Guidance for the Management of Legacy Safety Systems

Disclaimer

The Association would welcome any comments on this publication, see http://www.61508.org/contact.htm. Whilst every effort has been made to ensure the accuracy of the information contained in this document, neither The 61508 Association nor any of its members will assume liability for any use made thereof.

Guidance for the Management of Legacy Safety Systems

Introduction

Engineered systems are relied upon for safety in a wide range of work environments. There is however, a general lack of awareness of the exact role played by such systems, and whether adequate safety is, in fact, being achieved. This is particularly true of systems that have been in place for many years.

This document develops the principals identified in the "Legacy Systems Basic Principles for Safety" document to give additional guidance on the management of Legacy safety Systems, focussing on how electrical, electronic, or programmable devices achieve adequate safety in conjunction with other technologies such as mechanical systems and operational expectations.

These guidelines have been produced by The 61508 Association to assist its members and others to consider how to deal with legacy systems. The Association would welcome any comments on this publication, sent to legacy@61508.org.

Intended Audience

This document is intended to be used by managers and technical staff with roles and responsibilities relating to legacy systems.

It will also be of relevance to those that support these roles, including:

- owners
- company, site and operating unit managers
- suppliers of systems, sub-systems and components
- safety assessors
- regulatory authorities
- consulting engineers
- organisations with contractual obligations

Legacy System:
A safety related system which performs one or more safety functions as defined in IEC 61508 but which was designed and installed before the publication and adoption of IEC 61508.

Note: this document applies to systems using technologies such as Electrical, Electronic, Programmable Electronic Systems, mechanical, and hydraulic systems.

SUMMARY

Safety related systems are installed to prevent the plant getting into a state where it presents a hazard to people. The majority of process plants were built prior to 1998 and IEC 61508. In many cases neither the plant nor the safety related equipment has been updated for several years.

What is reasonably practicable can change over time with advances in safety management techniques and in the capabilities of safety technology such as safety related systems. Modern standards such as IEC 61508 provide a more effective benchmark for the management, specification, design, implementation, operation, maintenance and modification of safety-related systems than may have existed when legacy systems were originally put in place. It is appropriate to periodically review both the management of functional safety and the technical suitability of the safety related systems on process plant.

The recognised Standard for functional safety and safety related systems is IEC 61508 or other appropriate sector specific functional safety standards, such as BS EN 61511, 2004, for the process sector. A legacy system is an electrical/electronic/programmable electronic system (E/E/PES) that performs one or more safety functions as defined in IEC 61508 but which does not necessarily meet IEC 61508 and/or related standards because it was designed and installed prior to the introduction of IEC 61508, 1998

The 61508 Association has provided some high level basic principles for the management of legacy systems. The basic principles document highlights 11 key principles associated with the management of legacy systems.

This document provides a guide for a non-nuclear process industry approach to managing legacy systems and builds on the 61508 Association basic principles document.

CONTENTS

Page

1 INTRODUCTION 5
2 SCOPE 5
3 LEGAL REQUIREMENTS 6
4 RESPONSIBILITIES AND ROLES OF THE ORGANISATION MANAGEMENT 7
5 THE IEC 61508 AND IEC 61511 STANDARDS 7
6 IMPLICATIONS FOR LEGACY SYSTEMS 8
7 DETERMINING THE LEVEL OF CONSEQUENCE OR RISK 10
8 REVIEW OF FUNCTIONAL SAFETY MANAGEMENT PROCEDURES 11
8.1 Tolerable Risk Criteria 11
8.2 Management Responsibilities and Roles 12
8.3 Technical Co-ordinator 12
8.4 Change Management 13
8.5 Maintenance and Repair Policies and Strategies 13
8.6 Inspection and Test Policies and Strategies 15
8.7 Safety Related Systems Documentation (Safety File) 16
8.8 Data Collection 18
8.9 Competence Management 19
9 SAFETY RELATED SYSTEMS TECHNICAL SUITABILITY REVIEW 19
9.1 List of Potential Safety Related Systems 20
9.2 Assessment of Representative Sample 23
9.3 Qualitative Consideration of All Safety Related Systems 24
10 ACTION PLAN 25
11 ON-GOING ACTIVITIES 26
11.1 Periodic Audit of the Functional Safety Management Procedures 26
11.2 Periodic Review of Each Safety Related System 26
12 SUMMARY 28
13 REFERENCES 29
14 GLOSSARY OF TERMS 30

FIGURES

1 INTRODUCTION

Safety related systems are installed to prevent the plant entering a state where it presents a hazard to people. The majority of process plants were built prior to 1998 and the publication of IEC 61508. In many cases neither the plant nor the safety related equipment has been updated.

An organisation is responsible for compliance with health and safety legislation which includes reducing risks to people to as low a level as is reasonably practicable (ALARP) and being able to demonstrate that risks to people have been reduced to ALARP. What is reasonably practicable can change over time with advances in safety management techniques and in the capabilities of safety technology such as safety related systems. Modern standards, such as IEC 61508, provide a more effective benchmark for the management, specification, design, implementation, operation, maintenance and modification of safety-related systems than may have existed when legacy systems were originally put in place. It is appropriate to periodically review both the management of functional safety and the technical suitability of the safety related systems on process plant.

The recognised Standard for functional safety and safety related systems is IEC 61508 or other appropriate sector specific functional safety standards. A legacy system is an electrical/electronic/programmable electronic system (E/E/PES) that performs one or more safety functions as defined in IEC 61508 but which does not necessarily meet IEC 61508 and/or related standards because it was designed and installed prior to the introduction of IEC 61508.

The 61508 Association has provided some high level principles for the management of legacy systems. The basic principles document, free to download at www.61508.org, highlights 11 key principles associated with the management of legacy systems.

This guidance document provides a guide for a non-nuclear process industry approach to managing legacy systems and builds on the 61508 Association basic principles document. Here more information is provided on how to manage legacy systems to comply with an organisation's responsibility for health and safety

This document will provide useful guidance to both managers and technical staff with roles and responsibilities relating to legacy systems.

2 SCOPE

A legacy system is an electrical/electronic/programmable electronic system (E/E/PES) that performs one or more safety functions as defined in IEC 61508 but which does not necessarily meet IEC 61508 and/or related standards because it was designed and installed prior to the introduction of the modern standards.

Note: Upgrading of existing systems should follow the concepts of IEC 61508 and/or any appropriate sector standards.

This document provides guidance for people who are responsible for managing, maintaining or operating equipment with legacy systems. It is intended that following the guidance will either ensure the legacy systems continue to provide the necessary risk reduction required to provide a safe working environment or identify any additional risk reduction required.

Functional safety management is: the setting of policy; provision and direction of resources; implementation of practices and procedures; creation and management of documentation and records; review and oversight of activities related to safety related systems (i.e. any system that performs one or more safety functions as defined in IEC 61508), including legacy systems. This document is also relevant to people in managerial positions associated with functional safety management.

