The Buncefield Enquiry Findings and Costain's Approach to Best Practice in Integrity Level Assessment

Dr Jonathan Mark Bunch ***MEng CEng MIChemE***
Design Safety Consultant

Robert Beresford ***BEng CEng MIChemE***
Principal Process Engineer

Costain Energy and Process, Costain House, Styal Road, Manchester, M22 5WN. United Kingdom

Abstract

Since the Buncefield incident of 2005, when a large fire followed the largest peacetime explosion on British soil since the Flixborough Explosion, as the result of a gasoline tank overfill, the regulator in the UK requires that a fit and appropriate risk assessment of Safety Instrumented Systems is performed. The explosion caused injury to some forty people, destroyed many neighbouring buildings, both businesses and homes as well as much of the site, which has lost revenue ever since.

In 2009 a nationwide review of Integrity Level assessments using Layers of Protection Analysis (LoPA) was undertaken by the Enquiry, which found many errors, shortcomings and omissions. The issue of Integrity Level assessment has therefore received increased regulator interest and many studies at other facilities have had to be repeated.

This paper describes Costain's approach to achieving best-practice for a client in the assessment of existing plant. An approach is described whereby an initial assessment is completed using Risk Graph as a screening exercise, followed by the re-evaluation of higher SIL, using LoPA. Advantages are that effort is reduced, the higher risks are addressed in appropriate detail and the safety of the resulting design is robust. The approach reduces the effort required during the meeting, increases the overall safety of the facility and provides a better estimate of the costs, which, in turn, provides an advantage to the client company. In the case of new-build plant the approach achieves the aims of the regulator, other interested parties, such as Local and National Government and the local community, and provides greatest benefit at lowest cost to the operating company. The approach described is valid for hydrocarbon facilities in the GCC area and the further Middle East and will help in the assurance of overall design safety for both existing and future facilities.

Abbreviations

AIL	Asset Integrity Level
ATG	Automatic Tank Gauging
BPA	British Pipeline Agency
BS	British Standards
CASS	Conformity Assessment of Safety related Systems
CCTV	Closed Circuit Television
COMAH	Control Of Major Accident Hazards
EIL	Environmental Integrity Level
HAZID	Hazard Identification Study
HAZOP	Hazard and Operability Study
HOSL	Hertfordshire Oil Storage Ltd
HSE	Health and Safety Executive
HSL	Health and Safety Laboratory
IChemE	Institution of Chemical Engineers
IEC	International Electrotechnical Commission
IL	Integrity Level
LoPA	Layers of Protection Analysis
PFD	Probability of Failure on Demand
QRA	Quantitative Risk Assessment
SCADA	Supervisory Control And Data Acquisition
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System

The Buncefield Enquiry Findings and Costain's Approach to Best Practice in Integrity Level Assessment

Introduction

Before the devastating explosion and subsequent fire, the Buncefield Terminal was the fifth largest fuel depot in the UK, receiving fuel from Humberside in the north-east and Merseyside in the north west and supplying fuel to both Heathrow and Gatwick International Airports as well as to road tankers. It had a capacity of 60 million gallons and handled up to 2.37 million tonnes of oil products every year. It is owned by Hertfordshire Oil Storage Ltd (HOSL).

The explosion and fire destroyed over a quarter of the site.

The Buncefield Incident(1)

Figure 1 – Aerial view of the smoke dispersion from the Buncefield fire

Overview of Buncefield Operations

Fuel products were supplied by three discrete pipeline systems:

- 10" pipeline (FinaLine) from Lindsay Oil Refinery on Humberside, which terminates in the HOSL West site;
- 10" pipeline from Merseyside via Blisworth, (M/B North), which terminates in the BPA's Cherry Tree Farm site;
- 14" pipeline from Thameside via a tee junction close to the site – the Hemel Tee (T/K South), which terminates in the BPA main site.

On arrival at site, the batches of product were diverted into dedicated tanks for each product type.

The fuel stored in the tanks at Buncefield was then either transported off site in road tankers for distribution, or in the case of the majority of aviation fuel, via two BPA-operated 6" pipelines to London airports.

Timeline of Events

10 December 2005 Around 19.00, Tank 912 in bund A at the (HOSL) West site started receiving unleaded motor fuel from the T/K South pipeline, pumping at about 550 m^3/hour.

11 December 2005 At midnight, a stock check of products was carried out; no abnormalities were reported. From approximately 03.00, the level gauge for Tank 912 recorded an unchanged reading. However, filling of Tank 912 continued at a rate of around 550 m^3/hour. Calculations show that at around 05.20, Tank 912 would have been completely full and starting to overflow. The protection system, which should have automatically closed valves to prevent further filling, did not operate.

From 05.20 onwards, continued pumping caused fuel to cascade down the side of the tank and through the air, leading to the rapid formation of a rich fuel/air mixture, or vapour cloud, that collected in bund A.

