Version 2

ASSESSMENT OF COMAH SAFETY REPORTS
MECHANICAL ENGINEERING ASPECTS

Section Paper

Background

This paper was written to promote a consistency of approach by Mechanical Engineering Assessors in the application of the Technical Assessment Criteria contained in the COMAH Safety Report Assessment Manual. It was based on the analysis of a small number of early COMAH safety reports and the intention had been to revise the paper over time to take account of comments received from assessors. Unfortunately resource constraints have precluded any such revision and there may be some areas where our understanding and approach has developed since the writing of the paper. It should also be recognised that assessment is not always a precise science, and relies on the professional judgement of the assessor taking account of the site specific issues posed by an individual site. Thus the approach described in this paper should not be considered as a prescriptive guide to the assessment process but as indicative of the way in which a Mechanical Engineering Assessor will approach assessment against the Technical Assessment Criteria.

1. Summary

1. This paper outlines the background to the development of the Technical Assessment Criteria contained in the COMAH Safety Report Assessment Manual. It explains how these criteria are intended to be used for the assessment of mechanical engineering aspects of safety reports and provides examples of how they have been applied in practice. This paper is concerned principally with aspects of the safety report assessment process, although the interface with follow-up inspection is considered, where appropriate. This paper does not aim to provide guidance on standards relevant to particular plant, processes or circumstances. Such information is presented elsewhere.

2. The purpose of this paper is to promote consistency of approach amongst assessors. It is anticipated that it will require revision as further experience is gained by HID Discipline Specialists, RSGs and external specialists.

2. Introduction

3. The Council of the European Union adopted Directive 96/82/EC on the control of major hazards involving dangerous substances on 9th December 1996. This Directive (known as Seveso II) is implemented in the UK as The Control of Major Accident Hazard Regulations 1999 (COMAH), which came into force on 1st April 1999 [1].

4. One of the main features of COMAH is the requirement for operators of top-tier sites to produce a safety report. The key requirement of a safety report is to demonstrate that all measures necessary have been taken to prevent major accidents and to limit the consequences to people and the environment (COMAH Regulations 7, 8 and Schedule 4). The Competent Authority (CA) has corresponding duties to communicate the conclusions of it's examination of the safety report to the operator and to prohibit the operation of the site if the measures taken by the operator are seriously deficient (COMAH Regulations 17 and 18).

5. The CA has developed criteria to assist with the assessment of safety reports against the requirements of COMAH Schedule 4 and procedures for the manage-

ment of the assessment process. These assessment criteria and procedures are contained in the COMAH Safety Report Assessment Manual (SRAM) [2]. The SRAM has been made publicly available via the HSE website [3]. Additional guidance to industry concerning the contents of safety reports has also been published [4].

6. The CA will appoint an assessment team for each COMAH safety report consisting of inspectors from HSE and EA/SEPA. Assessment teams will be formed to provide an appropriate range of specialist skills, depending on the complexity of the establishment. Members of the multi-disciplinary assessment team will use the assessment criteria set out in Part 2 of the COMAH SRAM to guide their assessment. The assessment criteria are structured to cover the following topics:

- Description of the establishment
- Predictive aspects
- MAPP and Safety Management Systems
- Technical aspects
- Emergency response

7. Each member of the assessment team is required use the relevant assessment criteria to produce 3 outputs:

- Identify if there are any series deficiencies in the measures taken
- Identify whether the required demonstrations have been made
- Identify issues to be taken forward in the inspection programme

8. Matters relevant to Mechanical Engineering Systems are dealt with under technical aspects and are contained in the Technical Assessment Criteria.

3. Development of the Technical Assessment Criteria

9. Technical Assessment Criteria were developed to assist with the assessment of the following demonstrations, set out in COMAH Schedule 4, Part 1:

> *that the necessary measures have been taken to prevent major accidents and to limit their consequences for persons and the environment; and,*
>
> *that adequate safety and reliability have been incorporated into the design, construction, operation and maintenance of any installation and equipment and infrastructure connected with it's operation which are linked to major hazards within the establishment.*

10. The Technical Assessment Criteria were designed to be used by three primary groups: Process Safety Specialists, Controls Systems Specialists and Mechanical Engineering Specialists. It was decided at the outset that the Technical Assessment Criteria should form an integrated set, giving maximum flexibility to how they might be used in practice. The criteria were drafted by a CHID working group containing the necessary mix of disciplines, plus the services of a large engineering consul-

tancy and a secondee from a major petrochemical company. The draft criteria were subject to the usual internal and external consultation and appear in Part 2 Chapter 5 of the SRAM (reproduced for convenience in Annex 1).

11. In formulating the Technical Assessment Criteria, the development team drew on past experience both within HSE and externally [5, 6, 7 and 8]. The objective was to develop a set of criteria which were flexible enough to be applied to any COMAH establishment. Whilst achieving sufficient consistency of approach by assessors, without unduly limiting their discretion and professional judgement. The format of the Technical Assessment Criteria is consistent with other criteria in the SRAM and comprise a series of 23 generic criteria, supplemented by explanatory guidance. Neither the criteria nor the explanatory guidance is discipline specific.

12. The Technical Assessment Criteria is supplemented by a further level of guidance (Level 3 Guidance) for use by assessors. This guidance has been developed in conjunction with a major engineering consultancy and is available on the HSE Intranet. The Level 3 Guidance provides summaries of important standards and references, guidance on specific technical measures, reviews of relevant accidents and other helpful documents.

13. The Level 3 Guidance does not however, deal specifically with use of the criteria by Mechanical Engineering Specialists or with the outputs from the assessment. Also, since the Technical Assessment Criteria and supplementary Guidance are designed to be applicable to the whole range of COMAH sites, they must be applied with discernment. It is the purpose of this paper to expand on these issues.

4. Mechanical Engineering Technical Assessment - A Model

14. It is useful for the Mechanical Engineering Assessor to have an overall framework or model in which to consider a safety report. One such model is illustrated in Fig 1.