3 LEGAL REQUIREMENTS

The Health & Safety at Work Act, 1974 requires that;

- Every employer shall ensure, as far as is reasonably practicable, safety and welfare at work of all employees.
- Every employer shall conduct his undertaking so as to ensure, so far as is reasonably practicable, that persons not in his employment who may be affected thereby are not exposed to risks to their health or safety.

The Management of Health and Safety at Work Regulations 1999 applies to every work activity and requires every employer to undertake risk assessments and record findings.

The Provision and Use of Work Equipment Regulations 1998 (PUWER) came into force on 5th December 1998. In general terms, the Regulations require that equipment provided for use at work is:

- Suitable for the intended use.
- Safe for use, maintained in a safe condition and in certain circumstances, inspected to ensure this remains the case.
- Used only by people who have received adequate information, instruction and training.
- Accompanied by suitable safety measures, e.g. protective devices, markings, warnings.

The PUWER regulations apply to any equipment which is used by an employee at work and a safety related system is regarded as equipment used by Plant Operators.

Safety related systems are covered by the above and hence there is a legal requirement that safety related systems provide an acceptable level of protection to employees. You should ensure that your company practices and procedures can demonstrate compliance with the legal requirements for safety and with any guidance material describing good practice, including such material published by the HSE.

The HSE are the principal enforcement agency for workplace safety and for the risk of harm to people from work-related activities, although the police might well become involved in the case of serious injury or fatality. The HSE bases its regulatory expectations upon legal requirements and has stated that it regards IEC 61508 as its preferred way of meeting the legal requirements in respect of safety related systems.

Hence you should ensure that your company practices and procedures can demonstrate compliance with the legal requirements for safety and with any guidance material describing good practice, including such material published by the HSE.

4 RESPONSIBILITIES AND ROLES OF THE ORGANISATION MANAGEMENT

An organisation is responsible for compliance with health and safety legislation which includes reducing risks to people to as low a level as is reasonably practicable (ALARP) and being able to demonstrate that risks to people have been reduced to ALARP. In order to comply with this in respect of; functional safety; safety related systems; legacy systems; and to comply with the 61508 Association's principles document, the organisation management needs to:

- Define the organisational objectives related to process safety and to safety related systems including legacy systems.
- Determine and define the organisation's tolerable risk criteria for people
- Ensure that appropriate management procedures for safety related systems are in place and are applied, throughout the life of the safety related system.
- Ensure that competent technical and engineering staff are available, aware of their roles and responsibilities and have sufficient resources and authority to carry out their roles and to discharge their responsibilities.

5 THE IEC 61508 AND IEC 61511 STANDARDS

The requirements for safety related systems are defined in three international standards that have been adopted as Euro-Norms and by the BSI as national standards.

These standards are:

- IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems.

- IEC 61511 Functional safety related systems for the process industry sector.
- BS EN 62061 Safety of Machinery: Functional Safety of safety-related electrical, electronic and programmable electronic control systems.

The first is a generic standard and the second is specific to the non- nuclear process industry. The third, BS EN 62061 is primarily aimed at developers and manufacturers of complex machinery. It deals with the Safety-Related Electrical Control Systems (referred to as SRECS) of machines; it also applies to modifications of machinery and related SRECS. Requirements to mitigate risks arising from other hazards are provided in relevant sector standards. For example, where a machine(s) is part of a process activity, the machine electrical control system functional safety requirements should, in addition, satisfy other requirements (e.g. IEC 61511) insofar as safety of the process is concerned. The reader is referred to the standards to understand their scope of applicability.

Both IEC 61511 and BS EN 62061 are daughter standards of IEC 61508 and make reference to IEC 61508. There are, or are being developed, other daughter standards for other specific industries e.g. nuclear and railways. The text in this document refers to IEC 61508 and uses IEC 61508 terminology, but in all cases this should be taken to refer equally to both IEC 61508 and IEC 61511.

The HSE were heavily involved in the development of these standards and have adopted them as the benchmark against which they will measure the performance of organisations (duty-holders) in providing and managing adequate safety related systems. This is encapsulated in a statement from the board of the HSE:

"*IEC 61508 will be used as a reference standard for determining whether a reasonably practicable level of safety has been achieved when E/E/PE systems are used to carry out safety functions. The extent to which Directorates/Divisions use IEC 61508 will depend on individual circumstances: whether any sector standards based on IEC 61508 have been developed and where there are existing specific industry standards or guidelines.*" (HSE Board Paper B/00/105).

The standards cover the whole life cycle of the safety related system and cover operation, maintenance and testing as well as initial risk assessment, design, build, installation, commissioning, and de-commissioning. Thus there are long term implications arising from the standard.

6 IMPLICATIONS FOR LEGACY SYSTEMS

The basic principles for managing legacy systems have been outlined in the 61508 Association basic principles document which includes the following statement:

"*Safety-related systems designed and installed before the publication of IEC 61508 are not required to be replaced or upgraded just because the standard has been published. There may be varying degrees of design information and operational records relating to*

legacy systems which can be used as a source of evidence to assess the adequacy of those systems. The organisation should be able to demonstrate that the measures in place to control the risks of hazardous events are adequate when seen in the light of the standard and the requirements of the law."

This makes it clear that it is not considered essential that legacy systems are brought into full compliance with IEC 61508. Rather it is a matter for reviewing the available evidence and providing a well-justified case for whatever decision is taken; whether it is to leave a legacy system in service indefinitely, to carry out limited modifications or to replace it at an appropriate time. This document describes an approach to the management of legacy systems that complies with the 61508 Association basic principles document, though without retrospectively producing all of the documentation that would have been produced when the safety systems were originally designed and installed had the standard IEC 61508 existed and been followed at the time.

It is thought that the full retrospective application of the standard IEC 61508 to legacy systems will involve companies in a considerable amount of work and expense, whilst providing a minimal reduction in actual risk of harm to humans; such an activity is likely to be counter-productive in risk reduction terms as it would divert limited expert resource away from activities that would deliver greater risk reduction. It should be remembered that the HSE wants to see the expenditure on safety in the areas where it will provide the most benefit, rather than in those areas where the risk is already appropriately managed. This document outlines an approach to managing legacy systems that identifies the areas of most risk and if necessary reduces the risk whilst avoiding effort and documentation that produces little benefit.

It would seem from the above that provided the systems are well managed, perform reliably and risks are at a level comparable with relevant tolerable risk criteria and are ALARP, then the legacy systems can be continued to be used. It is only when these factors are compromised or cannot be demonstrated that the organisation will be required to consider whether the equipment should be replaced. This document is concerned with a practical demonstration of the suitability and fitness-for-purpose of legacy systems.

