THE ASSESSMENT OF TECHNICAL ASPECTS OF COMAH SAFETY REPORTS

R F Evans
Health & Safety Executive, Chemical & Hazardous Installations Division, Bootle

Under European Union Council Directive 96/82/EC the UK is obliged to introduce new legislation to replace the Control of Industrial Major Accident Hazards (CIMAH) Regulations 1984. To implement this directive new Regulations, the Control of Major Accident Hazards (COMAH) Regulations will come into force on 3 February 1999.

In preparation for implementing the new Regulations HSE has drafted a set of criteria to assist its staff in the assessment of Safety Reports. This paper describes those criteria and a pilot exercise whereby the criteria were tested on safety reports voluntarily submitted by industry.

Keywords: Major hazard, Safety Report, Legislation

INTRODUCTION

Under European Union Council Directive 96/82/EC the United Kingdom is obliged to introduce new legislation to replace the Control of Industrial Major Accident Hazards (CIMAH) Regulations 1984. To implement this directive new Regulations, the Control of Major Accident Hazards (COMAH) Regulations will come into force on 3 February 1999. Among the changes the new Regulations will impose new duties on the Competent Authority[1]. These include the requirements to:

- within a reasonable period of receipt of a safety report, communicate the conclusions of its examination of the report to the operator, if necessary after requesting further information; or

- prohibit the bringing into use, or continued use, of the establishment concerned where the measures taken by the operator for the prevention and mitigation of major accidents are seriously deficient.

It was recognised, therefore, that there was a need to be prepared, before the Regulations came into force, to assess safety reports in a reasonable time and identify any possible serious deficiencies.

PREPARING FOR THE NEW REGULATIONS

[1] The Competent Authority comprises the HSE and the Environmental Agency or the Scottish Environmental Protection Agency as appropriate.

HSE in conjunction with the environmental agencies has drawn up a manual called the *Safety Report Handling, Assessment and Review Principles & Processes* manual, known as SHARPP for short. This has undergone widespread consultation and been subject to a pilot exercise to ensure its fitness for purpose.

The manual contains the following parts:

Guiding Principles

These are described in another paper but include such things as the purpose of assessment, the system aims and objectives etc.

Procedures

These are essentially the administrative procedures for dealing with safety reports.

Assessment Criteria

These are the criteria against which safety reports will be assessed and cover the following topics:

Information on the Safety Management System

Description of the Establishment

Predicting the Consequences of Major Accidents

Technical Risk Reduction Measures

TECHNICAL ASSESSMENT CRITERIA

The Purpose of the Criteria

The technical assessment criteria are summarized in the appendix to this paper. Their purpose is to provide a framework for the technical assessment of safety reports whilst not unduly limiting the discretion of the assessor thus achieving a balance between the conflicting requirements of consistency of assessment between safety reports and the need for flexibility. They are not intended to be regarded as detailed technical guidance although work is in hand to produce such guidance by drawing on existing codes and standards and generating new guidance as appropriate.

The assessment criteria will be made publicly available in the interests of openness and it is expected they will assist authors of safety reports by providing an insight as to how the competent authorities will assess their work. It should however be noted that they are primarily intended to assist assessors and are not intended as a guide to the writing of safety reports.

Drafting the Criteria

The criteria were drafted by a working group. To ensure that the final document reflected the views not only of the Competent Authority but also of those who would have to draft safety reports the working group was composed of members of the Environmental Agency, the HSE, a consultancy and a major petrochemical company. The petrochemical company representative worked on secondment to HSE as a member of the working group but, at the same time, was involved in drafting, on behalf of his parent company, a safety report for the pilot exercise. He was therefore able to give a valuable insight into problems our criteria posed for those writing safety reports.

A separate group consisting of members of the Environmental Agency and the HSE was set up to peer review the document and two consultation exercises were carried out: the first internal only, the second internal and with some informal external consultation.

The process of drafting the criteria was essentially an iterative one starting with a brainstorming session to obtain an initial set of criteria that were then peer reviewed. The document was revised in light of the comments from the review team. The process of review and redrafting was then repeated.