At 05.38, a vapour cloud, from escaped fuel, started to flow out of the north-west corner of bund A towards the west. The vapour cloud was about 1 m deep.

At 05.46, the vapour cloud had thickened to about 2 m deep and was flowing out of bund A in all directions.

Between 05.50 and 06.00, the pumping rate down the T/K South pipeline to Tank 912 gradually rose to around 890 m^3/hour. By 05.50, the vapour cloud had started flowing off site following the ground topography.

At 06.01, the first explosion occurred, followed by further explosions and a large fire that engulfed over 20 large storage tanks. The main explosion event was centred on the car parks between the HOSL West site and the Fuji and Northgate buildings. The exact ignition points are not certain, but are likely to have been a generator house in the Northgate car park and the pump house on the HOSL West site.

Loss of Fuel Containment

The Escape of Fuel

The investigation concentrated on finding out how the site was operating in the crucial period leading up to the explosion and what was happening in the vicinity of bund A.

At the time of the incident, approximately 06.00 on 11 December 2005, the pipelines were transporting the following products into the HOSL West site:

- FinaLine was delivering unleaded petrol at a flow rate of approximately 220 m^3/hour into Tank 915 at HOSL West (also in bund A);
- M/B North line was delivering diesel oil at a flow rate of approximately 400 m^3/hour into Tank 908 in bund D;
- T/K South line was delivering unleaded petrol at a flow rate of approximately 890 m^3/hour into Tank 912.

The initial investigation stated with some confidence the initial loss of containment occurred from Tank 912 in bund A, and that this was most likely due to an overfill of unleaded petrol.

Instrumentation and Control Systems

Tank 912 was fitted with instrumentation that measured and monitored the level and temperature of the liquid in the tank; a servo level gauge measured the liquid level and a temperature sensor measured the temperature. The instruments were connected to an automatic tank gauging (ATG) system in common with all the other tanks on the site. Tank levels were normally controlled from a control room using the ATG system.

The ATG system enabled the operator to monitor tank levels, temperatures and valve positions, and to initiate the remote operation of valves all from the control room on HSOL West site. The ATG system was also able to trend data and had an event logging system, integrated with the alarm system. The ATG contained a large database which recorded levels, temperatures, alarms, valve positions, and other related information indexed against times and dates for a user-configurable period, which can be several months. The records from this database provided valuable information for the investigation.

The tank also had an independent safety switch, which provided the operator with a visual and audible alarm in the control room when the level of liquid in the tank reached its specified maximum level (the 'ultimate' high level), in the form of a flashing lamp (one for each tank) and an audible buzzer. This alarm also initiated a trip function to close valves on relevant incoming pipelines. The ultimate high level safety switch on the tank sensed when the liquid reached its specified maximum level, should all other alarms and controls fail to prevent this. In addition, the ultimate high level safety switch alarm signal from any overflowing tank in HOSL West would be sent to computer control and instrumentation relating to both the FinaLine and BPA pipelines.

When the BPA site received an alarm/trip signal from the HOSL West site, the BPA computer control system was configured to close the relevant pipeline manifold valve feeding in product to the tank(s) on the HOSL West site. BPA also had a high-level supervisory control and data acquisition (SCADA) system, which had the facility for alarm and event logging both locally at Buncefield and remotely at the BPA control centre at Kingsbury, Warwickshire.

An override keyswitch in the HOSL West control room could be used to inhibit the alarm/trip signal to BPA during testing of the ultimate high level safety switches. Putting the keyswitch in the override position would illuminate a red lamp on the annunciator panel.

Evidence from Control Systems Records

Examination of the records for Tank 912 from the ATG system suggests an anomaly. Shortly after 03.00 on 11 December, the ATG system indicated that the level remained static at about two thirds full. This was below the level at which the ATG system would trigger alarms.

However, the printouts from the BPA SCADA systems indicate that the T/K South line was delivering a batch of 8400 m^3 of unleaded petrol, starting around 19.00 the previous evening. The delivery was being split between Tank 912 at the HOSL West site and BPA's site at Kingsbury, giving a flow rate to Tank 912 of around 550 m^3/hour. These SCADA printouts further indicate that approximately seven minutes before the incident, the Kingsbury line was closed, leading to a sharp increase in the flow rate to Tank 912 to around 890 m^3/hour.

Examination of the valve positions shown by the ATG database confirm that the inlet valve to Tank 912, which was connected to the BPA petrol manifold, was open at the time of the incident. Based on this evidence, it is concluded that Tank 912 was still filling after 03.00.

Temperature records also provide evidence that the inflowing fuel was warmer than the tank contents. Records for Tank 912 show the tank temperature continuing to rise after 03.00, supporting the above conclusion that the product was still feeding into the tank from the pipeline.