The key basic principles from the 61508 Association document cover issues related to:

- Organisational responsibilities for safety.
- Increasing expectation in safety management and safety technology.
- Demonstrating that legacy systems are fit for purpose.
- Having adequate safety management procedures in place.
- The rigour and prioritisation of technical review.
- The competence of the review team.
- Hazard identification and risk assessment.
- Risk reduction measures.
- Technical review of legacy systems (E/E/PES).

- Action planning.
- Updating operation and maintenance procedures.
- Periodic audit and review.

The steps to compliance with the principles are represented by two flow charts; Figures 1 and 2 of this document. The first flow chart shows a review of the safety management procedures. The second flow chart shows a review of the continued technical suitability and fitness-for-purpose of the safety related systems and, in particular, the legacy systems.

The expected extent and rigour of the review of suitability and fitness-for-purpose of safety related systems described in the 61508 Association basic principles document depends upon the expected consequences and risk from a hazardous occurrence on the protected plant and process. Objective criteria to determine whether consequences and risks are regarded as high or low are given in the next section.

Where the consequence and/or risk are high the review of the technical suitability of all of the safety related systems should be carried out using the (quantitative or semi-quantitative) Safety Integrity Level, SIL Determination-based functional safety approach described in the IEC 61508 Standard; see the glossary for a short description of these methods.

Where the consequence and risk are low, the review of technical suitability can be based on a representative sample of the safety related systems using the SIL Determination-based functional safety approach described in the IEC 61508 Standard, (see 8.2 Management Responsibilities and Roles). However, all safety related systems should be considered (qualitatively) for continuing suitability and fitness-for-purpose (see 8.3 Technical Co-ordinator).

7 DETERMINING THE LEVEL OF CONSEQUENCE OR RISK

There are several factors that have to be taken in to account:

- Historical safety record of safety related protection systems
- How well systems have been managed
- The test frequency
- How stable has the design and use of the plant been over time
- Consequences of hazards present.

In deciding if your plant is HIGH or LOW consequence /Risk the following questions should be considered:

- Is the site a COMAH or non-COMAH site?
- If COMAH, is it top tier?
- What would be the consequences of an occurrence of the credible hazards?
- Could the hazards have an effect at, or beyond, the site fence?

- Is the plant and process stable over time, or are there numerous changes of design, operation and materials?
- Is there history and experience with the plant, process and safety systems?
- Has this history and experience demonstrated that the safety system functionality and integrity is suitable?
- Have the safety systems been periodically tested and the outcome of tests recorded
- Is their a non-conformance procedure in place, recorded and actions followed through?
- Do the results of this testing demonstrate that the safety system integrity is suitable?
- Is there established and effective management of the legacy safety systems, for example a Management of Change procedure, with a good track record?

The answers to all of these questions should help you decide which category of plant you are operating and the approach you should consider for the management of your legacy systems.

8 REVIEW OF FUNCTIONAL SAFETY MANAGEMENT PROCEDURES

The 61508 Association principles document includes:

"*The law requires that an adequate safety management system is in place. An effective functional safety management system is an essential element in achieving adequate risk control. An assessment of the company's approach to the management of safety-related systems (functional safety management system) should be carried out. The objective is to ensure that the policies and activities follow current good practice and regulatory expectation in regards of functional safety, such as described in IEC 61508. The correction of any identified inadequacies in the safety management system should be included in the Action Plan*."

This document uses the term "procedures" when referring to management systems; this is a difference in terminology with the 61508 Association basic principles document.

This document can't cover every situation and the reader should always refer to the relevant standards for their business activity. However the most common items that are necessary to include in functional safety management procedures are described below:

8.1 Tolerable Risk Criteria

Tolerable risk criteria are values set by the organisation to define the tolerable frequency targets for different levels of consequence used for the design and assessment of safety related systems. The 61508 basic principles document states that an

organisation's management needs to determine and define the organisation's tolerable risk criteria.

Guidance on suitable measures, and numerical values, is given in the HSE document "*Reducing Risks, Protecting People*", but, technical input from a specialist in safety related systems is likely to be required to assist management in discharging this responsibility.
There can be different expectations for tolerable risk between new and existing process plants (where legacy systems will be). The following is an extract from the *HSE guidance Principles and guidelines to assist HSE in its judgements that duty-holders have reduced risk as low as reasonably practicable*:

"*It should be borne in mind that reducing the risks from an existing plant ALARP may still result in a level of residual risk which is higher than that which would be achieved by reducing the risks ALARP in a similar, new plant. Factors which could lead to this difference include the practicability of retrofitting a measure on an existing plant, the extra cost of retrofitting measures compared to designing them in on the new plant, the risks involved in installation of the retrofitted measure (which must be weighed against the benefits it provides after installation) and the projected lifetime of the existing plant.*

All this may mean, for example, that it is not reasonably practicable to apply retrospectively to existing plant, what may be demanded by reducing risks ALARP for a new plant (and what may have become good practice for every new plant)".

Note: ALARP may be demonstrated by a Cost Benefit Analysis (CBA) where the organisation has defined the value of gross disproportionality.

8.2 Management Responsibilities and Roles

The principle organisation management responsibilities and roles are as described in Section 4 RESPONSIBILITIES AND ROLES OF THE ORGANISATION MANAGEMENT. The means of delivering these should be documented and should be understood by all relevant people, including those to whom roles are delegated.

8.3 Technical Co-ordinator

A technical co-ordinator should be appointed for each safety related system. The technical co-ordinator should have:

- Adequate knowledge and understanding of the 6508/61511 requirements for safety related system, and, for legacy systems:
  - over view of the safety philosophy involved
  - the engineering principles employed
  - the equipment used to implement the system.
- Relevant process and plant knowledge.

- Adequate qualifications and/or experience appropriate to the SRS.

The role of the technical co-ordinator includes:

- Acting as a focal point for the safety related system. Generally taking on a co-ordinating role for all engineering activities concerning the safety related system, but not necessarily managing all operational and maintenance issues.
- Ensuring that adequate documentation and records are maintained.
- Initiating the periodic review (Section 11.2 Periodic Review of Each Safety Related System).
- Initiating appropriate action should shortfalls or defects become apparent with the safety related system.
- Informing management of any issues or deficiencies that arise with the safety related system

The technical co-ordinator should have adequate seniority or empowerment to be effective in these roles.

8.4 Change Management

Procedures and practices should be in place to ensure that safety related systems are not subject to change, modification or replacement without a proper assessment being made of the implications. Generally any safety related system, including any legacy system, that is to be changed, modified or replaced should be subject to a functional safety assessment, including SIL Determination, based upon the (quantitative) approach described within the IEC 61508 Standard.

Generally the technical co-ordinator (Section 8.3 Technical Co-ordinator) will have a role in any change or modification of a safety related system.

When changes are made, or deficiencies in current documents identified, the documents should be updated. Good record keeping can help to ease future reviews.