Throughout this exercise we were well aware of the need to draw from past experience of other parts of HSE in safety report and safety case assessment. Therefore, although we drew heavily on the *Assessment Principles for Offshore Safety Cases*[1] and *Safety Assessment Principles for Nuclear Plants*[2], at the same time we also tried to learn from past mistakes. For example from our experience with the manual for assessing Offshore Safety Cases we new that it would not be possible, in the time available, to produce detailed technical guidance of a good quality and we concentrated instead on identifying the main assessment criteria with a view to developing the technical guidance later. By doing this we achieved two things: we were able to produce an assessment manual in advance of the Regulations coming into force and we provided a framework for the subsequent technical guidance.

We also drew on *AVRIM 2*[3], a document drawn up for the Dutch Government to assist in the inspection of Major Hazard Installations.

The Structure of The Criteria

There are 2 fundamental technical criteria and these are that:

- the safety report should show a clear link between the measures taken to reduce risks and the major accident hazards described in the report; and
- the safety report should show how the measures taken will reduce the risks from foreseeable failures which could lead to major accidents.

All other criteria are seen as being subordinate to the above and are classified under the following headings:

Design This includes conceptual design, plant layout, process design and the detailed design of equipment.

Construction This includes the manufacture, installation, construction of civil structures, testing, initial inspection and commissioning.

Operation This includes plant start up, shut down, normal operation and emergency shutdown.

Maintenance This includes preventive maintenance, repair, replacement, periodic examination by a competent person and the assessment of any defects found.

Modification This includes all alterations (including decommissioning) which could affect the integrity of the installation.

THE PILOT EXERCISE

It was recognised that no matter how much consultation and peer reviewing were carried out the best way to find out how our assessment criteria would work in practice would be to test them in circumstances as near as possible to those in which they would eventually be applied. A pilot exercise was, therefore, carried out whereby four establishments voluntarily submitted safety reports written to meet the requirements of the draft COMAH Regulations. To assist them in this they were provided with early drafts of the assessment criteria. The establishments in question were:

The Elf terminal at Flotta

The ISC establishment at Hythe

BP Chemicals at Hull

The British Gas Transco Establishment at Cheltenham

The safety reports were assessed by teams whose composition reflected that of the sort of typical team that would be expected to assess statutory safety reports in practice. They used the draft manual for the basis of their assessments and their conclusions were sent to the operators. Although the reports were assessed as though they were real COMAH safety reports, the primary purpose of the exercise was to obtain information about how the assessment criteria and procedures worked in practice. This information was passed on to the team that was managing the pilot project and, in conjunction with the findings of a formal external consultation exercise that was carried out at the same time, was used as the basis of further revisions of the manual.

The conclusions of the pilot exercise were that some further guidance had to be given as to how assessors should use the assessment criteria but that the technical assessment criteria were about right. The main criticism of the technical assessment criteria arising out of the pilot study was that they gave the impression that all the criteria had to be met whereas in practice not all criteria would apply to all safety cases and the assessor would have to apply

considerable judgement in deciding which criteria applied in each case and how much weight to give to them

The consultation exercise generated few comments on the technical assessment criteria and most of them came from within the HSE rather than from external organizations. Most of the comments related to the need to clarify certain points.

The technical assessment criteria were amended to take account of comments received, where appropriate. Other papers presented at this conference deal with how these exercises led to changes in other parts of the SHARPP manual.

CONCLUSIONS

As a result of the consultation and pilot exercises we have a set of assessment criteria that we believe will enable us assess safety reports with the right balance between consistency and flexibility. Initially assessors will have to draw largely on their own knowledge and experience when assessing safety reports but in the long term we hope to be able to provide more technical guidance. It is expected that this guidance will be made publicly available as well as the assessment criteria and will therefore be of some assistance to industry in drafting safety reports

REFERENCES

1. Health and Safety Executive, Offshore Safety Division, 1997, Assessment Principles for Offshore Safety Cases

2. Health and Safety Executive, Nuclear Safety Division, Safety Assessment Principles for Nuclear Plants.

3 Dutch Ministry of Social Affairs, AVRIM 2.

Appendix

TECHNICAL ASSESSMENT CRITERIA

Criterion 1

The Safety report should show a clear link between the measures taken and the major accident hazards described.