15. An important philosophy underpinning the assessment of hazardous installations is the prevention of loss of containment. The avoidance of loss of containment relies primarily on the integrity of the containment in which the hazardous materials are held. The mechanical integrity of the containment boundary thus forms the core issue for consideration by the Mechanical Engineering Specialist.

16. The issue of Mechanical Integrity can itself be subdivided into issues of Initial Integrity and Continuing Integrity. Adequate initial integrity is delivered by adherence to suitable design principles, often embodied in codes and standards. Full consideration having been taken of design details, operating and fault conditions, materials properties and potential failure modes. Related issues include the provision of protective systems and the design of any secondary containment. Delivery of the design intent is provided by suitable controls on manufacture (particularly welding) followed by appropriate inspection and testing.

17. Following a consideration of the initial integrity, attention must be turned to the continuing integrity of the containment, throughout it's service life. This is ensured

by; operating the plant within the limits for which it was designed; by carrying out appropriate maintenance and through periodic examination by a competent person, to identify significant in-service degradation. Finally, procedures must be in place to ensure that modifications to the plant will not compromise the integrity of the containment.

18. The concepts of initial and continuing integrity may thus be mapped directly onto the plant life cycle, as indicated in Fig 1. This is convenient, since the plant life cycle also forms the basis for the structure of the Technical Assessment Criteria (see Annex 1), which are used to assess the Technical Measures described in the safety report.

19. Since the Technical Assessment Criteria form an integrated set (e.g. they also include Control Systems and Process Safety issues) not all will be equally applicable to Mechanical Engineering issues. Only those criteria which are likely to be applied in detail by the Mechanical Engineering Specialist are listed in Fig 1.

5. Top Level Criteria

20. The structure of the Technical Assessment Criteria is illustrated in Annex 1. The criteria are headed by two top level criteria:

Criterion 5.1 - ***The safety report should show a clear link between measures taken and the major accident hazards described.***

Criterion 5.2 - ***The safety report should demonstrate how the measures taken will prevent foreseeable failures which could lead to major accidents*.**

21. Although these two top level criteria are not specifically concerned with the assessment of Mechanical Engineering issues, they are nonetheless important and should be used.

22. In order to assess the significance of the technical measures described in the safety report, it is necessary to have a clear understanding of how major accidents might occur, their likelihood, their consequences and how the various measures in place defend against them. This is the key to identifying assessment priorities and ensuring a proportionate response. Criterion 5.1 and the supporting guidance is designed to assess if the safety report delivers a satisfactory analysis.

23. Criterion 5.2 is the top level criterion under which subordinate criteria for design, construction, operation, maintenance and modification are brigaded together. This criterion is a convenient place for the assessor to identify key issues for the assessment and to summarise the overall findings.

24. The Mechanical Engineering Specialist should use the findings from the hazard identification process to identify mechanical systems which are important to the safety of the installation. This will undoubtedly include: containment structures for hazardous substances (e.g. pressure systems, tanks, pipework, seals, etc.); protective systems (e.g. PRVs); secondary containment (e.g. bunds) and equipment whose reliability is important to safety (e.g. pumps, compressors, ESDVs, etc.).

25. Priority should be given to systems and elements which are described in the various MA scenarios, provided that the safety report is sufficiently comprehensive (e.g. provided criterion 5.1 is satisfied). Where there is any doubt of the completeness or suitability of the presentation given in the safety report, views should be sought from the Predictive Assessor. If the risk assessment provided is insufficient for the purposes of prioritisation and it is not appropriate to reject the report, then the Mechanical Engineering Specialist will need to set assessment priorities based on his/her own experience and knowledge. The assessment record should reflect this.

6. Design Criteria

Criterion 5.2.1.1 - ***The safety report should show that the establishment and installations have been designed to an appropriate standard***

26. This criterion presents a number of principles which complement other more specific design criteria. The principle of most relevance to Mechanical Engineering Assessors is that concerning the avoidance of loss of containment.

27. This criteria will be satisfied from the mechanical engineering perspective if the MA scenarios presented deal with loss of containment and set out the technical measures which avoid and/or mitigate it.

28. Detailed assessment of the technical measures specified can generally be considered under the more specific design criteria, such as 5.2.1.7.

Criterion 5.2.1.2 - ***The Safety report should show that a hierarchical approach to the selection of measures has been used***

29. The safety report should demonstrate that priority has been given to the elimination of hazards, in preference to a reliance on control measures. Consideration of this criterion is likely to be relevant to all disciplines, including mechanical engineering.

30. This criterion is mainly applicable to pre-construction safety reports, where it is practicable to influence the design concept. It should always be applied in such cases. It will also be relevant to modification reports, where significant design changes are involved.

31. Exceptionally, this criterion may be applied to existing establishments, where the report is clearly at odds with accepted standards, (Annex 2, Example 1).

Criterion 5.2.1.3 - ***Layout of the plant should limit the risk during operations, inspection, testing, maintenance, modification, repair and replacement***

32. This criterion is concerned with all aspects plant layout and is relevant to all types of safety report.

33. It should be applied by Mechanical Engineering Assessors, where there are concerns regarding the location of mechanical equipment (Annex 2, Examples 2) and 3).

34. Evidence that these matters have been considered in the design will usually be sufficient for the purposes of assessment. Specific doubts concerning the positioning and accessibility of plant should generally be clarified at the follow-up inspection.

Criterion 5.2.1.4 - ***Utilities that are needed to implement any measure defined in the safety report should have suitable reliability, availability and survivability***

35. This criterion will be relevant to Mechanical Engineering Assessors where the failure of water, steam or air systems may lead to a MA and should be applied to all types of safety report.

36. Information concerning the design of such systems need only provide a description in general terms and specifications such as operating pressures and temperatures are not usually required. The evidence presented should demonstrate that the systems are capable of performing their required function under all foreseeable conditions. Assessment should focus on the measures taken to prevent loss of the utility or mitigate the consequences (Annex 2, Example 4).