8.5 Maintenance and Repair Policies and Strategies

The maintenance of a Safety Related System (SRS) has two objectives;

- That the safety related system will actually perform the required design intent of the safety function; i.e. that, basically, it works. This is verified by proof testing in accordance with the HSE guidance to inspectors for proof testing.
- That the condition of the equipment and system is such that the likelihood of fault or failure in the future is reduced to ALARP; i.e. that the system is in good condition. Note: this objective may be integrated with the requirements of EX certified equipment.

Maintenance also has a possible role in reducing the likelihood of external factors, such as: physical damage; interference, environmental effects, each resulting in the safety function not being effectively delivered. However, it might be necessary to make engineering changes to the safety related system to achieve this. Any such changes should be considered and co-ordinated by the technical co-ordinator for the safety related system.

Adequate maintenance strategies and maintenance requirements (maintenance policies) should be established for all safety related systems.

Factors to be considered should include:

- Criticality of the safety function.
- Design and architecture of the safety related system.
- Anticipated frequency that protection will need to operate.
- Protected plant and safety related system history.
- History from similar plant and safety related systems.
- Potential for maintenance or testing induced defects.

Maintenance methods should be documented for safety related systems where:

- There are specific requirements.
- There are maintenance requirements beyond normal good practice that can be expected of trained competent technicians.
- There are activities that, if not performed correctly or comprehensively, could compromise the performance of the safety related system.
- There are requirements that must be carried out with a specified periodicity or in specified circumstances.

For example, it would be appropriate to document that a particular pressure transmitter should be calibrated at 12-monthly intervals; that the calibration error should not be more than 5% of full range; but it would not be necessary to document how to carry out such a calibration. The detailed maintenance and calibration requirement should be documented in a method statement with any associated risk assessment.
It is expected that routine activities, such as maintenance and calibration, will be executed by competent personnel. Competence will be assessed by a management of competence procedure. This will be linked to a person's training records to demonstrate that they are competent to perform such tasks.

On completion of any maintenance activity the safety related system should be tested or checked for proper operation, that is, a demonstration that the design intent is achieved as far as is practicable. A minimum set of post-maintenance tests and/or checks should be defined and documented for each safety related system, noting that in some

circumstances the range of possible tests and checks might be constrained if the plant is running.

Equipment forming part of a safety related system should be identified as such within work management systems, on work instructions, and where practicable related documentation.

It is good practice to identify safety related systems equipment (i.e. equipment involved in implementing Safety Functions) in such a way that it is readily identifiable. Any plant identification (labels, colour, etc.) should be regularly inspected and maintained to ensure that it is not degraded to the point where its function is impaired. General industry practice seems to be gravitating towards using the colour red to denote equipment involved in safety related systems; it is therefore recommended that, unless there is reason otherwise, the colour red should be used for this purpose.

Where maintenance activities have been carried out as the result of a fault detected by a proof test; or a safe (spurious operation) failure within the safety related system; or, if a fault or failure within a safety related system is identified during maintenance activities, then, the faulty equipment, and the nature of the fault (the failure mode), should be determined and recorded. The recording system should be such that the comprehensive fault and failure history of the safety related system, and the constituent equipment, can be confidently retrieved, reviewed and analysed. Following all remedial or modifications work a documented proof test must be carried out.

8.6 Inspection and Test Policies and Strategies

Safety related systems can be compromised by hidden faults and failures; i.e. faults and failures that do not reveal themselves, but would compromise the delivery of the safety function should there be a demand upon the safety related system. It is important that these are identified and rectified in a timely manner; this is the objective of inspections, tests and checks of safety related systems.

The organisation management, through the functional safety management procedures, should ensure that:

- inspections
- checks
- tests

identified in:

- the maintenance requirements (maintenance policies)
- the hardware reliability calculations relating to the safety related system

are carried out and adequately recorded, at the required frequencies, by competent personnel.

Inspection, test and check activities to be considered could include:

- Equipment item or system functional checks.
- Safety Function proof tests.
- Simulation.
- Physical inspection.
- Reinstatement. (Re-commissioning)

Management procedures should be in place to ensure that any defects are recorded and that appropriate action is taken if a defect is found. A record should be kept of the repairs carried out to a defect; the timescale for remedying the defect should be commensurate with the risk that the defect poses; temporary measures, or even shutdown of part of the plant or process, may need to be considered. Where potential events can be foreseen, formal procedures should be in place detailing the necessary actions.

Time intervals for inspections, tests, and checks of legacy systems should be based upon one of the following:

- Previous experience. Where there are no known issues, and the test failure rate is low, the existing intervals can be maintained. Where there are issues, or the test failure rate is not low, consideration should be given to more frequent inspections, tests and checks (consideration should also be given to engineering changes to address the issues and/or reduce the failure rate).
- The demand rate on the safety related system. The intervals between inspections, tests and checks should be significantly less than the intervals between demands. Should there be other protection, additional to the safety related system, this can be relaxed to some extent, but specialist safety related systems engineering advice should be taken should in both cases.

If a fault, or failure within a safety related system, is identified during an inspection, check or test activities, the identity of the faulty equipment, and the nature of the fault (the failure mode), should be determined and recorded. The nature of the recording system should be such that the comprehensive fault and failure history of the safety related system, and the constituent equipment, can be confidently retrieved, reviewed and analysed.

8.7 Safety Related Systems Documentation (Safety File)

Adequate documentation and records for each safety related system should be maintained in a Safety File. This should include:

- Design, engineering and commissioning documents, including drawings, schedules and other records if available.
- Operational Procedures and other operational documents.
- Maintenance, test records, documentation and policies.
- Records of each periodic review (Section 11.2 Periodic Review of Each Safety Related System).
- All documentation and records relating to modifications.
- Copies of any correspondence.
- All documentation related to any relevant hazard and risk analysis, functional safety assessment and any assessments done in accordance with IEC 61508/11.

Following the BP Texas City and the Buncefield incidents, the HSE are increasing their expectation of record keeping even on non-COMAH sites. The HSE expectation is still not fully clarified but it is anticipated that for SRSs the following types of information is now likely to be expected by the HSE; (refer to HSE guidance to inspectors for proof testing)

- Demands on the safety related system.
- Successful/unsuccessful execution of the safety function on demand.
- ALL faults and failures of the safety related system.
- ALL inspections, checks and tests of the safety related system, including the as-found and as-left condition.
- Competency information for all people interacting with the safety related system, including any training certificates and records specific to functional safety and safety related systems.

The previous management of documentation related to safety related systems should be reviewed as part of the review of the functional safety management procedures. Should the previous management of documentation be judged inadequate e.g. less than comprehensive or prone to errors, then a programme of document verification should be considered. Documents should be assessed when safety related systems are technically reviewed for suitability and fitness-for-purpose (Section 9.3 Qualitative Consideration of All Safety Related Systems) and as part of a periodic review (Section 11.2 Periodic Review of Each Safety Related System).