The evidence to date is consistent with continued filling of Tank 912 after 03.00, despite the ATG system showing a static level reading. On the basis of calculations, Tank 912 would have been completely full at approximately 05.20, overflowing thereafter. This timing is entirely consistent with CCTV evidence and eyewitness accounts that report a dense vapour cloud at various times between 05.38 and 06.00. The overflow of unleaded petrol would therefore have been in the order of 300 tonnes by 06.00.

Alarm Systems Testing

Simulation of the ultimate high level tank alarms (from the relevant electrical substation on site) and tests on the annunciator panel and the link to BPA prove that they worked normally. Tests on the override switch found that it had no effect on the audible and visual alarms from the annunciator, but it did, when switched to override, inhibit the alarm/trip signals being sent to BPA.

Information from the BPA SCADA system indicates that no ultimate high level alarm was received from HOSL West, but it has not been possible to test the ultimate high level safety switch or intervening wiring between Tank 912 and the substation, as they have been damaged in the fire.

Figure 2 – View of the smoke plume from the side of the M1 motorway

Costs to the Operator as a Result of the Incident

The Buncefield site was covered by the COMAH (Control of Major Accident Hazards) Regulations, which are enforced by the Health and Safety Executive in the UK. Charges were brought under this and other Health, Safety and Environmental legislation resulting in guilty verdicts and subsequent fines totalling £6 million.

A number of claims for damages are now proceeding. The value of these supplementary claims is estimated at between £700 million and £1 billion.

The operating companies faced a substantial loss of revenue following the incident. The scale of these losses is difficult to estimate but Kevin Myers, deputy chief executive of the Health and Safety Executive has said, in an interview for The Daily Telegraph, "The fines pale into insignificance in relation to the billion pounds worth of estimated economic loss and the damage to the reputation of the companies."

The Buncefield Enquiry

The UK Government set up an enquiry into the incident, chaired by Lord Newton of Braintree. The remit of the enquiry went beyond a simple investigation of the causes of the incident and was required; in particular:

- To identify and transmit without delay to duty holders and other appropriate recipients any information requiring immediate action to further safety and/or environmental protection in relation to storage and distribution of hydrocarbon fuels
- To make recommendations for future action to ensure the effective management and regulation of major accident risk at COMAH sites. This should include consideration of offsite as well as onsite risks and consider prevention of incidents, preparations for response to incidents, and mitigation of their effects
- To ensure that the relevant notifications are made to the European Commission.

The Buncefield Enquiry Recommendations

The main five areas in the Design and Operation Recommendations Report are:

- The need for systematic assessment of the level of inherent safety required at sites;
- The need for high integrity systems to protect against escape of fuel;
- Preventing escalation of loss of primary containment incidents and preventing harmful substances from causing a major accident to the environment;
- Operating major hazard sites with high reliability organisations; and
- Improving culture and leadership to deliver high safety performance. The broad aim being '...to catalyse improvements in the fuel storage sector so that it is continually alert to the major hazard potential of its operations.'(1)

Review of Integrity Level Assessments from Bulk Hydrocarbon Storage Sites

With Integrity Level Assessment, and the associated performance assurance, given such weight by the enquiry, the Health and Safety Laboratory (HSL) was asked by the Health and Safety Executive to conduct a review of a sample of LoPA assessments to determine the quality, accuracy, implementation, areas of best practice and the effectiveness of the technique(2). LoPA is one of several techniques for establishing Integrity Levels of Safety Instrumented Functions and is briefly described later.

The report findings are summarised:

1. The quality of data sources varied widely; data was inappropriate and contained uncertainties
2. The degree of rigour applied to the LoPA study varied widely
3. Inconsistencies in the handling of dependencies between initiating events and protection layers
4. Initiating events sometimes broken down into components and the assumption that each component was independent, which may not be the case
5. Human factors were a dominant factor in a number of initiating event frequencies and conditional modifier error probabilities
6. Insufficient use of sensitivity studies

7. Miscellaneous issues, including poor logical arguments and the omission of supporting information

Integrity Level Assessment Review Recommendations

The recommendations were:

1. To improve the knowledge and training of those carrying out LoPA Studies
2. To develop better procedures and guidance for the study, including such matters as sensitivity analysis and standards of documentation and support information to be included
3. To improve the quality of data used in LoPA studies.

Integrity Level Assessment

Integrity Level Assessment is a form of risk assessment for which the requirements, definitions and applications of a Safety Instrumented System (SIS) are effectively covered by the IEC standard 61508 (3). The application of IEC 61508 to the process industries, including oil and gas, is covered in IEC 61511, parts 1(4), 2(5) and 3 (6).