37. This criterion need not be applied where the safety report demonstrates (e.g. by reference to a HAZOP) that loss of utilities will not lead to a MA.

Criterion 5.2.1.5 - **Th*e Safety report should show that appropriate measures have been taken to prevent and effectively contain releases of dangerous substances***

38. This criterion addresses numerous issues concerning the measures taken to prevent and contain releases and is applicable to all types of safety report. Issues relevant to mechanical engineering assessment centre on the integrity of joints and seals, temporary connections and the integrity of secondary containment.

39. When considering the integrity of joints, particularly in pipework, the assessor will need to carefully consider the nature of the substance contained. Toxic materials requiring a different philosophy from flammables, (i.e. joint minimisation verses the convenience of flanged connections). Assessors should be guided by relevant published guidance. The demonstration need not provide specific reference to detailed technical specifications, although general information should be provided to indicate that flanges and other joints have been adequately designed. The demonstration should also address the measures taken to ensure flanged connections and other joints are properly made. See Annex 2, Example 5.

40. A suitable demonstration should be provided for seals, where failure could lead to a MA, for example water seals on gas holders. The safety report is unlikely to contain technical details of seals on rotating machinery, floating roofs etc.. In such cases, assessment should be confined to potential causes of seal failure and the

identification of critical areas for inclusion in the follow-up inspection. See Annex 2, Example 6.

41. Temporary connections will include flexible hoses and similar equipment used for transfer operations. The design of flexible hoses etc. is considered under 5.2.1.7.

42. Secondary containment should be assessed for it's adequacy (e.g. the contained volume within a bund). See Annex 2, Example 7. The integrity of the secondary containment is considered under 5.2.1.7.

Criterion 5.2.1.6 - *The safety report should show that all foreseeable direct causes of major accidents have been taken into account in the design of the installation*

43. This criterion specifies a series of direct causes of loss of containment, most of which should be considered by Mechanical Engineering Assessors, to a greater or lesser degree. This criterion is applicable to all types of safety report.

44. The degradation mechanisms; corrosion, erosion and vibration (fatigue) merit particular attention. The vulnerability of containment to impact, overpressure and temperature effects should also be considered in detail. External loading is dealt with at 5.2.1.8. Defective equipment issues are considered under 5.2.4.3. Wrong equipment and human error issues are likely to be considered by other assessors.

45. The demonstration should be made in sufficient detail to show that credible direct causes of loss of containment have been identified and that the prevention/mitigation measures in place are appropriate. See Annex 2, Examples 8, 9 and 10.

Criterion 5.2.1.7 - *The Safety report should show how structures important to safety have been designed to provide adequate integrity*

46. The key purpose of this criterion is to verify that engineering structures have been designed with adequate initial integrity. This criterion is particularly relevant to the Mechanical Engineering Specialist and is unlikely to be applied by other assessment team members. It should be applied to reports for both new and existing installations.

47. When considering the coverage of the information provided, the assessor should be guided by the analysis of MA scenarios. Particular attention should therefore be given to structures which contain hazardous substances, where failure may lead to a significant release. Usually, evidence need only be provided for major vessels and pipework. It is unlikely that evidence will need to be presented for components such as flanges, pumps and valves, unless they feature in the MA scenarios [Annex 2, Example 11]. Other types of structure should be included, where the arguments presented place reliance on their integrity, such as control rooms, bunds and foundations [Annex 2, Example 12].

48. In general, adequate initial integrity will be demonstrated simply by reference to national or international codes and standards. In such cases it will be sufficient for

the safety report to give the reference, the principle design parameters (design pressure, design temperatures capacity, etc.) and category of construction, if applicable (e.g. BS 5500, Category 1) [Annex 2, Example 13]. In certain cases integrity issues may extend to the function of the equipment as well as it's strength (e.g. pig traps closure interlocks [Annex 2 Example 14]).

49. Where in-house codes and standards are called up, it will be necessary to determine their pedigree. Often, such in-house standards are based closely on well known standards. If this is known to be the case, they may be accepted without further enquiry. Otherwise, it will be necessary request additional information, which may involve detailed assessment of the relevant documents. If this is the case, findings should be shared with Mechanical Engineering Specialist colleagues to minimise duplication of effort.

50. In some cases, the structure may not have been designed to a code or standard and/or the relevant design parameters may not be known. In such cases the company should be pressed to carry out a design review, or similar work. Absence of information may not be a significant issue in certain cases. Low pressure gas holders are a typical example [Annex 2 Example 15].

51. Areas for special attention are listed in the guidance to the criteria, such as mixing of design codes, novel designs and non-standard approaches to demonstrating integrity. In general, insufficient information will be given in the safety report for a full assessment and these issues will need to be taken forward to the inspection programme [Annex 2, Example 16].

52. Where evidence is provided for the integrity of civil structures which is outside conventional standards or norms, or in cases of any doubt, a Civil Engineering Specialist should be consulted.

<u>Criterion 5.2.1.8</u> - *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*

53. The purpose of this criterion is to identify and assess the various loading conditions which may compromise the integrity of the containment. This criterion is likely to be applied exclusively by Mechanical Engineering Assessors and is applicable to all types of safety report.

At the most basic level, it will be simply necessary to compare design conditions with the expected operating conditions and to assess the margin, [Annex 2, Example 17]. Where the safety report indicates (or the assessors thinks) that process upset, shut down upset etc. may generate more extreme conditions, these should also be assessed.

54. The amount of evidence presented should be proportionate to the risk and complexity of the process. Often the assessment carried out against criteria 5.2.1.6 and 5.2.1.7 will have also adequately covered the issues addressed by this criterion.

<u>Criterion 5.2.1.9</u> - *The Safety report should show that materials of construction used in the plant are suitable for the application*

55. The purpose of this criterion is ensure that an appropriate degree of attention has been given in the safety report to the issue of materials selection. This criterion is likely to be applied exclusively by Mechanical Engineering Assessors. It is applicable to all types of safety report, but is likely to figure more prominently in the case of a pre-construction safety report..