Documentation should be stored in a way that facilitates easy retrieval and maintenance. If information is stored in a maintenance management system then it should be searchable by a systematic reference so that all entries relating to particular plant items are readily obtainable. Information can be stored in a combination of two ways:

- Either gathering the required information together in one location, be that a physical location or a computer-based storage location.

- Or by listing references to where the information can be obtained (e.g. as a list of relevant drawing numbers or as pointers to maintenance management system records).

In all cases, the information and/or the references should be maintained in an up to date and comprehensive form.

The above documentation and records, or reference to where the information is maintained, should form the basis of a discrete Safety File for each safety related system.

8.8 Data Collection

It is thought likely that some companies will need to change the way that information on safety related systems is managed:

- A Safety File will need to be produced and maintained for each safety related system (Section 8.7 Safety Related Systems Documentation (Safety File). This might well require information already available to be drawn together. It might require information, kept personally by individuals, to be brought into an information management process.
- Data will need to be collected on the demands on, and performance of, each safety related system. This might well be done in a data logging system.
- Data will need to be collected on the testing and maintenance of safety related systems, including as-found information and all failures and failure modes (Sections 8.5 Maintenance and Repair Policies and Strategies and 8.6 Inspection and Test Policies and Strategies).

Although the HSE publication, HSG 254, 'Developing Process Safety Indicators' is primarily concerned with managing hazards arising from COMAH sites, it is recognised that the document may be applicable to other parts of the process industry. The document asserts that measuring process safety performance provides some degree of assurance that risks are being adequately controlled. The approach taken in this HSE publication is similar to that being proposed here. The HSE document places an emphasis on the use of leading indicators (eg: results of planned inspections or tests) with limited use of a few lagging indicators (actions in response to incidents).

Each safety related system needs attention to pick up any deterioration and to ensure early corrective action taken. It is expected that monitoring the demand level and proof tests of the safety related system will facilitate this activity.

One of the outcomes of reviewing existing functional safety management procedures is likely to be identification of the need to enhance the management process for collecting appropriate data so that the performance of the safety related protection systems can be demonstrated. If cause for concern is then identified, action can be taken to reduce the risk associated with any particular system.

Data for monitoring the demands on, and performance of, safety related systems was not routinely built into legacy systems. Appropriate judgement must be used on:

- The practicality of collecting this data.
- The appropriate means of doing this (automatic data logging or manual recording).
- Ensuring that the means of collecting the data does not compromise the functionality or reliability of the protection system.

Legacy system operators generally fail to collect reliability data for specific items of equipment used in safety related systems. Even where work management systems are used these do not always capture "as-found", "as left", and failure mode information. An appropriate work management recording process, covering both testing and maintenance work (including any investigation and/or maintenance work carried out by operations staff) should be established.

8.9 Competence Management

All technical work relating to safety related systems should be carried out by people from an appropriate range of disciplines and possessing the necessary competencies. The range of disciplines will depend on the nature of the plant, process and safety related system technology, but should include those with an understanding of the process under control as well as those trained in hazard and risk assessment and in functional safety and safety-related systems. Those with experience of operations and maintenance should be included.

There should be a management process in place to ensure, and to demonstrate that, the competency and resource requirements are understood and that a suitable number of competent people are available and are deployed to address the technical issues and work associated with the safety related systems.

9 SAFETY RELATED SYSTEMS TECHNICAL SUITABILITY REVIEW

The 61508 Association principles document includes:

"*IEC 61508 provides a risk based approach to specifying, designing, implementing and using safety related systems. Legacy systems will have been created using different designs or standards. The continuing suitability and fitness for purpose of such legacy systems should be confirmed by conducting a technical review …….*"

and:

"*The rigour of the technical review of the legacy systems, and hence the resources allocated to the task, should be related to the hazards, consequences and risks associated with the operating unit. The more serious the consequences and the more likely the hazardous events, the more thorough the review needs to be. A preliminary survey should be conducted in order to identify the likely higher risk areas and to determine the rigour and prioritisation of the review.*"

On non-nuclear process industry plants or operating units the technical review of continuing suitability and fitness-for-purpose of the safety related legacy system, should be based on hazard identification and risk assessment conducted in four stages:

- Creating a list of potential Safety Related Systems.
- Carrying out an IEC 61508 SIL Determination-based (quantitative or semi-quantitative) functional safety assessment of a representative sample of safety related systems.
- Carrying out a (qualitative) consideration of all potential safety related systems.
- Implementing an Action Plan to deal with any safety related systems determined as providing insufficient risk reduction. Prioritise the systems to consider those first where the risk is perceived the greatest and consider the other systems over a longer period of time.

Note that the above approach to legacy systems involves both knowledge of the hazards and an awareness of the level of risk posed by the hazards.

9.1 List of Potential Safety Related Systems

The 61508 Association principles document includes:

"*A record of the hazards associated with the plant and process should be available and up to date. In the absence of such a record, a hazard identification and risk assessment should be undertaken. A good starting point is a list of all existing safety-related systems, but care should be taken because there may be hazards:*

- That were not previously identified or understood.
- That are not currently protected by safety-related systems.
- That have arisen since the last hazard and risk assessment.
- That have changed in risk since the last hazard and risk assessment."

A register should be prepared of all potential safety related systems. Identifying the systems and hazards is an important step in managing safety and the register should be adequately maintained and readily available.

The register should:

- Include all hazards and hazard mechanisms, whether or not these are protected by safety related systems.
- Include hazards and hazard mechanisms that are protected by purely mechanical devices since they contribute to a lowering of the integrity level required for the safety related system.

It is suggested that the register should provide the following information:

- Plant Area
- Hazardous Situations
- Hazard
- Safety Function
- Protection Equipment
- Indication of Risk Reduction

The register should be initially determined and then periodically reviewed by a Hazard Identification, Risk Assessment and Safety Related System Workshop (a "Functional Safety Assessment" workshop might be an easier title) involving at least:

- Process, plant, C&I and protection system staff.
- Relevant plant and process engineers.
- Operations staff.
- Safety related systems specialist.

The workshop group should include all the staff necessary to ensure that there is:

- Operational experience and knowledge of the plant, process and protection functionality and systems.
- Engineering experience and knowledge of the plant, process and protection functionality and systems.
- Expertise and knowledge on the plant, process and protection principles applied.
- Sufficient seniority or empowerment to make technical judgements and decisions.

It is suggested that the workshop should first identify all potential hazards associated with the plant and process and all protection functions and systems. The workshop should then consider whether each item:

- Has the potential to cause risk of harm to humans should the hazard occur and/or the protection function fail

  AND

- Requires, or has, risk reduction which is implemented using an E/E/PE system.

Those that do should be categorised as safety related systems. The consideration should be done on the basis of the qualitative or semi-quantitative application of expert judgement and experience.