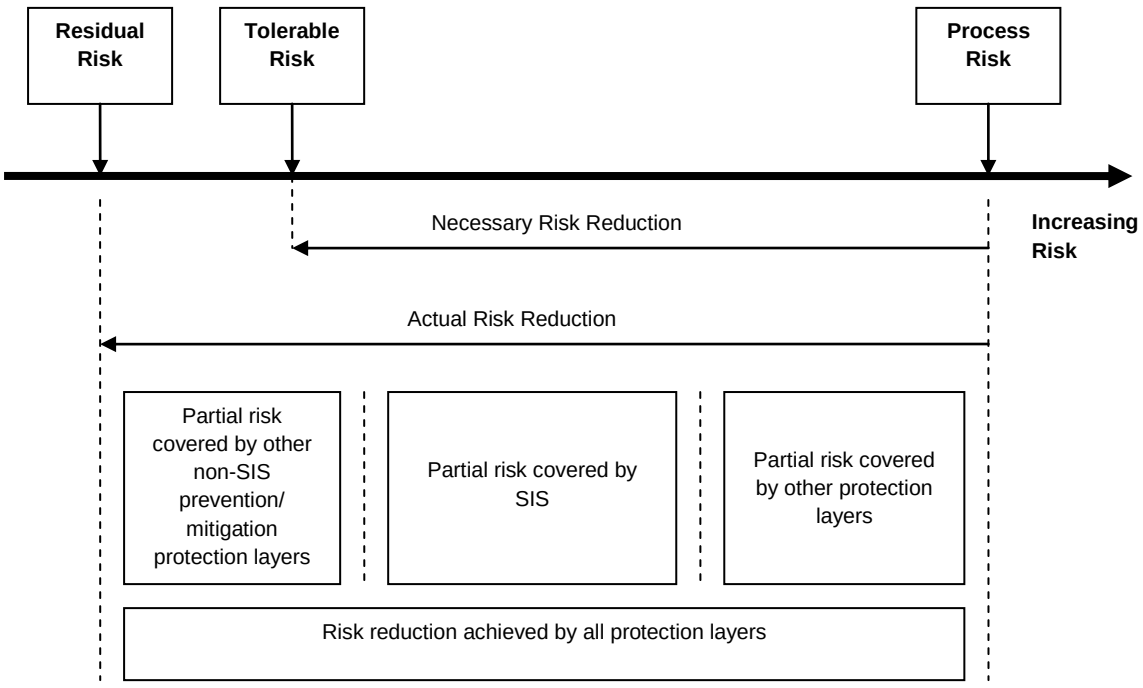

Figure 3 – Risk Reduction: General Concepts

Figure 3 shows the relationship between the risk reduction afforded by various protection layers. The intention of an integrity level assessment is to establish the maximum probability of failure on demand (PFD) of a SIS such that the overall process risk is reduced to less than the maximum tolerable level. In an assessment, the PFD's of other protection and mitigation layers are combined with the likelihood of the hazardous event occurring and the possible consequences of that event, to leave a 'risk gap' which must be closed by the chosen SIS integrity level. A Safety Integrity Level is defined in terms of the PFD as shown in Table 1 below.

Integrity Level	Average Probability of Failure on Demand (PFDavg)
4	$<=10^{-5}$ to $<10^{-4}$
3	$<=10^{-4}$ to $<10^{-3}$
2	$<=10^{-3}$ to $<10^{-2}$
1	$<=10^{-2}$ to $<10^{-1}$

Table 1 – Integrity Level and PFD

Each method to determine SIL attempts to deal with the following issues, either explicitly or implicitly:

- the severity of each consequence - fires, injuries, fatalities, environmental damage, property damage, business interruption, etc.
- the likelihood, or frequency, of each initiating cause of the undesired event – requirement to operate occurs x times per year,
- the capability of non-SIS layers of protection. No layer of protection is perfect; for example, a pressure relief valve may fail to open 1 out of 100 times it is required to operate,
- the frequency of the mitigated event compared to a target frequency – if the frequency of the mitigated event is low enough, the risk is viewed as tolerable. The more severe the consequences, the lower the target frequency.

Two IEC techniques for performing such studies are described here.

Risk Graph

Figure 4 shows a typical Risk Graph. In this semi-qualitative method, four parameters are used to define the risk:

1. Consequences of the risk (divided into four consequence bands dependent on the severity)
2. The degree of occupancy of the hazardous area (classified as either Rare or Frequent)
3. The probability of avoiding the hazard (either Possible or Not Likely)
4. The demand rate of the hazardous event (shown here in four bands dependent on the frequency of demand on the SIS).

Setting values for the bands defined under these parameters is known as calibration of the risk graph. Calibration is under the control of the company concerned based on its corporate criteria. In the UK, the risk to both individuals and society in general, has a maximum in the guidance, which is set by the competent authority.