The safety report should include a summary of the findings of the hazard identification process. It should show how the identified hazardous events have been ranked on the basis of their perceived likelihood of occurrence and consequences.

For hazardous events that could lead to a major accident, the safety report should show that risk-reduction measures have been put in place to reduce the risks to as low a level as is reasonably practicable. This may be done using qualitative or quantitative methods as appropriate to the circumstances. The report should justify the method chosen.

Criterion 2

The safety report should demonstrate how the measures taken will prevent foreseeable failures which could lead to major accidents

General The safety report is required to show that the necessary measures have been taken to prevent major accidents and to limit their consequences for people and the environment. The safety report is also required to show that adequate safety and reliability have been built into the design, construction, operation and maintenance of the installation. These demonstrations are closely linked and a single set of assessment criteria has been developed based on the life cycle of the installation.

Criteria 1 & 2 are seen as fundamental. Criterion 2 has been subdivided into lower level criteria, which have been grouped as follows:

2.1 design, which includes conceptual design, plant layout, process design and detailed design of equipment;

2.2 construction, which includes the manufacture, installation, construction of civil structures, testing, initial inspection and commissioning;

2.3 operation, which includes plant start up, shut down, normal operation and emergency shutdown;

2.4 maintenance, which includes preventive maintenance, repair, replacement, periodic examination by a competent person and the assessment of any defects found; and

2.6 modification, which includes all alterations (including decommissioning) which could affect the integrity of the installation.

Appendix

The lower level assessment criteria are designed to be generally applicable, to the full range of installations within the scope of COMAH. However, they may not all be applicable in all cases. The assessor must decide which are appropriate.

2.1 Design

Criterion 2.1.1
The safety report should show that the establishment and installations have been designed to an appropriate standard

This is the main criterion for assessing whether the safety report shows that adequate provision for safety has been included in the design of an installation and covers such matters as containment, redundancy and diversity, and separation and segregation.

Criterion 2.1.2
The Safety report should show that a hierarchical approach to the selection of measures has been used

The design stage in an installation's life presents the best opportunity to reduce risk. The use of a hierarchical approach to the selection of measures will help to ensure that precedence is given to those measures that avoid major accidents, that is through inherent safety and prevention measures. Prevention cannot be guaranteed in all circumstances and therefore it will be necessary to identify other measures to control and mitigate the consequences of any major accidents to reduce risks to as low a level as is reasonably practicable.

Although the design of a new installation offers the best opportunity to apply these principles they may also be applied to the design of modifications and operators of older establishments should be alert to the possibility of taking advantage of technical advances in their industry to improve safety.

The levels in the hierarchy are as follows.

Inherent Safety Inherent safety is concerned with the removal or reduction of a hazard at source. Examples of inherently safe techniques include; substitution of a less hazardous process, use of corrosion resistant materials of construction, reduction or elimination of hazardous inventory, design for maximum foreseeable operation conditions, fail-safe design principles, and appropriate plant layout, etc..

Prevention Measures These are intended to prevent the initiation of a sequence of events that could lead to a major accident. They can be management systems or features of the design of the installation, and can apply during design, construction, operation, maintenance and modification.

Appendix

Control Measures These are intended to prevent a hazardous event from escalating into a major accident. They include measures directed at preventing or limiting small releases that have the potential to escalate to a major accident.

Mitigation Measures These are measures that are taken to reduce the consequences of a major accident once it has occurred. Examples of this include safety refuges, bunding systems, fire-fighting facilities, emergency response procedures, traverses or mounds for explosives buildings, etc.

Criterion 2.1.3

Layout of the plant should limit the risk during operations, inspection, testing, maintenance, modification, repair and replacement.

Design of the layout of a plant can make a big contribution to reducing the likelihood and consequences of a major accident. The safety report should show that due attention has been given to ensuring safety in the design of the layout of the installation. In particular, it should show how the layout prevents or reduces the development of major accident scenarios.

Criterion 2.1.4

Utilities that are needed to implement any measure defined in the safety report should have suitable reliability, availability and survivability

Failure of a utility, e.g. water, air, steam, electricity, often results in a process upset, and may have effects across the entire establishment. Failure of an emergency facility, e.g. fire water, has the potential to cause an escalation of a relatively small incident into a major accident. The safety report should justify the steps that have been taken in design, construction, operation and maintenance, to ensure that these utilities and facilities will be available when required.