It is advantageous to use the workshop as a means to capture as much relevant information as possible about each safety related system from the people present. Of particular importance is information about:

- The nature and source of demands upon the safety related system.
- The frequency of demands on the safety related system.
- The performance and reliability of the safety related system.
- The possible and seen failure modes of the safety related system.
- Operational issues and difficulties with the safety related system.

For further guidance see 61511.Part 2 section 10.3

This information is required for future stages.

Many of the items and issues identified in the workshop will not be, nor require, safety related systems. Non-E/E/PE safety systems should be recorded, as their maintenance, operation and performance may greatly affect the reliance on the E/E/PE safety related systems. It is suggested that these items should not be deleted from the register, but should be marked as non E/E/PE safety related systems, along with sufficient text to indicate to an informed and knowledgeable engineer the basis for the item or issue not requiring an E/E/PE safety related system. Although not required it may be beneficial to identify non-safety systems that protect plant/commercial loss. Much of this information will be generated in the process of identifying safety related systems.

More than one session is likely to be needed to complete an initial Hazard Identification, Risk Assessment and Safety Related Systems Workshop. It is recommended that each session should cover a logical plant or process areas, to allow the staff to attend only the relevant parts of the activity.

It is likely that many process plants will find it difficult, without proper consideration, to separate interlock, trip and protection systems from safety related systems. For this reason, it is recommended that all trip and protection systems are considered initially, so that there is a clear understanding of what each process or site is dealing with.

After capturing the knowledge of experienced staff, it should be possible to see which E/E/PE safety related systems are either used the most or require most component replacement. This knowledge will then help to identify the legacy systems that require most attention. Shortcomings in the information on E/E/PE safety related system performance, maintenance and testing should be noted for future improvement.

9.2 Assessment of Representative Sample

Conducting a full IEC 61508, SIL Determination-based, functional safety assessment of all legacy systems would be an expensive and time-consuming process, so it is sensible to focus the effort in a resource-effective way rather than slavishly performing a detailed analysis of all systems. The HSE document *SPC/Permissioning/12*, which provides guidance on ALARP decisions in the control of major accident hazards states that the level of risk can be used to determine the type of risk assessment that needs to be used; it is sensible to use the same approach to legacy systems so that most effort is focussed on the higher risk areas:

- If risks are Broadly Acceptable or at the bottom of the ALARP region the Qualitative risk analysis will suffice.
- If risks are in the middle of the Tolerable ALARP region then semi-quantitative risk assessments will suffice.
- For risks bordering the intolerable region then a full quantified risk assessment is required and, unless suitable justification can be put in place, additional protection should be provided to reduce the risk.

In order to characterise the level of residual risks on the process plant, a representative sample of safety related safety systems should be evaluated in a quantitative or semi-quantitative way, to provide a SIL Determination-based functional safety assessment of those systems. Criteria for selecting a representative sample of safety related systems could be :

- A spread of plant areas.
- A spread of functions delivered, such as alarms, inhibits, trips and active protection systems.
- A spread of the technology used, such as hard-wired systems, relay logic and programmable systems.
- A spread of system ages and different system suppliers.
- The nature of the hazards and related risks. Systems that protect against high consequence events should be prioritised into the sample.
- The demand rate. Systems that have a high demand rate should be prioritised into the sample.

Some process plants may have carried out IEC 61508 SIL Determination-based quantified functional safety assessments (associated with previous modifications). If so, and the assessments are appropriate and relevant, information from these can be used as part of the SIL Determination-based assessment sample. However, it might well be necessary to identify some additional (legacy) safety systems to provide a representative sample of such systems; quantitative IEC 61508 SIL Determination-based functional safety assessments of these systems will have to be undertaken.

Should any of the legacy protection systems included in the representative sample for quantified SIL Determination-based functional safety assessment be identified as not meeting the tolerable risk targets set (as described in Sections 4 RESPONSIBILITIES AND ROLES OF THE ORGANISATION MANAGEMENT and 8.1 Tolerable Risk Criteria), then the following applies;

- Consideration should be given to reducing the risk shortfall and complying with the principles of ALARP. This can be done through such steps as increasing the testing frequency and/or upgrading the protection system. Generally, any upgrade should be in full conformance with all requirements of IEC 61508 and/or related standards. As always, the consideration and a justification for the selected course of action should be documented.
- Consideration should be given to any inferences that can be drawn for other systems from the sampled system having fallen short of the tolerable risk target. It is likely to be appropriate to carry out some additional quantified SIL Determination-based functional safety assessments to ensure that a representative picture of the residual risk across the process plant is understood.

9.3 Qualitative Consideration of All Safety Related Systems

Every safety related system on the site, which is not subject to a quantitative or semi-quantitative SIL Determination-based functional safety assessment, should be subject to a qualitative consideration of its suitability and fitness-for-purpose. This is based on the register of safety related systems identified as per Section 9.1 List of Potential Safety Related Systems.

The use of a representative sample of safety related systems for quantitative or semi quantitative, SIL Determination-based, functional safety assessment will indicate (or otherwise) that the residual risks from the hazards and safety related systems on the process plant are generally compliant with the tolerable risk criteria and comply with ALARP. It then follows that if risks are well managed and broadly acceptable or at the bottom of the ALARP region then it will suffice to use qualitative risk assessment methods for the rest of the safety related systems rather than spending significant effort and scarce expert resource in obtaining data for a rigorous quantified or semi quantified, assessment.

Should assessments result in the conclusion that the residual risks from the hazards and safety related systems are generally not compliant with the tolerable risk criteria set, and/or do not comply with the ALARP principle, then SIL Determination-based (quantitative or semi quantitative), rather than qualitative, techniques will need to be more widely applied.

The information that should be considered in a qualitative manner about each safety related system in order to make the judgement of suitability and fitness-for-purpose should include:

- The Hazard and Hazard Mechanisms being protected against.
- The human exposure to the Hazard.
- The causal events of the Hazard Mechanisms.
- The frequency of demands.
- The Safety Functions.
- The dependency on the safety related system; do other layers of protection exist? Does the safety related system protect against all sources of demand?
- The equipment and systems providing the safety functions.
- The reliability of the safety related system.
- Vulnerability to hidden faults.
- The efficacy of testing and the testing results.

The judgement should be made by a **GROUP** of relevant competent people. The same criteria that applied to the constitution of the Hazard Identification, Risk Assessment and Safety Related System Workshop described in Section 9.1 List of Potential Safety Related Systems apply to this stage; hence this stage is often best done as part of the workshop described in Section 9.1 .

Judgement needs to be made on the basis of recorded evidence. If judgement is to be made purely on the basis of historical evidence, this needs to be recorded historical evidence. Should such recorded historical evidence not be available or not be sufficient, the judgement needs to be backed up with some degree of engineering consideration and recorded.