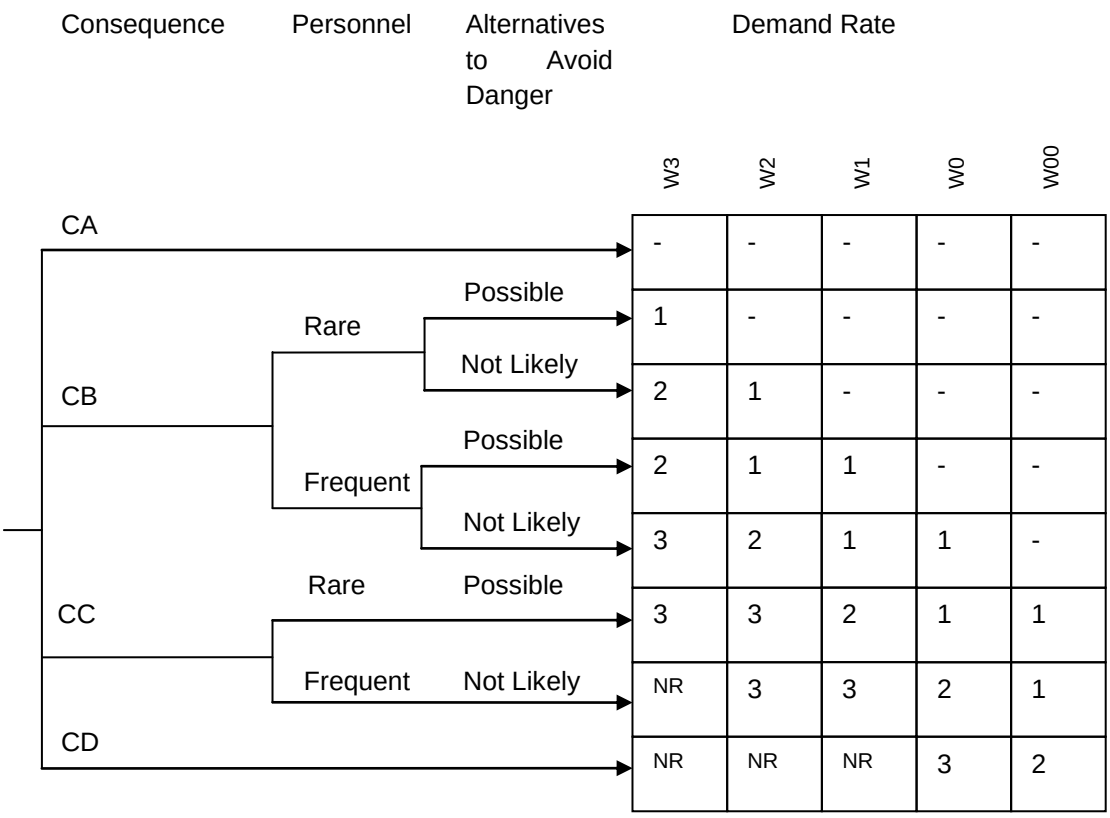

Figure 4 – Example of a Risk Graph

Risk graph methods have the following advantages, effectively summarised below(7):

- Precise hazard rates, consequences, and values for the other parameters of the method, are not required.
- No specialist calculations or complex modelling is required.
- They can be applied by people with a good “feel” for the application domain.
- Individual bias can be avoided.
- Understanding about hazards and risks is disseminated among team members (e.g. from design, operations, and maintenance).
- They do not require a detailed study of relatively minor hazards.
- They can be used to assess many hazards relatively quickly.
- They are useful as screening tools to identify:
    a. hazards which need more detailed assessment
    b. minor hazards, which do not need additional protection, so that capital and maintenance expenditures can be targeted where they are most effective, and lifecycle costs can be optimised.

Layers of Protection Analysis (LoPA)

This semi-quantitative method considers the protection layers to determine the risk reduction for a hazardous scenario. The method requires less input than performing, for example, a full Quantitative Risk Assessment (QRA), and is generally applicable for most hazardous events.

LoPA is a more rigorous method for assessment than risk graphs and is applied using both orders of magnitude values for PFD's and more specific frequency and probability data as appropriate. Being more sophisticated it requires greater effort on behalf of the assessment team. However, following the recommendations of the Buncefield Enquiry, it has become the UK regulator's 'preferred' method for integrity level assessment.

Overall Lifecycle Approach

Costain developed an approach for a recent client to completely assess a gas receiving terminal in the UK. The assessment exercise was extremely extensive and covered all SIF's on two sites and a number of off-shore facilities. In total 864 SIF's were to be assessed. The client naturally wished to reduce the time and effort involved in what was possible a very costly exercise and required us to produce an assessment procedure and approach that would make best use of both the client's and our own resources. The Overall Lifecycle Approach Model is presented in Figure 8, below.

