COMPLIANCE WITH LEGISLATION - TO WHAT EXTENT CAN A RISK ASSESSMENT USING THE FRAMEWORK OF IEC 61508 SATISFY THE REQUIREMENTS OF OTHER LEGISLATIVE REQUIREMENTS?

Lyn Fernie and Dick Schaap

AK EHS & Risk, Aker Kvaerner Engineering Services Ltd, Ashmore House, Stockton on Tees, TS18 3RE.

Vast amounts of resource are committed each year to deal with new legislative requirements. "Over the last 30 years the EU has generated over 300 directives, regulations, decisions and recommendations relating to chemicals and consumer protection, occupational health, environmental protection, process and transport safety and the management of chemical substances” CEFIC review 2002-2003. To minimise the cost of regulatory compliance operators need to do what they can to combine the various assessments required for the current and future legislation. The speaker will discuss whether this is feasible - can one risk assessment suit all requirements? If so, what is the most appropriate framework for risk assessment? The speaker will use a case study to demonstrate how an IEC 61508 assessment was expanded to include the requirements of Seveso II, ATEX, IEC 61508 and Criticality. The benefits of this approach will also be discussed, in particular the holistic approach that can then be adapted to generating and prioritising improvement programs.

INTRODUCTION

The European Commission has over the past years issued various directives on the major accident hazards, the safety of pressure equipment, machinery safety, explosion prevention and safety devices.

European Directives establish broad requirements and identify appropriate standards to achieve their aims. These directives and standards are often dealt with on an individual basis. However, to minimise the cost of regulatory compliance operators need to do what they can to combine the various assessments required for the current and future legislation.

Aker Kvaerner provides tools, methodologies, verification and independent consultancy to assist operators in the process, petrochemical, oil & gas, power, nuclear, water and pharmaceutical industries comply with the individual directives and guidelines. This paper will in particular consider the requirements of Seveso II, ATEX, IEC 61508 and their interrelation and propose an approach to integrate these requirements in a framework risk assessment for such industries.

THE NEED FOR EUROPEAN DIRECTIVES

The need for European Directives on safety and control of risk is dictated by a number of severe accidents involving multiple fatalities, injuries and environmental harm, some of the most significant accidents are listed below:
Ammonium Nitrate Explosion, Oppau, 1921
- Texas City Ship Explosion (Ammonium Nitrate), 1947
- Refinery Fire at Feyzin, 1966
- Cyclohexane Explosion, Flixborough, 1974
- Dioxin Release, Seveso, 1976
- LPG BLEVE, Mexico City, 1984
- Methyl Isocyanate Release, Bhopal, 1984
- River contamination from fire water run off, Switzerland, 1986
- Vapour Cloud Explosion, Pasadena, USA, 1989
- Jet Fire, Castleford, UK, 1992
- Explosion in a Grain Silo, Blaye, France, 1997
- Cyanide spill in the River Tisza in Baia Mare, Romania, 2000
- Explosion at fireworks warehouse in Enschede, Netherlands, 2000
- Ammonium Nitrate Explosion, Toulouse, 2001
- Fire Skikda Refinery, 2004
- Train Crash, Iran, 2004
- Vinyl Chloride Explosion, Illiopolis, 2004

For operators, loss of production facilities, social acceptance and insurance premium reductions are additional motivators to comply with the directives in a pro-active and integrated way.

EUROPEAN DIRECTIVES

A number of European Directives, guidelines and standards have been published in response to these major accidents. Those relevant to this discussion are summarised below:

Seveso II (96/82/EC)

The aim of the Seveso II Directive is two-fold. Firstly, the Directive aims at the prevention of major-accident hazards involving dangerous substances. Secondly, as accidents do continue to occur, the Directive aims at the limitation of the consequences of such accidents not only for man but also for the environment.

The scope of the Seveso II Directive is limited solely to the presence of dangerous substances in establishments. It covers both, industrial "activities" as well as the storage of dangerous chemicals.