56. The extent to which this criterion should be applied will depend on the hostility of the operating environment and the operating conditions. For example, high temperature operation in a corrosive environment will clearly merit attention, since correct materials selection is paramount.

57. If the duty is non- aggressive, the assessment carried out against criterion 5.2.1.7 will also have adequately covered the issues addressed by this criterion, where materials have been selected in accordance with the requirements of a recognised code.

58. If materials selection is an important issue, then an indication in the safety report that this matter has been considered in a systematic manner will usually be sufficient. The expectation is not for materials specifications to be catalogued for the whole plant. However the assessor should ensure that the safety report presents a consistent picture [Annex 2, Example 18].

59. Detailed issues concerning the suitability of particular materials for use in specific circumstances should be carried forward to the inspection programme.

<u>Criterion 5.2.1.10</u> - *The Safety report should show that adequate safeguards have been provided to protect the plant against excursions beyond design conditions*

60. This criterion is likely to be primarily applied by Process Safety and Control Systems Assessors. It is applicable to all types of safety report.

61. Those elements of the Criterion which concern the consideration of operating limits etc. will have been considered by the Mechanical Engineering Assessor under 5.2.1.7 and 5.2.1.8.

62. Paragraph 59 of the guidance to the criterion deals with the provision of pressure relief. The Mechanical Engineering Assessor should ensure that appropriate provision has been made for pressure/vacuum relief, [Annex 2, Example 19]. Particularly the specification of set pressures [Annex 2, Example 20] and where the nature of the process fluid may compromise effective operation.

63. The Process Safety Assessor will carry out any detailed assessment of the relief and disposal system.

<u>Criterion 5.2.1.11</u> - *The safety report should describe how safety-related control systems have been designed to ensure safety and reliability*

64. This criterion need not be applied by Mechanical Engineering Assessors.

<u>Criterion 5.2.1.12</u> - *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*

65. This criterion need not be applied by Mechanical Engineering Assessors.

<u>Criterion 5.2.1.13</u> - *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*

66. In the majority of cases, this criterion need not be applied by Mechanical Engineering Assessors.

67. An exception may need to be made where there is clear evidence that non-electrical equipment may generate an ignition source and that a tangible risk is posed to the safety of the plant. Alternatively, an assessment may need to be made where the safety report makes reference to standards applied to non-electrical equipment (ATEX Directive). In which case the correct reference to appropriate standards may need to be verified.

<u>7. Construction Criteria</u>

<u>Criterion 5.2.2.1</u> - *The safety report should show that the installations have been constructed to appropriate standards to prevent major accidents and reduce loss of containment*

68. This criterion concerns the standards of construction used for hazardous installations. The Mechanical Engineering Assessor should apply this criterion to the construction of engineering structures, with particular attention being focused on structures containing hazardous substances.

69. Criterion 5.2.2.1 should always be applied to pre-operation safety reports. It will also be appropriate to apply the criterion to pre-construction safety reports in general terms, so as to gain assurance that the construction phase will be effectively managed. (Annex 2, Example 21)

70. The extent to which this criterion should be applied to existing installations requires careful consideration. The thoroughness of the demonstration required will generally be governed by the extent to which reliance is placed on measures to ensure adequate initial integrity. For example, the safety of a 2 year old installation which has not yet undergone a full in-service examination programme (see criterion 5.2.4.3) will still depend in large measure on the level of integrity delivered by the construction phase. In contrast, a gas holder which was constructed 80 years ago will not (Annex 2, Example 22). Indeed, it is unlikely that the evidence described in the guidance to criterion 5.2.2.1 will be available for existing older plant.

71. There is a close relationship between this criterion and criterion 5.2.1.7. Codes and standards for containment such as vessels and pipework cover both design and manufacture/construction. In such cases, little additional assessment will be required, over and above that done under 5.2.1.7.

Criterion 5.2.2.2 - ***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***

72. This criterion is a follow-up to criterion 5.2.2.1 and the comments made above also apply here.

73. However, even for existing older plant, para 82 of the guidance to criterion 5.2.2.2 [2]. should still be satisfied and reference made to compliance with code requirements (Annex 2, Example 23). It is accepted that even this limited information may not be available in exceptional cases, such as for low pressure gas holders.

8. Operation Criteria

Criterion 5.2.3.1 - ***The safety report should show that safe operating procedures have been established and are documented for all reasonably foreseeable conditions***

74. This criterion is applicable to pre-operation safety reports and safety reports for existing installations. In general, this criterion will be applied by other assessors and there is also a considerable overlap with the SMS assessment criteria.

75. It will be usually only be necessary for the Mechanical Engineering Assessor assess the evidence that mechanical plant and equipment are always operated within safe limits.

9. Maintenance Criteria

Criterion 5.2.4.1 - ***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***

76. The purpose of this criterion is to enable to assessment of maintenance management systems. Assessment against this criterion should normally form part of the target agenda for assessment. It is appropriate to apply this criterion to safety reports for existing installations. It may also be applied to pre-operation safety reports, although allowance will need to be made for the fact that the maintenance system will not be in operation (Annex 2, Example 24). This criterion is not applicable to pre-construction safety reports. It is anticipated that both Mechanical Engineering and Electrical/Control systems Assessors will apply this criteria to their respective areas of interest.

77. The assessment criteria distinguish between maintenance (this criterion) and in-service examination (criterion 5.2.4.3.). This criterion is aimed at routine activities to monitor, repair or replace mechanical plant and equipment and includes for exam-

ple, vibration monitoring of rotating plant. Issues relevant to containment integrity (in-service examination) should be addressed under criterion 5.2.4.3.