The assessment begins with a Risk Graph assessment of all SIF's as a screening exercise. This first iteration produces a database of SIF's that are assessed as IL 2-and-below and those of IL 3-and-above (box 1 in Figure 8). Risk graph, being more conservative than LoPA, will frequently assess SIF's as IL 3-and-above, when a more detailed treatment using LoPA might assign IL 2-and-below. Risk Graph is an order of magnitude method whereas LoPA allows either order of magnitude or more precise actual/derived/calculated values to be used. The database of IL 2-and-below is then subject to a periodic review in accordance with IEC 61508.

The database of SIF's of SIL 3-and-above is then re-assessed using LoPA (box 2 in Figure 8). Two outcomes are possible; either the Integrity Level is confirmed as being 3-and-above or the level is reduced to either 1 or 2. In the latter case the revised level is recorded and that SIF joins the database of IL 2-and-below.

The database of IL 3-and-above is now subject to a further assessment using some form of QRA(8). Our clients' corporate policies are frequently to reduce the number of SIL 3-and-above SIF's. QRA using some more sophisticated analysis such as fault tree or event tree analysis will either confirm a level of 3 or 4 for the SIF. If a level of 3 is confirmed then the SIF is added to the database if IL 3 SIF's.

It is a 'rule of thumb' that IL 4 is reserved for nuclear installations and some highly specific applications and clients usually have an expectation that there should be no residual IL 4 SIF's. Consequently, any IL 4 SIF's, that are not removed during the preceding assessments, are referred to the Corporate Design Safety Authority who will authorise a re-design (box 4 in Figure 8) of the system under consideration. A re-design may add in layers of protection to reduce the frequency of the hazard, increase mitigation measures to reduce the consequences or re-configure the process to remove or reduce the risk entirely. A re-design, it must be remembered, may affect the outcomes of other safety studies based on the original design. The design safety authority should again be consulted to establish those studies and how the changes should be addressed, whether by an update or a complete re-study.

The output of the first round of assessments is two databases or lists of SIF's; those of IL 1 and 2, and those of IL 3. These must be assessed again periodically to reflect any changes in legislation, in plant or process or in the base data used in the original assessments (boxes 5a and 5B in Figure 8).

The lifecycle approach allows the IL 1 and 2 SIF's to be re-assessed using Risk Graph and the IL 3 SIF's to be re-assessed using LoPA. Because there is no repeat of an IL 3 SIF going through the Risk Graph process, the approach again offers a substantial saving of time and resource.

Experience of Using the Approach

Reduced time and effort

Costain has monitored closely the application of the approach to the integrity level assessment of a gas receiving terminal, for one of its clients. The results of our monitoring, and previous assessments that used either risk graph or LoPA in isolation, has allowed the following observations.

A risk graph assessment exercise of 'n' SIF's might take 'm' hours.

The corresponding LoPA exercise, we would normally expect to take 2m hours.

Our experience has been that, on average, every 100 SIF's assessed yields perhaps 25 SIL 3-and-above SIF's. The number of SIF's taken to LoPA is then:

$$\frac{25n}{100} \tag{1}$$

To subject these to LoPA will take:

$$\frac{25}{100} \times 2m = \frac{50}{100} m = 0.5m \tag{2}$$

Thus, using this method would take:

$$m + 0.5m = 1.5m \tag{3}$$

To subject all SIF's to LoPA alone would take 2m hours and therefore the time saved is:

$$2m - 1.5m = 0.5m \tag{4}$$

Thus, the time that would have been taken to review all SIF's using LoPA only, is reduced by about 25% by using this approach. On a large assessment exercise, this can represent tens of thousands of pounds.

The time saved, over a purely LoPA based assessment, is dependent on the number of SIL 3-and-above SIF's and, hence, how hazardous the facility is. In particular, if all the SIF's were SIL 3-and-above, then the amount of time taken to assess them would be increased using this approach. If the number of SIL 3-and-abve SIF's is greater than 50% of the total, then there is no advantage to the approach. However, our experience has been that, on average, time savings of between 15 and 25% on LoPA, are consistently achieved.

Reduced repetition

After the initial assessment has been finished for a particular exercise, the IEC standard requires that a re-assessment is undertaken at prescribed intervals in order to take into account any changes that may have occurred. These changes may include those to the plant, to neighbouring plant, the degree of occupancy, changes in the use of the surrounding area, more appropriate base data etc.

For the re-assessment exercise, SIF's can be re-assessed using the same technique as previously. This effectively matches the criticality of the SIF with the appropriate technique, removes the need to re-assess using another technique, while preserving the rigour of the first assessment. If a loop is re-

assessed as SIL 3 from SIL 2, then it will move up into the LoPA assessment list and vice-versa. In the majority of cases, however, there will be only a few changes meaning that the time saved is greater for the re-assessment exercise.