Pressure Equipment Directive (97/23/EC)

The directive provides, together with the directives related to simple pressure vessels (87/404/EC), transportable pressure equipment (99/36/EC) and Aerosol Dispensers (75/324/EEC), for an adequate legislative framework on European level for equipment subject to a pressure hazard.

Its purpose is to harmonise national laws of Member States regarding the design, manufacture, testing and conformity assessment of pressure equipment and assemblies of pressure equipment. It therefore aims to ensure the free placing on the market and putting into service of the equipment concerned within the European Union and the European Economic Area.
Under the Community regime of the Directive, pressure equipment and assemblies above specified pressure and/or volume thresholds must:

- be safe;
- meet essential safety requirements covering design, manufacture and testing;
- satisfy appropriate conformity assessment procedures; and
- carry the CE marking and other information.

Pressure equipment and assemblies below the specified pressure / volume thresholds must:

- be safe;
- be designed and manufactured according to sound engineering practice; and
- bear specified markings (but not the CE marking).

**Machinery Directive (98/37/EC)**

The Machinery Directive provides the regulatory basis for the harmonisation of the essential health and safety requirements for machinery at European Union level. Essentially performing a dual function, the Directive not only promotes the free movement of machinery within the Single Market, but also guarantees a high level of protection to EU workers and citizens.

Machinery is described in the Directive as "an assembly of linked parts or components, at least one of which moves, with the appropriate actuators, control and power circuits, etc., joined together for a specific application, in particular for the processing, treatment, moving or packaging of a material".

**ATEX 137 (1999/92/EC)**

ATEX 137 lays down the minimum requirements for improving the safety and health protection of workers potentially at risk from explosive atmospheres.

The employer shall take technical and/or organisational measures appropriate to the nature of the operation, in order of priority and in accordance with the following basic principles:

- the prevention of the formation of explosive atmospheres, or where the nature of the activity does not allow that,
- the avoidance of the ignition of explosive atmospheres, and
- the mitigation of the detrimental effects of an explosion so as to ensure the health and safety of workers.

These measures shall where necessary be combined and/or supplemented with measures against the propagation of explosions and shall be reviewed regularly and, in any event, whenever significant changes occur.

**COMMONALITY BETWEEN THE EUROPEAN DIRECTIVES**

European Directives generally establish broad requirements and general duties, but the implementation is left to the manufacturers and operators. This is true of the directives referred to above, they are formulated under the New Approach, meaning that the directive provides for a flexible regulatory environment that does not impose any detailed technical solution. This approach allows European industry to develop new techniques thereby increasing international competitiveness.
One common theme is that risk assessment is increasingly the cornerstone of the European Directives. There is therefore the potential to use this commonality to introduce a framework approach to meeting the requirements of a number of directives. In fact this is advocated in some of the directives – the following extract is taken from the ATEX 137 Directive:

“An assessment of explosion risks may be required under other Community acts; whereas, in order to avoid unnecessary duplication of work, the employer should be allowed, in accordance with national practice, to combine documents, parts of documents or other equivalent reports produced under other Community acts to form a single ‘safety report’”

RISK ASSESSMENT

A risk assessment considers the likelihood and magnitude of a range of possible adverse effects, and then makes a judgement about these outcomes by comparison with criteria. The validity of any judgements made are crucially dependent on the quality of the risk assessment.

A risk assessment should:

? Identify all possible initiating events that might lead to adverse effects.
? Identify the event sequences whereby the initiating events can lead to the adverse effects.
? Evaluate the extent of the risk:
  o Likelihood of adverse event occurring.
  o Potential severity of harm/damage.
? Compare calculated risk with some criteria, standard or policy to assess the level of tolerability.
? Identify risk reduction measures or risk control strategies.

Some of the risk control strategies applied by operators are listed below:

? Risk based design techniques.
? Risk based inspection.
? Piping system integrity analysis.
? Reliability centred maintenance.
? Proof testing for instrument loops.
? Hazardous area inspection.