10 ACTION PLAN

The 61508 Association principles document includes:

"*A prioritised action plan should be prepared to deal with any inadequacies in the functional safety management system and any deficiencies in the safety-related systems. In cases of serious shortfall, interim measures will need to be taken while longer term solutions are implemented. When E/E/PES are replaced or upgraded, the new ones should be specified, designed and implemented in line with IEC 61508. A different approach would need to be considered if there are incompatibility problems in relation to other, existing systems and practices.*"

Actions in the Action Plan do not need to be delivered immediately or even in the short term; some actions could be planned for implementation during, say, a future outage. However, whenever remedial, risk-reducing, measures are to be delayed (e.g. until a future outage period):

- The increased residual risk during the interim period should be assessed and a judgement made of its tolerability. If it not regarded as tolerable, additional interim risk-reduction measures will need to be put in place.
- Consideration should be made of whether the residual risk during the interim period constitutes ALARP; if there are reasonably practicable interim measures that can be applied without imposing a grossly disproportionate burden compared with the risk reduction that would result, such measures should be applied.

11 ON-GOING ACTIVITIES

Sections 8 , 9 and 10 cover activities that need to be completed only once. They could be repeated at intervals, but it would only be relevant to do this at extended intervals.

However, there are some functional safety management activities that will need to be repeated periodically.

Inspections and Testing of safety related systems is required periodically though the policy or framework for these Inspections and Tests is covered in Section 8.6 Inspection and Test Policies and Strategies.

The 61508 Association principles document includes:
"*Periodic audits of the effectiveness of the functional safety management system should be conducted, with the results being used to drive on-going improvements in safety and operations. Periodic technical reviews, sponsored by senior management, should be carried out to ensure that each safety-related system continues to be fit for purpose and results in sufficient risk reduction to meet the organisation's tolerable risk criteria*."

11.1 Periodic Audit of the Functional Safety Management Procedures

An essential part of formal safety management procedures is the conduct of periodic audits of the management of functional safety and of safety related systems. Without such audits there will be little evidence that the necessary procedures are being implemented. Formal scheduled audits should be carried out by a team consisting of appropriate management, operating and maintenance personnel. The team should provide a record of findings and follow-up activities with a plan for corrective and preventative actions.

It could be worth considering the principles for monitoring the effectiveness of risk control systems as described in the HSE publication HSG254, *Developing Process Safety Indicators*, the process of setting and monitoring leading and lagging indicators can provide a good level of assurance at senior level of the effectiveness of safety systems.

11.2 Periodic Review of Each Safety Related System

The Technical Co-ordinator (Section 8.3 Technical Co-ordinator) should initiate a periodic technical review of each safety related system. The review should consider:

- Whether the Safety Functions of the safety related system are still appropriate.
- Whether the Safety Integrity Levels (SIL) are still appropriate (for systems managed to IEC 61508).
- Whether technology or regulatory expectation has moved on to the extent that the current systems can no longer be regarded as reducing risks to ALARP.
- What demands have been made on the system
- What maintenance has been carried out (Section 8.5 Maintenance and Repair Policies and Strategies)
- Results of inspections, checks and tests (Section 8.6 Inspection and Test Policies and Strategies).
- Any failure to deliver the safety functionality on demand.
- Any spurious operation.
- Any reported issues.
- Whether any changes to the safety related system would be beneficial to improve safety, reliability, operability and maintainability.
- Whether the documentation and records are adequate and in good order (Section 8.7 Safety Related Systems Documentation (Safety File).
- Whether the maintenance strategies and maintenance requirements (maintenance policies) are still appropriate (Section 8.5 Maintenance and Repair Policies and Strategies).

Periodic reviews can take place to a programme suitable to the process plant; they can be grouped together or spread out, they can be carried out during outage periods or they can be deliberately kept away from outage periods. It is appropriate to carry out a single Periodic Review of a safety related system covering all similar process plants on the site, unless there are significant differences between the need for the demands on, or the implementation of, the safety related system between such process plants..

It is recommended that the periodic review of each safety related system should take place at an interval appropriate to the system but in any case not exceeding 5 years. A competent person should be consulted if doubt exists on the appropriate frequency.

It is also suggested that good practice will include interim reviews of the demand and maintenance data for the safety related systems conducted typically every two years. If systems are known to provide more risk reduction, equivalent to SIL 2or 3, then a more frequent review may be appropriate.

The Safety Function should be re-proven on each unit at the time of the periodic review unless:

- The Safety Function is simple

  AND

- The Safety Function has been proven in operation on the process since the previous periodic review OR has been subject to proof testing

  AND

- The above is adequately recorded in documentation, logs, and computer records or similar.

12 SUMMARY

This document has outlined a procedure for managing safety related systems that have remained essentially unchanged on process plant for many years and were installed prior to the adoption of the standard 61508. These systems are referred to as Legacy Systems.

There is a significant difference between the issues related to the management of legacy safety systems in different industrial sectors and on different sites. Following the BP Texas City and Buncefield incidents however, there is an expectation that even non-COMAH sites will record much more information about their existing safety related systems.

It is judged that there is no need to replace legacy systems merely to comply with the IEC 61508 Standard. Nor is there a requirement for the retrospective application of the IEC 61508 Standard to legacy systems. It is sufficient to clarify and demonstrate that the legacy system is "Fit for Purpose".

The approach recommended by these guidelines for non-nuclear sector is to:

- Review the functional safety management procedures (Section 8).
- Create a list of the potential safety related systems (Section 9.1).
- Carry out a qualitative consideration of all safety related systems for suitability and fitness-for-purpose (Section 9.3).
- Carry out a SIL Determination-based functional safety assessment of a representative sample of low consequence safety related systems (Section 9.2) and all High consequence safety related systems.
- Implement an Action Plan for any discrepancies or shortfalls identified (Section 10).
- Carry out Periodic Audits of the functional safety management procedures (Section 11.1).
- Carry out periodic reviews of each safety related system (Section 11.2).

13 REFERENCES

[1] Health and Safety at Work Act 1974.

[2] Management of Health and Safety at Work Regulations 1999 Approved Code of Practice and Guidance (HSE Pubs L21 ISBN 0-7176-2488-9).

[3] Safe use of work equipment - Provision and Use of Work Equipment Regulations (PUWER) 1998 Approved Code of Practice and guidance (L22, HSE Publications 1992, reprinted 2001, 2004 ISBN 0717616266).

[4] The 61508 Association publication “Legacy Systems: Basic Principles for Safety”.

[5] 'Out of Control - Why control systems go wrong and how to prevent failure' (Second Edition HSG238 ISBN 0-7176-2192-8).

[6] Developing Process Safety Indicators, HSE 2006. ISBN 0 7176 6180 6

[7] IET/BCS publication *Competence Criteria for Safety-related System Practitioners*.