Client Advantage

In addition to the reduced time, effort and resource associated with the approach, it is important to mention that Integrity Levels are not always driven by safety interests. An assessment is usually performed three times, once considering the safety consequences of the event, once considering the environmental hazards and a further assessment using the potential effects on the asset and any associated loss of revenue. Thus the loss of income associated with damage or the loss of a particular facility or process item can be given appropriate weight when considering the consequences under each of these three categories.

Regulatory Compliance

The philosophy in the regulation of safety management systems is that resources should be aimed at those hazards producing the highest risk. As part of a demonstration that the hazards are fully understood, an integrity level assessment identifies those hazards and the potential risk from them. Because there is a corresponding relationship between the degree of risk and the rigour with which this approach treats the risk, resources are targeted appropriately and the risk is therefore understood, to the benefit of both client and regulator.

How the Buncefield Recommendations are Addressed

Costain took the recommendations following the review of LoPA assessments by the HSE (2), seriously and in July 2010 was formally able to apply for CASS (Conformity Assessment of Safety Related Systems) certification(9) of its Safety Instrumented Systems assessment and design procedures. The CASS Scheme provides a rigorous and internationally acceptable structure under which certification of safety related systems can take place. It ensures consistency and transparency in the assessment of products, integrated systems and the associated functional safety management systems, and clarifies issues of interpretation with the generic standard. As an example of Costain's responsibilities under the certification scheme all potential chairs for assessment studies are required to undergo training(10) in LoPA from a reputable organisation e.g. IChemE and demonstrate their ability before they are able to conduct studies on behalf of clients.

The lifecycle approach model fits into our existing Integrity Level Assessment systems and procedures.

Our software for conducting assessments contains a set of standard data for frequencies and PFD's (e.g. frequencies for some initiating events, failure rates for equipment and frequencies for Human Factors events are included) that will be used during the study. This data is updated regularly to reflect the most current guidance. That the data is included in the software ensures that an effective audit trail is maintained.

Training records for those chairing studies and the qualifications, experience and roles of those participating in them are recorded. Procedures to control and ensure consistency of approach define the make-up of the assessing team.

Sensitivity studies may be performed easily where the data is less certain or where a result is a border-line value. The effects of small changes in one or two variables may be easily examined in detail within the assessment meeting and fully documented.

Further Work

We recognise that a true lifecycle approach includes the development of the method to reflect changes in both the legislation and IEC 61508. In addition, changes to the application of assessments, to best practice and to the experience of others has allowed us to refine and update the approach. In particular, a variety of sources of information are routinely monitored and relayed into the continuing development and application of the approach. These include IEC 61508 Working Groups and Forums, whose purpose is to monitor and provide a focal point for feedback to the IEC such that experience and best practice can inform subsequent revisions and disseminate information, working papers and revisions for comment. The benefit of this networking allows us closer ties with parties who may take similar approaches, to share knowledge and to potentially win further business.

Each application of the approach allows us to refine the performance data. This allows us to ensure that the approach remains valid across the wide range of industries with which we work and ensure that the benefits are available to all our clients.

The approach will not necessarily be applicable to every case. Where only a few SIF's are to be assessed then directly proceeding to LoPA may be the best use of resources. However, we have seen real benefits to our clients in using this approach; it is simple, it retains the rigour of assessment required by the greatest hazards and it provides the most cost-effective solution for the customer.

Further Information

http://www.buncefieldinvestigation.gov.uk

http://www.hse/gov.uk/buncefield/response.htm

Figures

Figure 5 – The Buncefield site prior to the explosion

Figure 6 – After the explosion

Figure 7 – The smoke plume photographed looking South by an aircraft leaving Luton Airport (1)