78. In general it will be appropriate for the assessment to concentrate on the key maintenance activities identified by the safety report. Evidence of the existence of appropriate procedures will normally suffice, with detailed points being carried forward to the inspection programme. Detailed procedures should only be pursued if weaknesses are identified which could lead to a possible MA. Further enquiries may need to be made where there is a blanket reference to maintenance standards or procedures, in a manner which does not discriminate between safety critical activity and plant maintenance carried out solely for the purpose of production efficiency (Annex 2, Example 25).

Criterion 5.2.4.2 - ***The safety report should show that there are appropriate procedures for maintenance that take account of any hazardous conditions within the working environment***

79. This criterion is concerned with maintenance work in hazardous conditions. It must be remembered however that the safety report is concerned only with major accidents, hence the scope of this criterion should be interpreted accordingly.

80. Usually, this criterion need only be applied by Mechanical Engineering Assessors to the extent of identifying issues for the inspection programme, where specific hazardous activities are identified.

Criterion 5.2.4.3 - ***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***

81. The purpose of this criterion is to guide the assessment of systems in place for the periodic in-service examination of safety critical plant. Assessment against this criterion should normally form part of the target agenda. It is appropriate to apply this criterion to existing installations. It may also be applied to pre-operation safety reports, to the extent of ensuring that adequate provision has been made for future in-service examination (Annex 2, Example 26). This criterion is not applicable to pre-construction safety reports.

82. This criterion should be applied by Mechanical Engineering Assessors to containment structures and particularly to pressure systems. All containment structures should be included, where failure may lead to a MA. For example atmospheric storage vessels containing dangerous substances; or steam boilers, where failure may act as an accident initiator.

83. It is likely that little justification for the inspection frequencies used will be offered. In which case the assessor should refer to industry norms. Where the operator has implemented a Risk Based Inspection system, the inspection frequencies adopted may differ substantially from current published guidance. In which case the matter should be investigated during the follow-up inspection.

84. It will not usually be possible to make a judgement on the suitability of specific inspection methods, on the basis of information provided in the safety report. Where an issue is identified, this should be reserved for the follow-up inspection. (Annex 2, Example 27).

Criterion 5.2.2.4 - ***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***

85. This criterion is a follow-up to criterion 5.2.2.3 and the comments made at paragraphs 81 and 82 are equally applicable.

86. This issue was included as a separate criterion to highlight it's importance and because this matter is often overlooked. (Annex 2, Examples 28 and 29).

87. Where a 3rd party performs the competent person duty, it may be sufficient for the safety report to indicate that reliance is placed on their expert judgement concerning the significance of any defects found.

10. Modification Criteria

Criterion 5.2.5.1 - ***The safety report should describe the system in place for ensuring modifications are adequately conceived, designed, installed and tested***

88. The purpose of this criterion is to assess whether there are sound procedures for managing change in the plant design. As such, this criterion is applicable to safety reports for existing installations and for pre-operation safety reports. This criteria should always be included in the target agenda.

89. In general, this criterion will also be applied by other assessors and there is also a considerable overlap with the SMS assessment criteria. The Mechanical Engineering Assessor should examine the issues described in the guidance to the criterion, to ensure that the procedures and systems described provide adequate coverage for mechanical plant and equipment. The output from the mechanical engineering assessment will contribute to the overall view formed by the assessment team.

11. Conclusion

90. This paper was developed from an analysis of a small number of early COMAH safety reports, for the purposes of promoting consistency of approach by Mechanical Engineering Assessors, in applying the Technical Assessment Criteria.

91. Where possible, examples have been given to indicate the extent of information required; to illustrate where additional information has been requested and where issues have been carried forward to the follow-up inspection programme.

92. It is intended that this paper should be revised in due course, on the basis of comments received from assessors. So as to achieve an convergence of approach, as far as it is practicable.