THE NEED FOR INTEGRATED ASSESSMENTS

All too often it is found that connection between the various drivers is not made and a series of risk assessments are carried out to meet separate legislative or corporate requirements. Each of these carries its own action / improvement plan and maintenance / inspection regime, making holistic risk management an impossible task. Specifically comparison between differing risk reduction measures or risk control strategies becomes difficult as the basis for the various assessments is not common. So, although the techniques employed to reduce risk are often aimed at lifecycle cost optimisation, it is often not possible to achieved optimised lifecycle costs.
Considering that risk assessment forms a common denominator for compliance with European Directives it would seem logical that there is a basis for an integrated approach using a framework risk assessment.

The benefits of a framework risk assessment are:

- Less duplication of effort
- All risks considered
- Trade off between risks considered
- One assessment, one dossier
- A central register of hazards and risks – hazard log
- A holistic approach to risk management
- Significant cost savings by optimising maintenance and inspection work

The different directives require a proportionate approach to be taken to risk and therefore the question to be posed is “to what extent can one risk assessment give compliance with all directives, legislation and standards and what basis should be used for this framework risk assessment”.

**RISK ASSESSMENT BASED ON FUNCTIONAL SAFETY AND IEC 61508**

A set of guidelines exist that, if correctly implemented in an organisation, can help companies fulfil their legal obligations, reduce serious financial business risks, and contribute to the bottom line through effective use of maintenance resources. The international standard IEC 61508 provides a generic framework for achieving functional safety with regard to Electrical/Electronic/Programmable Electronic (E/E/PE) safety related systems. It is mainly concerned with the E/E/PE safety related systems whose failure could have an impact on the safety of people or the environment. IEC 61511 is the daughter standard for the process industry sector.

**IEC 61508 and IEC 61511**

The standards use the concept of the Safety Lifecycle (from concept design, through hazard and risk analysis, specification, implementation, operation, maintenance to eventual decommissioning) as a framework to achieve functional safety in a systematic and auditable manner.

The safety lifecycle phases from IEC 61511 are listed below:

- Hazard and risk assessment
- Allocation of safety functions to protection layers
- Safety requirements specification for the safety instrumented system
- Design and engineering of safety instrumented systems
- Installation, commissioning and validation
- Operation and maintenance
- Modification
- Decommissioning

The above phases are supported by the management, planning and verification phases of the standard.
The IEC 61511 lifecycle is illustrated in Figure 1 below. It indicates the range of activities that need to be considered under the standard.

**FIGURE 1: IEC 61511 LIFECYCLE**

The key approach of both standards is the use of risk assessment to determine the design of control and protection systems. The standards require the use of risk assessment to determine what the necessary risk reduction is for the process and then taking account of inherent safety, allocating that risk reduction to safety systems. These safety systems can be mechanical devices such as relief valves as well as instrumented protective systems. In fact, appropriately applied Safety Integrity Level (SIL) assessment often leads to a re-consideration of how the
necessary risk reduction may be achieved. The necessity to design and maintain a SIL rated system can lead to more lateral thinking in terms of alternative risk reduction methods and helps to avoid the “belt and braces” approach that is often the tendency of the design team.

IEC 61508 / IEC 61511 provide a basis that can be used for integrated risk assessment by incorporating more than just the quantification of the benefit of instrumented safety systems as risk reduction measures. The output of the integrated risk assessment can be used as the basis for the criticality assessment and the development of maintenance and inspection strategies, such as Risk Based Inspection and Reliability Centred Maintenance, again, not just the proof test interval for instrumented systems.

The complexity of the risk assessment may be increased and therefore it is recommended that the integrated risk assessment is carried out by knowledgeable and experienced HSE practitioners.