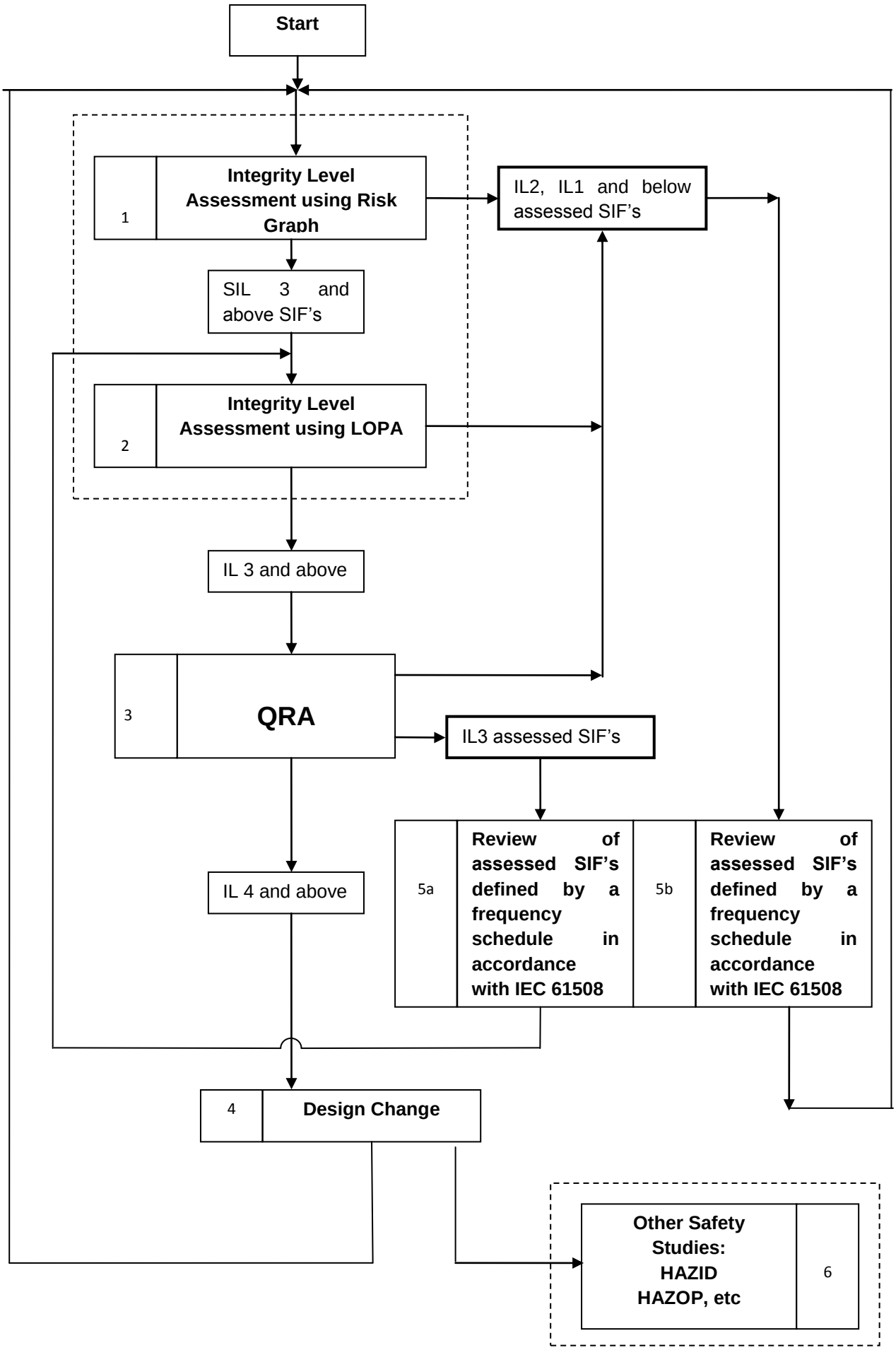

Figure 8 – The lifecycle Integrity Level Assessment Flowchart used for a Client

References

1. **Buncefiel Major Incident Investigation Board.** The Buncefield Incident, 11 December, 2005 - The Final Report of the Major Incident Investigation Board. Kew : The Office of Public Sector Information, 2008. Vol. 1.

2. **Health and Safety Laboratory.** A Review of Layers of Protection Analysis (LOPA) Analyses of Overfill of Fuel Storage Tanks. s.l. : HSE, 2009. RR716.

3. **British Standards.** IEC-61508 Functional safety of electrical/electronic/programmable electronic safety-related systems. 2000.

4. —. IEC-61511-1:2004 Functional Safety - Safety Instrumented Systems for the Process Industry Sector - Part 1: Framework, Definitions, System Hardware and Software Requirements. 2004.

5. —. IEC-61511-2:2004 Functional Safety - Safety Instrumented Systems for the Process Industry Sector - Part 2: Guidelines for the Application of IEC 61511-1. 2004.

6. —. IEC-61511-3:2004 Functional Safety - Safety Instrumented Systems for the Process Industry Sector - Part 3: Guidance for the Determination of the Required Safety Integrity Levels. 2004.

7. **Gulland, W. G.** Methods of Determining Safety Integrity Level (SIL) Requirements - Pros and Cons. s.l. : 4-Sight Consulting, 2004.

8. **Dowell, A.M.** Layer of Protection Analysis: A New PHA Tool After Hazop, Before Fault Tree Analysis. *International Conference and Workshop on Risk Analysis in Process Safety.* New York : AIChE/CCPS, 1997.

9. Conformity Assessment of Safety Systems. *CASS Scheme.* http://www.cass.uk.net/.

10. **The Institution of Electrical Engineers.** Competence Guidelines for Safety-Related System Practitioners. s.l. : IEE, 1999.

11. **Blackmore, R.** IEC-61508 - Practical Experience in Increasing the Effectiveness of SIL Assessments. New Orleans : ISA, 2000.

12. **Buncefield Standards Task Group.** Final Report. 24 July 2007.