12. References

1. A guide to the Control of Major Accident Hazards Regulations 1999. Publication L111.

2. COMAH Safety Report Assessment Manual.

3. www.hse.gov.uk/chid/comah2/index.htm

4. Preparing safety reports: Control of Major Accident Hazards Regulations 1999. Publication HSG190

5. Assessment Principles for Offshore Safety Cases. Publication HSG181.

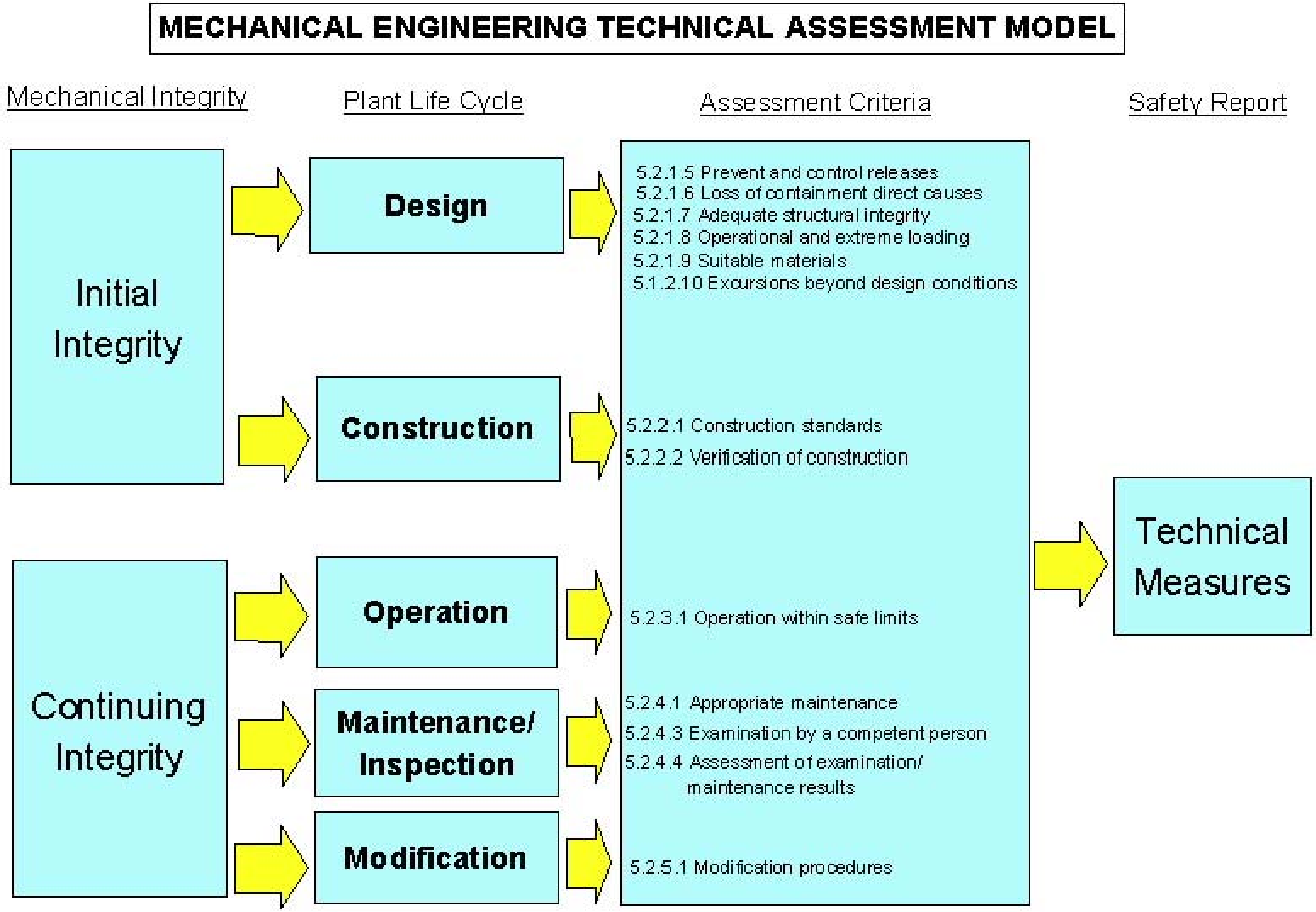
6. Safety Assessment Principles for Nuclear Plants. HSE Nuclear Safety Division.

7. Guidance for Specialist Inspectors on the Technical Assessment of CIAMH Safety Reports. OC 317/6 (cancelled).

8. AVRIM2. Dutch Ministry of Social Affairs.

9. HSE Intranet. http://intranet/drafts/chid_l3guidce/index.htm

Fig 1: Mechanical Engineering Technical Assessment - A Model



Annex 1

Technical Assessment Criteria

Top Level Criteria

Criterion 5.1 - The Safety report should show a clear link between the measures taken and the major accident hazards described

Criterion 5.2 - The safety report should demonstrate how the measures taken will prevent foreseeable failures which could lead to major accidents

5.2.1 Design

Criterion 5.2.1.1 -The safety report should show that the establishment and installations have been designed to an appropriate standard

Criterion 5.2.1.2 - The Safety report should show that a hierarchical approach to the selection of measures has been used

Criterion 5.2.1.3 - Layout of the plant should limit the risk during operations, inspection, testing, maintenance, modification, repair and replacement

Criterion 5.2.1.4 - Utilities that are needed to implement any measure defined in the safety report should have suitable reliability, availability and survivability

Criterion 5.2.1.5 - The Safety report should show that appropriate measures have been taken to prevent and effectively contain releases of dangerous substances

Criterion 5.2.1.6 - The safety report should show that all foreseeable direct causes of major accidents have been taken into account in the design of the installation

Criterion 5.2.1.7 -The Safety report should show how structures important to safety have been designed to provide adequate integrity

Criterion 5.2.1.8 - 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

Criterion 5.2.1.9 - The Safety report should show that materials of construction used in the plant are suitable for the application

Criterion 5.2.1.10 - The Safety report should show that adequate safeguards have been provided to protect the plant against excursions beyond design conditions

Criterion 5.2.1.11 - The safety report should describe how safety-related control systems have been designed to ensure safety and reliability

Criterion 5.2.1.12 - 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

Criterion 5.2.1.13 - 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

5.2.2 Construction

Criterion 5.2.2.1 - The safety report should show that the installations have been constructed to appropriate standards to prevent major accidents and reduce loss of containment

Criterion 5.2.2.2 - 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

5.2.3 Operation

Criterion 5.2.3.1 - The safety report should show that safe operating procedures have been established and are documented for all reasonably foreseeable conditions

5.2.4 Maintenance

Criterion 5.2.4.1 - 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

Criterion 5.2.4.2 - The safety report should show that there are appropriate procedures for maintenance that take account of any hazardous conditions within the working environment

Criterion 5.2.4.3 - 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

Criterion 5.2.2.4 - 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

5.2.5 Modification

Criterion 5.2.5.1 - The safety report should describe the system in place for ensuring modifications are adequately conceived, designed, installed and tested.

Annex 2

Examples of evidence from COMAH Safety Reports

Example 1

An installation handling ethylene oxide claims compliance with the relevant CIA guidance. But the installation stores ethylene oxide at ambient temperature, whereas the CIA guidance recommends refrigerated storage, thus eliminating hazards associated with pressurised storage. Further information was therefore requested asking the operator to justify why refrigerated storage had not been adopted and requesting details of any additional measures in place.

Example 2

Safety report for atmospheric storage tanks containing a flammable substance. The report indicates that transfer pumps have been located outside the bunded area in order to minimise potential sources of ignition. The pump areas are provided with a separate sump. Demonstration satisfactory.

Example 3

The plant layout philosophy described in a pre-construction safety report does not consider maintenance activity. Request made for additional information.

The response received confirmed that the design layout philosophy did include maintenance activity and plant inspection, but that reference to these issues had been omitted in error. Information provided claimed that the design procedure calls for formal layout reviews and that check list headings include maintenance. No further action proposed.