[8] Guidance on ‘as low as reasonably practical’ (ALARP) decisions in the control of major accident hazards (COMAH). (SPC/Permissioning/12) see subsection on Risk Assessment rigor. http://www.hse.gov.uk/comah/circular/perm12.htm.

[9] **“**Principles and guidelines to assist HSE in its judgements that duty-holders have reduced risk as low as reasonably practicable” HSE Website. http://www.hse.gov.uk/risk/theory/alarp1.htm.

[10] SPC/Permissioning/09 – “HID’s approach to As Low as Reasonably Practicable (ALARP) decisions”. HSE website. http://www.hse.gov.uk/comah/circular/perm09.htm.

[11] “Assessing compliance with the law in individual cases and the use of good practice”, HSE website. Revised May 2003 http://www.hse.gov.uk/risk/theory/alarp2.htm.

[12] http://www.hse.gov.uk/risk/theory/r2p2.pdf - Reducing risks, protecting people (R2P2) gives guidance on HSE's decision making, including the use of good practice, and on tolerable risk criteria.

14 GLOSSARY OF TERMS

Phrase	Description
Legacy System	An electrical, electronic or programmable electronic system (E/E/PES) which performs one or more safety functions as defined in IEC 61508 but which was designed and installed before the publication and adoption of IEC 61508.
Quantitative SIL Determination	Analysis that numerically determines the required SIL for a safety function.
Semi - Quantitative SIL Determination	Analysis that numerically estimates the required SIL for a safety function.
Qualitative Consideration of Suitability and Fitness-for-Purpose	The consideration, without calculations, of evidence to arrive at a judgement of the suitability and fitness for purpose of a safety related system. This should consider both the demand and protection issues associated with the safety related system.
Tolerable Risk Criteria	Quantified limits for tolerable risk. These are defined in terms of the tolerable likelihood of occurrence of stated consequences, generally fatality of an identified individual (Individual Risk) or of a hazardous events resulting in a set number of fatalities (Group/Societal Risk). These criteria should be set by an organisation's top management.
Technical Coordinator	Site person appointed to co-ordinate and oversee the functional safety management of a specified safety related system.
Functional Safety Assessment	The full application of the approach described in the IEC 61508 Standard, including hazard and risk assessment, Safety Function and SIL Determination, safety related systems design, integrity assessment and validation.
Safety Integrity Analysis	Assessment of a proposed or actual safety related system against a safety requirements specification to confirm that it meets the required random hardware failure criteria (PFD_{avg} or fph), hardware architectural requirements (hardware fault tolerance) and systematic failure criteria (SIL).
Safety Related System	An electrical, electronic or programmable system implementing one or more safety functions.
Functional Safety	Part of the overall safety relating to the equipment under control (EUC) and the EUC control system which depends on the correct functioning of the E/E/PES safety-related systems, other technology safety-related systems and external risk reduction facilities.
Functional Safety Management	The provision of policies, methods and resources to manage functional safety and safety related systems on a plant.

Figure 1: Legacy System Management Procedures Review Flowchart [61508 Assoc]

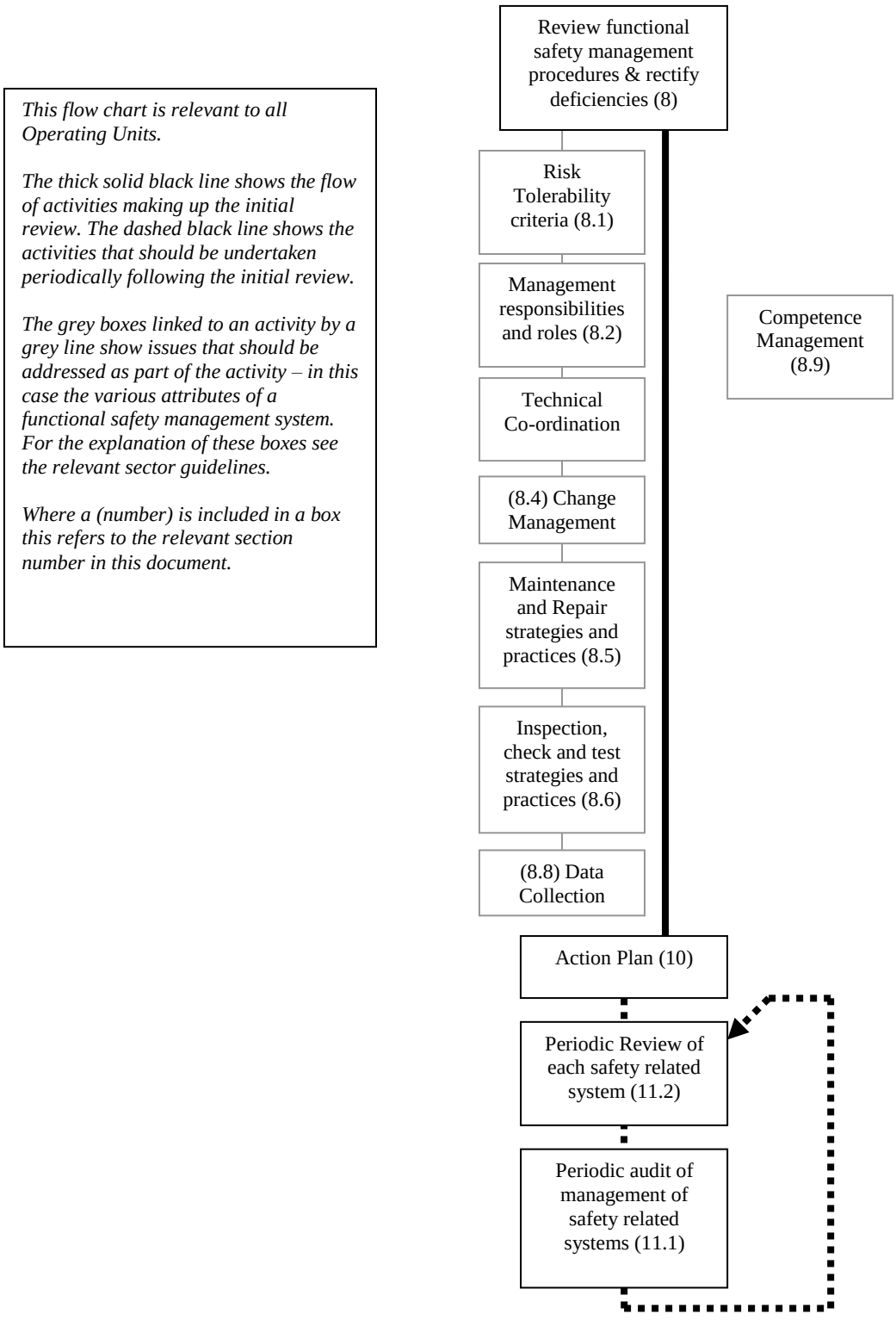

Figure 2: Legacy System Technical Suitability Review Flowchart [61508 Assoc]