correctly). The likelihood of the inadequate connection escalating to guillotine failure will be dependent upon the extent of the inadequate connection.

Secondly, a coupling failure may occur should the operator disconnect the transfer hoses whilst the chlorine is still being transferred. This could occur where the hoses are disconnected given that the isolating valves are open or passing (either the operator fails to close the manual and actuated valves, or they fail to close on demand/fail to danger). It is unlikely (although possible) that the operator would attempt to disconnect the hose whilst the transfer is still in progress.

The third cut-set leading to coupling failure is where the operator commences chlorine transfer given that the filling hose is not connected. This event involves failure by the operator to detect that the hose is not connected, through failure of the pressure drop and leak tests and visual inspection of the coupling; prior to opening the manual and actuated filling valves.

Base Event Quantification

The base events for the fault tree are currently being quantified using historical failure data, human reliability analysis and engineering judgement. Where appropriate, failure data have been adopted from previous research concerning tanker transfer operations. The values assigned to the base events are entered into the Data Editor facility of Fault Tree Manager™ (11) and used to quantify the tree.

Minimal Cut Sets

The Minimal Cut Set (MCS) Editor of Fault Tree Manager™ will then be used to determine the MCSs for the fault tree, giving a true Boolean reduced tree. These MCSs are the smallest combinations of equipment and human failures that are sufficient to cause a guillotine release. Following production of the MCSs, the Analysis Editor is used to calculate the probability of the Top Event; 'Guillotine Failure of the Hose/Coupling per Connection'.

It is expected that this failure rate will be lower (i.e. less likely) than the value currently being used in RISKAT calculations due to the numerous safety systems included in the reference site (and thus modelled in the fault tree).

Intermediate Events

The failure rates of the three main intermediate events (pullaway, hose burst, coupling failure) will then be calculated and the percentage contributions of these intermediate events to the overall failure rate be computed and compared with, for example, the research by Tinline and Kierans (12). The authors extracted 162 hose and loading arm incidents from the MHIDAS[8] and MARCODE[9] databases and examined them with regard to the direct and underlying causes of release, ignition and isolation failures. A three-dimensional classification scheme described in Bellamy et al. (13) was employed to analyse the incident data.

The intermediate events that contribute most significantly to the top event can then be assessed further to determine the major components of these events. The base event sensitivity can then be calculated and the most important will most likely contribute to the intermediate events deemed important through the above analysis.

Human Factor Contributions versus Hardware / Engineering Contributions

From the above analyses, it can be postulated that the transfer operator plays an important role in preventing a guillotine failure of the hose/coupling connection. For example, one of the main ways in which a failure can be detected, or prevented from escalating further, is through the pressure drop and leak tests. If these tests are omitted or carried out ineffectively by the operator, (and there is often little independent checking of these actions) then a guillotine failure is much more likely to occur.

---

8 Major Hazard Incident Data Service, SRD

9 Database of Investigated Incidents (originally Marches Code), HSE

Some of the base events can clearly be labelled as human factors failures (such as 'Operator knowingly using a defective hose') and others may be seen as engineering failures (for example, 'Barrier down but unable to halt tanker'). However, many of the events which at one level appear to be hardware failures, may involve a human factors contribution at the level of underlying causes. For example, base event 'Barrier is raised, interlock has failed or been defeated'. It is possible that the interlock fails due to a lack of maintenance - which can be considered to be a human failure at the organisational level.

Thus it is difficult to estimate the human factors contribution to the fault tree, although it can be judged to be significant. Following the quantified analysis it will be possible to estimate how much of the base event sensitivity to the overall failure rate is composed of human factor issues, including management / organisational failures. This can then be compared to the research by Tinline and Kierans (12) referred to above, who reported that 35.5% of hose and coupling failures could be attributed to an human factors underlying cause.