Criterion 2.1.5

The Safety report should show that appropriate measures have been taken to prevent and effectively contain releases of dangerous substances.

The safety report should identify means by which dangerous substances can be accidentally released from the containment and the measures provided to prevent the occurrence. The safety report should demonstrate the suitability of measures to prevent releases.

Criterion 2.1.6

The safety report should show that all foreseeable direct causes of major accidents have been taken into account in the design of the installation

All foreseeable direct causes of loss of containment accidents should be considered at the design stage. The majority of direct causes fall into one of the following categories. The safety report should show that these have been considered and suitable measures taken:

Appendix

a) Corrosion
b) Erosion
c) External loading
d) Impact
e) Pressure
f) Temperature
g) Vibration
h) Wrong equipment
i) Defective equipment
j) Human error

Criterion 2.1.7
The Safety report should show how structures important to safety have been designed to provide adequate integrity.

The safety report should provide sufficient evidence to show that the design of all structures important to safety has been based on sound engineering principles. This includes process and storage vessels, pipework and other items that form the primary containment boundary. Other key structural items such as support structures, bund walls, civil foundations, control rooms, buildings or barriers designed to withstand the effects of accidental explosions should also be included.

Criterion 2.1.8
The Safety report should how the containment structure has been designed to withstand the loads experienced during normal operation of the plant and all foreseeable operational extremes during its expected life.

This assessment criterion is a follow-up to the more general requirements for adequate structural integrity.

The safety report should provide details of the normal operating conditions of the plant and any foreseen operational extremes. Evidence presented in the safety report should include all of the conditions that the containment must withstand, such as external loads, ambient temperatures and the full range of process variations (e.g. normal operation, start-up and shutdown, turndown, regeneration, process upset, emergencies and uncovenanted explosions).

Criterion 2.1.9
The Safety report should show that materials of construction used in the plant are suitable for the application.

Appendix

The safety report should provide evidence that all materials employed in the manufacture and construction of the plant are suitable. Particular attention should be given to the selection of materials used for the primary containment of hazardous substances.

Evidence should be provided to show that materials have been selected with regard to the nature of the environment in which they are to be used. In particular the evidence presented should consider the substances being handled and process conditions such as temperature, pressure and flow. The evidence presented should pay particular attention to possible sources of corrosion and erosion. Evidence presented should also consider the external environment, such as the effects of sea air in coastal areas.

Criterion 2.1.10

The Safety report should show that adequate safeguards have been provided to protect the plant against excursions beyond design conditions

Typically, a plant will be designed to operate within a given range of process variables, the 'normal operating limits'. These are the operating constraints that apply to normal operating conditions. There will also be 'safe operating limits' that are the rated values upon which safety of the plant is based. An excursion beyond the 'safe operating limit' may result in a significant risk of loss of containment, fire or explosion.

Safe operation depends on the measures to prevent excursions from occurring, for example, safety-related control systems, relief systems, shutdown procedures, emergency vent and disposal systems, etc.. The safety report should contain a description of the philosophy underlying the application of these measures, and should describe the foreseeable events that have been taken into account, drawing links between identified hazards, system integrity and the use of suitable standards or good industry practices. It should show how each measure has been designed and constructed and operated so as to be available whenever the plant is operating.

Criterion 2.1.11

The safety report should describe how safety-related control systems have been designed to ensure safety and reliability.

Any safety-related control system that is required to prevent or limit the consequences of a major accident (whether to people or the environment), should be designed in accordance with an appropriate code or standard. This should include an identification and consideration of all the components and devices in the system that need to function to ensure safety. The evidence presented should show that the complete system from sensor to final element, including any software has been considered.

Criterion 2.1.12

The Safety report should show how systems which require human interaction have been designed to take into account the needs of the user and be reliable.

Appendix

An analysis of accidents indicates that most result from human error. The safety report should show how human factors have been accounted for in the design of equipment and operating, maintenance and modification of systems. This should include consideration of how human errors can be reduced and the role of management systems in reducing human errors and identification of the safety implications of human errors and what back up systems are in place.