Example 4

A gas holder is equipped with trace steam heating of the water seals. Freezing of the water seals can lead to a loss of containment. Water seals are also inspected during extreme cold weather. An alarm is activated at system control should the boiler become unavailable. Further details concerning the design of the steam heating system were requested.

Additional information indicated that steam is piped from the boiler to a main around the gas holder. Steam is injected into the water seal via a flexible hose at three separate points around the circumference. Each hose is equipped with an anti-syphon valve to prevent water being withdrawn. A visual inspection of the hoses and a check that anti-syphon valve is clear is carried out weekly. Correct operation of anti-syphon valves is checked annually.

Written demonstration is satisfactory. The condition of the steam heating hoses and review of relevant maintenance records carried forward to the inspection plan. Also carried forward was a review of the system for initiating extreme weather inspections.

Example 5

Safety report for a natural gas storage import and export system states that all piping is fully welded with flanged connections where necessary. A follow-up question was submitted to clarify “where necessary”.

The response provided stated that flange joint were kept to a minimum and generally restricted to equipment/skid connections and control valves. Pipework connected to equipment/skids to be subjected to stress analysis which will result on minimum loads and moments exerted on flanged joints. Procedure will ensure that all flange bolts have the correct torque during construction. Satisfactory evidence.

Example 6

An assessment considered the integrity of seals on transfer pumps from a storage tank, but no information was provided. Request for information made to clarify the type of seals used and the measures in place to reduce the likelihood of seal leaks and fires.

Response indicated that low sill and drainage had been provided for the transfer pump area. High hazard pumps are glandless magnetic drive and positive displacement pumps have downstream relief valves. Satisfactory evidence, but maintenance regime for high risk transfer pumps considered for follow-up inspection.

Example 7

Safety report claims that the bunds around a group of floating storage roof tanks complies with HSG 176, para 140. Calculations were also provided on how the bund capacity had been calculated. Satisfactory evidence.

Example 8

Safety report simply states that internal corrosion allowances are adequate. Also, natural gas is stored in a cavern, mined in salt strata. There is thus a theoretical possibility of internal corrosion caused by contaminated wet gas following gas extraction from the cavern. This issue is not addressed by the safety report. Further information requested on these issues.

Additional information states that for dry sweet gas systems a corrosion allowance of 1.5mm has been selected. For wet, sweet natural gas systems an estimate was made using a correlation for wet CO_2 corrosion. 3mm selected giving a design life of 25 years. Previous operating experience indicates that brine entrainment into the gas stream is not feasible and no accelerated corrosion rates have been experienced. Acceptable evidence, but a check of corrosion at the condensate receiver discharge to be considered for follow-up inspection.

Example 9

Safety report for a natural gas storage import and export system states that erosion is not a problem. The reason given is that pipes are sized to give velocities for minimum erosion and that the gas is clean. Satisfactory evidence.

Example 10

A generic proof pressure test argument is referred to, to discount the possibility of fatigue failure of HP natural gas pipework. Additional details were requested, since this is a novel approach and merits further attention.

The additional information provided called up IGE/TD/9 rather than giving additional details of the proof test argument. Reference to IGE/TD/9 indicated that this standard is limited to drawing the reader's attention to the possibility of fatigue. The safety report thus failed to make an adequate demonstration that fatigue had been adequately assessed by the operator. However, the safety report was accepted, since HSE knowledge of the operator indicated that fatigue failure of HP pipework was not known to be a problem. Recommendation made that the follow-up inspection further considers the operating history and the possibility of fatigue.

Example 11

Pre-construction safety report cites small bore pipework (size range undefined) as a credible source of a jet fire. Although jet fires have been identified as one of the main types of MA scenarios, no further consideration of measures taken to reduce the likelihood of small bore pipework failure have been presented. Further information requested concerning design and construction standards to be used for the installation of small bore pipework.

Written response states that small bore pipework has been designed to ANSI B31.3 and socket welded joints on all size lines to be 100% radiographed. Response also indicates that jet fire from small bore pipework is in fact unlikely to lead to escalation due to the provision of a vent and blowdown system.

Residual questions concerning the integrity of small bore pipework carried over to follow-up inspection.

Example 12

Pre-operation safety report concerning the design of a methanol floating roof storage tank. The performance of the roof seal could be compromised by distortion of the tank, so check provision of adequate foundations. Calculation sheet provided in the safety report showing details of concrete ring beam with bituminous sand in-fill. Demonstration considered to be made.

The storage tanks were provided with secondary containment in the form of bund walls. No information was provided concerning their design. A request for further information was made. Information provided indicated that the bund walls had been designed to withstand the full hydrostatic pressure from complete loss of the largest vessel. No further action.

Example 13

Pre-operation safety report states that “ storage and transfer pipes are designed to industry standards”. Request for additional information made. Response indicated design to AMSE B31.3 and design pressures were provided. Design temperatures not provided, but was not a significant safety issue in this case, since operation is at ambient temperature.

Example 14

Pre-operation safety report indicated the provision of pig traps on various product transfer lines. Request for additional information made concerning the design standards used for the pig traps and the means for isolation prior to opening the closure door.

Additional information referred to an in-house specification for the pig trap. Additional information also described the provision of an interlock to prevent opening of the pig trap under pressure.

A review of pig trap design and operational procedures was carried forward to the follow-up inspection plan.

Example 15

Safety report for a low pressure gas holder built in 1926. No design information was provided for the gas holder itself. It was not constructed to a code and records for the design do not exist. Of particular concern was the lack of any information on design pressure. The design of water seal gas holders results in the internal pressure being self limiting to nominal maximum operating pressure of 32.5 mbar. But friction in the roller guide system could cause the pressure to rise to 65 mbar before water is ejected from the cup seals.

A request for further information was made, indicating that whilst it is accepted that the long service history would have proven the design, certain design data should be made available in the report. Particularly the gas holder design pressure.

The response obtained confirmed that the original design pressure was unavailable, but that the gas holder was considered to have a safety factor of 4. No further action was considered to be appropriate.