**CASE STUDY**

For all installations with the potential to cause a major accident, a risk assessment is necessary under the Seveso Directive, where all significant hazards are addressed, and suitable controls provided. The outcome of the risk assessment must enable the decision-makers to identify any shortcomings in the existing or proposed preventative measures.

The site discussed in this case study required an assessment of risk for the purposes of Seveso and the vehicle used for this assessment was IEC 61508. However to minimise the resource required and to reduce the overlap with assessments carried out for the recently introduced ATEX 137 Directive, the aim of the assessment was to combine the risk assessments for ATEX, Seveso and IEC 61508. In addition, the output was to be used as the basis of criticality assessment and development of integrated maintenance and inspection strategies.

A procedure for an Integrated or Framework Risk Assessment based on IEC 61508 / IEC 61511 was developed, this is outlined below.

**Principles and Content of the Procedure for an Integrated or Framework Risk Assessment based on IEC 61508 / IEC 61511**

The procedure is segmented as follows:

- Common Requirements
- Concept Development
- Overall Scope Definition
- Process Hazard and Risk Analysis and Protection Layer Identification
- Overall Safety Requirements Allocation

The ‘Common Requirements’ section gives requirements for project managers to establish and implement a ‘Lifecycle EHS Plan’, to then monitor and verify implementation of the plan and finally to instigate a ‘Functional EHS Assessment’ once implementation of the rest of the procedure is complete.

The ‘Functional Safety Assessment’ is required to evaluate the assessments made against the following criteria:
Have all hazards of the process or equipment been considered?
Are the assessments based on sufficient and firm information?
Are the assessments neither unduly pessimistic nor optimistic?
Are the assessments technically correct?
Have realistic risk reduction values been allocated?

The ‘Concept Development’ section sets down the data gathering requirements to ensure that the process, equipment and its environment are sufficiently understood before detailed assessment commences. The procedure sets down the information requirements under the following headings:

- Process definition
- Chemicals and services
- Physical and hazardous property data
- Plant location and local environment
- Legislative, consultation and risk requirements

Within the ‘Concept Development’ section there is an opportunity to decide which of the European Directives, national regulations, or corporate guidelines will be addressed by the framework risk assessment, and to modify the approach accordingly.

The ‘Overall Scope Definition’ section requires the boundary of the process and equipment being assessed, to be defined. The output is a defined and documented basic design, operating philosophy, control system and alarm response, together with a preliminary P&ID showing controls and alarms.

The ‘Process Hazard and Risk Analysis and Protection Layer Identification’ section is based on the output from ‘Concept Development’ and ‘Overall Scope Definition’. The stated objectives are to:

- To identify hazards and hazard scenarios associated with the process and equipment.
- To eliminate or reduce risks arising from the equipment under control where possible prior to further assessment (inherent safety).
- To identify hazard scenarios requiring risk reduction.
- To identify the necessary level of risk reduction to be achieved.

The focus of this section of the procedure is to assess all hazard scenarios associated with the process and equipment. Various approaches can be taken at this stage, some are listed below:

- Risk graph or risk matrix (integrated and calibrated)
- Layers of protection analysis
- Assessment of fault tolerance
- Failure modes and effect analysis
- Quantified risk assessment

Each of the techniques has benefits and limitations and often lends itself to a particular category of hazard/risk assessment. For example the fault tolerance approach is particularly suited to ATEX 137 assessments of mechanical equipment, where the fault tolerance is the number of independent faults or system failures which is admissible, before the ignition source becomes active in the unprotected/unguarded situation. The fault tolerance is therefore a benchmark for the frequency and duration of the presence of an ignition source.
The assessment can be carried out for human harm, environmental or financial loss. The range of harm categories used in the assessment at this stage may need to be broad to enable a full spectrum of adverse effects to be covered and also to take account of society’s aversion to incidents affecting large numbers of people at one time.