Criterion 2.1.13

The Safety report should describe the systems for identifying locations where flammable substances could be present and how the equipment has been designed to take account of the risks.

The safety report should identify the system whereby hazardous (flammable and explosive atmosphere) areas have been identified and classified. This may have been via an area classification study in which areas where a hazard exists owing to the normal, occasional or accidental release of process materials to atmosphere have been designated in accordance with recognised standards.

Sources of ignition for flammable atmospheres may include electrical equipment, naked flame or hot surfaces, static electrical discharge, etc. The safety report should indicate how the likely sources of ignition have been considered in the design (e.g. electrical equipment selection for defined hazardous areas, avoidance of hot surfaces or naked flames or sparks associated with equipment such as through the use of spark arrestors, etc., control of static electrical build-up).

2.2 Construction:

Criterion 2.2.1

The safety report should show that the installations have been constructed to appropriate standards to prevent major accidents and reduce loss of containment.

The safety report should show that construction of plant and associated equipment is managed to ensure that it is built in accordance with the design intent. This criterion should be applied by assessors whenever new plant is constructed during the life cycle of the installation. Modifications are covered by a separate criterion.

Criterion 2.2.2

The safety report should describe how the construction of all plant and systems is assessed, and verified against the appropriate standards to ensure adequate safety.

The safety report should provide evidence that suitable assessment and verification of the construction process have been carried out. The evidence presented should show that the construction process has not compromised the design intent.

Appendix

The evidence presented should identify the key assessment and verification activities and the stages at which they are undertaken. The safety report should also provide an explanation of the methods used and show how they will ensure safety. The acceptance criteria for testing and examination programmes should be identified, where appropriate.

2.3 Operation:

Criterion 2.3.1

The safety report should show that safe operating procedures have been established and are documented for all reasonably foreseeable conditions.

The safety report should show that safe operating procedures have been established and documented for all foreseeable normal (including start-up and shut down) and abnormal operating conditions.

The report should identify how reviews of operating procedures are undertaken and recorded to take account of operational experience or changing conditions in the plant.

2.4 Maintenance:

Criterion 2.4.1

The safety report should show that an appropriate maintenance scheme is established for plant and systems to prevent major accidents or reduce the loss of containment in the event of such accidents.

The safety report should show that maintenance procedures are sufficiently comprehensive to maintain the plant and equipment in a safe state. The safety report should also show that maintenance activities will not compromise the safety of the installation and that maintenance staff will not be exposed to unacceptable risks.

Criterion 2.4.2

The safety report should show that there are appropriate procedures for maintenance that take account of any hazardous conditions within the working environment.

The safety report should identify the procedures that are necessary to take into account the working environment and enable maintenance activities to be carried out safely with respect to maintenance staff and to prevent a major accident.

The safety report should show that safe systems of work have been established so that all activities that could result in dangerous situations are or can be identified.

Criterion 2.4.3

The safety report should show that systems are in place to ensure that safety critical plant and systems are examined at appropriate intervals by a competent person.

Appendix

This criterion concerns those activities that are carried out over and above routine maintenance to verify the continuing integrity of safety critical plant and systems. Examinations by a competent person at appropriate intervals may be necessary because certain specialised skills or equipment is required, or because it is demanded by specific legislation (e.g. Pressure Systems and Transportable Gas Container Regulations). For the purposes of this criterion, examination also includes any necessary testing.

Criterion 2.2.4

The safety report should show that there is a system in place to ensure the continued safety of the installations based on the results of periodic examinations and maintenance.

Evidence should be presented to show that defects detected during maintenance or examination are properly assessed by a competent person to determine their significance and appropriate action taken.

2.5 Modification:

Criterion 2.5.1

The safety report should describe the system in place for ensuring modifications are adequately conceived, designed, installed and tested.

The safety report should show that there is a system in place to deal with all modifications on the establishment. Those modifications to a process and its associated equipment, to structures (including warehouses) or to operations and procedures that could affect the safety of the installation should be subject to a formal modification system. This includes both hardware (e.g. pumps, piping arrangements, structures) and software (e.g. control system software, operating systems). Decommissioning of facilities is also included under this heading.