SAFETY IMPROVEMENT SENSITIVITY ANALYSIS

Contribution of Various Safety Systems

The reference site has been purposely designed to include several safety systems, with the intention that they can be assigned failure values of unity and thus removed from the system to compute their contribution to the overall failure rate. (Thus enabling the failure rate of a site that varies from the reference system in the absence of such safety systems to be computed). Through the modification of the data utilised in the analysis, the following six scenarios will be produced and modelled using the fault tree:

Scenario 1. Absence of interlocked barriers and doors
Scenario 2. Pressure drop and leak tests not performed prior to each transfer
Scenario 3. Absence of Emergency Shutdown System
Scenario 4. No interlock to tanker brakes
Scenario 5. Inadequate hose replacement regime
Scenario 6. Visual inspection of hoses not performed prior to each transfer

The results of this analysis can subsequently be compared with the failure rate obtained in the original analysis. The scenarios can be prioritised in terms of their effect on the overall guillotine failure rate and thus the safety improvements relating to the particular scenarios can be placed in order of importance. The effect of these six scenarios on the three intermediate events described above can also be assessed.

Analysis of a 'Below Average' Site

A further scenario will be examined in an attempt to model a site that it significantly below-average in terms of safety standards. In order to achieve this, scenarios 1 to 4 above are combined and the failure data incorporated in the original analysis has been modified in order to reflect the absence of these various safety systems, so that the effect on the overall failure rate can be assessed.

CONCLUSIONS

This paper has described the development of a quantified fault tree analysis of a full bore loss of containment during the transfer of chlorine from storage to road tanker at a reference site. The overall failure rate is expected to be lower than that currently used in RISKAT calculations due to the numerous safety improvements included in the analysis reference system. The failure rate that will be obtained for this research is for a hypothetical 'above average' site, whereas the failure rate used by MHAU reflects 'average' conditions and standards.

Preliminary examination of the fault tree suggests that a failure of the hose/coupling leading to a smaller-than-guillotine release is much more likely and should be considered in a site-specific assessment. Several events can be seen to lead to small leaks; however, they are considered as unlikely to escalate further into guillotine failures. These smaller leaks require more detailed investigation; however, this is out of the scope of the current project.

The paper also describes how a subsequent sensitivity analysis of this fault tree will identify the main contributors to the failure rate, such that site-specific information may be used, where appropriate, to produce a site-specific failure rate for the operation. In addition, by producing a failure rate for a 'very poor' site, to be compared with the original reference site (deemed to be 'very good'), a range of failure rates will be produced.

The research thus outlines a possible method by which site-specific factors may begin to be modelled in the QRA of a tanker transfer facility and in other risk assessments at major hazard installations.

REFERENCES

1. Hurst, N. W., Nussey, C. and Pape, R.P. (1989). Development and application of a risk assessment tool (RISKAT) in the Health and Safety Executive. Chem. Eng. Res. Des., 67, 362-372.

2. Hurst, N. W., Davies, J. K. W., Hankin, R. and Simpson, G. (1994). Failure rates for pipework - underlying causes. Paper presented at Valve and Pipeline Reliability Seminar, University of Manchester.

3. HSE (1986). Guide to the Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1985, HS (R) 23, HMSO.

4. Taylor, J. R. (1994). Risk analysis for plant, pipelines and transport. London: E. and F. N. Spon.

5. Purdy, G. (1988). 'A practical application of quantified risk analysis' in B. A. Sayers (ed) Human factors and decision making: Their influence on safety and reliability. London: Elsevier Applied Science.

6. Pitblado, R. M., Williams, J. C. and Slater, P. H. (1990). Plant/Opns Prog., 9, 169.

7. Kirwan, B. and Ainsworth, L. K. (Eds.). (1992). Guide to task analysis. London: Taylor and Francis.

8. Kirwan, B. (1994). A guide to practical human reliability assessment. London: Taylor and Francis.

9. Munley, G. A. and Bardsley, A. S. (1993). A human factors analysis of LPG transfer tasks. SRD/HSE R599. SRD, Wigshaw Lane, Culcheth, Cheshire, WA3 4NE.

10. Reeves, A. B. and Prescott, B. L. (1989). Risk assessment of the chlorine road tanker loading operations at Hays Chemicals Ltd, Sandbach, Cheshire. HSE/SRD/080/0001/89. Confidential Report, UKAEA.

11. AEA Technology, U.K. (1994). Fault Tree Manager Manual.

12. Tinline, G. and Kierans, L. (1994). Process safety management audit manual. Four Elements Ltd, Greencoat House, Francis Street, London. SW1P 1DH.

13. Bellamy, L. J., Geyer, T. A. W., Astley, J. A. (1989). Evaluation of the human contribution to pipework and in-line equipment failure frequencies. Contract Research Report No 15/1989, Health and Safety Executive, Sheffield, UK.