Example 16

Refinery safety report describes a box repair on FCCU catalyst riser. The riser had eroded due to action of the following catalyst. No information was given to indicate if this was a short term fix, or a long term solution. Further information was requested to confirm that the repair conformed to ASME VIII, since the design details described do not fall within ASME design by rule (and in particular, how was the code applied to design the box-to-riser attachment welds). Copies of the repair documentation and risk assessment (referred to in the report) were requested. This issue was carried forward to the follow-up inspection programme.

Example 17

Ethylene oxide storage vessels are claimed to be designed and operated at a minimum temperature of 0^oC, but the lowest recorded temperature at the site is given as -9^oC.

This may not necessarily be a problem, due to the effects of thermal inertia and insulation on the vessel. But this discrepancy warrants further explanation in the safety report. Information requested.

Example 18

A safety report makes reference to the use of stainless steel and carbon steel for pipework and reactor vessels having nominally the same duty. The reason for the difference in choice of materials is not explained. Also, CIA guidance on the selection of materials for the containment of ethylene oxide recommends the use of stainless steel. Further information requested from the operator to explain this difference in choice of materials.

Example 19

Floating roof storage tanks containing flammable liquid are fitted with rigid geodesic domes. No evidence is presented to demonstrate that the floating roof/dome interspaced has been vented to prevent a build-up of a flammable atmosphere. The tanks are likely to have external flashing and centre vent to provide circulation, but there is a need to verify this. Request further information concerning measures taken to prevent a build-up of a flammable atmosphere between the floating roof and the dome on methanol tanks.

Additional information and process hazard review indicates that venting of the dome is in accordance with API 650 appendix H and that the dome will vent in the event of an internal explosion. Need to verify that the rupture strength of the dome will not compromise tank integrity, in the event of an internal explosion. But consider this at follow-up inspection.

Example 20

The set pressure of transfer line thermal relief is specified as 8 barg on drawings, vented back to storage tanks, but this is also the normal operating pressure. Request clarification of thermal relief set and operating pressures.

Additional information explains that the pressure margin is provided by line pressure drop. Check settings of thermal relief valves at follow-up inspection. Also, check that relief valves on positive displacement pumps are set less than line pressure.

Example 21

A pre-construction safety report provided no information on the management of the construction phase. Additional information was requested.

Additional information provided indicated the involvement of an engineering insurance organisation, including design verification and construction, plus systems of work and procedures. Project completion and handover documentation and change control procedures were referenced. A review of these documents was suggested to supplement assessment of the subsequent pre-operation report.

Example 22

For a low pressure gasholder safety report, the assessment concluded that the age of the gasholders made detailed consideration of the controls in place during their construction of low importance. Little information is likely to be available. No further action taken.

Example 23

A pre-operation safety report concerns an on-site pipeline used to transfer methanol to a jetty installation. A number of MA scenarios are associated with the integrity of the pipeline, but no information is provided concerning the type and level of post weld NDT carried out.

Additional information received indicated that a minimum of 10% radiography was carried out in accordance with BS 8010. But the pipeline was reportedly designed to ASME B31.3 (possibility of mixing codes).

The effectiveness of post weld inspection and testing in assuring adequate integrity has not been demonstrated, even with the additional information provided. Review at inspection follow-up within the first year and consider in particular the appropriate level of in-service inspection.

Example 24

In the case of a pre-operation safety report, it is stated that maintenance systems are currently under development for the site. Evidence is provided to indicate that plant data manuals contain plant vendors recommendations for maintenance and that reliance will be placed on contractors to proceduralise them. It was indicated that vibration monitoring of transfer pumps would be carried out monthly. Maintenance of pig traps was not discussed nor was non-routine work, such as freeing a trapped pig. Maintenance on site was to be exclusively carried out by contract staff

The evidence provided was not adequate, but was accepted on the basis that this was a pre-operation report and that the plant designer and builder was to be responsible for maintenance during the first year of operation. Maintenance issues would be followed up as part of the inspection programme.

Example 25

Safety report for a low pressure gas holder. The organisation of maintenance for mechanical systems was adequately described and reference was made to IGE/SR/4 and IGE/TD/9 for details of maintenance procedures.

No additional evidence was presented to justify the maintenance regime adopted, and the view was taken that over reliance had been placed on reference to standard codes. The reason was that whilst these codes may well be acceptable, the SR fails to identify those maintenance activities which are important to preventing/limiting MAs and did not attempt to justify the measures taken.

A review of maintenance schedules and documented procedures and records (including fault reporting) was suggested for follow up inspection.

<u>Example 26</u>

Pre-operation safety report for an installation having a floating roof storage tank. The report specifies a 10 yearly inspection period for the tanks and it is stated that a written scheme of examination is to be developed.

Include as a topic for follow-up inspection, but further information also requested to discover if this is an external or an internal inspection, plus information on the expected degradation mechanisms.

<u>Example 27</u>

In a safety report for a refinery FCCU unit, information was provided on a major repair to the catalyst riser section. The repair consisted of a box built around the riser, which would have made conventional inspection difficult. The safety report stated that an acoustic emission (AE) technique had been used.

This is an unusual application of AE and there are doubts that it is suitable as a primary inspection technique. The suitability of AE for the purpose of verifying the integrity of the box repair was carried forward into the follow-up inspection programme.

<u>Example 28</u>

A safety report for an existing batch chemical processing plant gives details of inspection frequencies and techniques, but does not provide any information on the basis for assessing the significance of defects found during maintenance or periodic in-service inspection. For example, the condition of the plant is described as not suffering from significant corrosion. But no indication has been given of the basis for this judgement. Further information was requested.

<u>Example 29</u>

In a safety report for a refinery FCCU unit, no information was provided on the assessment of in-service inspection results. For example, although the safety report stated that thermography is used to assess the condition of the catalyst riser, no reference was made to the existence of threshold temperatures for action, or the establishment of datum levels. Further information was requested.