The ‘Overall Safety Requirements Allocation’ section defines how to allocate the necessary risk reduction to risk reduction measures, taking into account the operational and financial acceptability of the allocated risk reduction measures. Once all other technologies have been considered, residual risk reduction is allocated to instrumented systems.

The output of the framework risk assessment is a methodically defined and substantiated allocation of safety requirements. The output can be used to identify the critical systems and optimise inspection and maintenance strategies.

In a recent paper from the HSE by Vernon (2004) a top tier Seveso site in the UK is described where IEC 61508 has been applied. This site has found that its application has lead to a significant reduction in maintenance overheads. This has been achieved through designing systems such that they require less frequent maintenance and also by setting maintenance frequencies using a risk based approach. It was found that in many areas the site had been over-maintaining its equipment. This reduction in maintenance and the consideration of how plant would be maintained at the design phase can also lead to reduced plant downtime for maintenance.

It is recommended that where Integrated Risk Assessments are applied that these are carried out in the context of a wider Management System.

**Application of the Integrated Risk Assessment**

The initial difficulty encountered was in the hazard identification step as the Seveso assessment required the identification of all major accident hazards, generally achieved by identifying large loss of containment events, often generic in nature, whereas ATEX requires the assessment of hazards which have lesser perceived consequences, and tend to be more specific as the environment of the equipment is important in the ATEX assessment, as the hazardous area zoning determines the category of equipment required. To overcome this difficulty, the range of guidewords adopted was expanded. In addition, a plant tour was conducted for each section of plant reviewed to ensure that no hazards or initiating events were overlooked.

To allow the ATEX assessment to be incorporated, it was necessary to have completed an initial hazardous area classification prior to the hazard identification step, however this led to some iteration.

The methodology adopted for the risk analysis step was a team based semi-quantitative approach using layers of protection analysis as an initial screening exercise followed by FMEA / fault tree analysis of scenarios that required a risk reduction greater than 2 orders of magnitude.

There was much debate during the risk analysis step regarding the treatment of differing types of scenarios and protection layers. The main discussion point was whether the basis for assessment should be conversion of all protection layers and risk reduction measures to SILs, use of a common factor, or use of a fully numerical assessment. Eventually a numerical
analysis was used, however this was found to be time consuming and led to lengthy discussions during the assessment meetings.

Following the initial pilot study, further work indicates that the use of a common factor provides a better approach as it allows the team to select the appropriate factor using word models and pre-prepared pick lists. The pitfall is that this method then becomes more subjective and perhaps introduces greater uncertainty. In addition, when using a factor based assessment, it has been observed that members of the assessment team find it hard to place events in a specific category. This problem can be eliminated by using a finer resolution for the factors utilised.

The routine of identifying the event sequences and formally applying consequence and frequency criteria can lead to some surprising results. Where the methodology has been applied to existing plant it has been found that some of the safety related systems previously considered to be critical are not necessarily so. It has also, conversely (but rarely) been shown that some systems that were deemed non-critical require higher further risk reduction than the assessment team would have anticipated.

**CONCLUSIONS**

Risk assessment forms a common denominator for compliance with many European Directives and therefore the authors set out to develop an integrated approach using a framework risk assessment based on IEC 61508 / IEC 61511.

When applied to a top tier Seveso site the procedure was found to provide risk assessments suitable for compliance with the Seveso Directive, the ATEX 137 Directive and IEC 61508. The advantage of the application of an integrated risk assessment procedure was that it provided a logical documented and justified rating for all risk reduction measures. In addition, the IEC 61508 / IEC 61511 approach requires the event sequences to be defined rigorously as part of the hazard and risk analysis step. This was found to be very useful when later attempting to quantify the frequency of undesired events.

The output from the integrated risk assessment proved to be a sufficient starting point to develop risk based inspection and maintenance strategies for the site, allowing a holistic approach to the lifecycle integrity management of the installation.

The procedure has since been developed further to incorporate the risk assessments required for the Machinery Directive and the Pressure Equipment Directive.

**REFERENCES**