Developed with CDOIF

Chemical and Downstream Oil Industries Forum

Guidance

Learning for COMAH Sites
from the
Buncefield Incident.
2017

Foreword

CDOIF members, as part of their role in promoting and leading on key sector process safety initiatives, originally developed guidance based on the final report of the Process Safety Leadership Group on the Buncefield Incident first published in December 2009. The aim was to adapt the approach of the original report to major hazard industries outside gasoline storage. Where organisations need further detail on the aspects of safe management of high hazard substances referred to in this document reference should be made to the original report.
However, the original working group was unable to complete the editing work.
EEMUA completed and released this guidance after members reviewed the original CDOIF work, and felt it was a valuable contribution to the field.

There are no limitations on further distribution of this guidance to other organisations outside of EEMUA or CDOIF membership, provided that:

1. It is understood that this guidance represents CDOIF's view of good practice as applied to high hazard facilities such as those storing large quantities of gasoline and other flammable liquids at the time of writing.
2. EEMUA and CDOIF accepts no responsibility in terms of the use or misuse of this document.
3. The guidance is distributed in a read only format, such that the name and content is not changed and that it is consistently referred to as "Learning for COMAH Sites from the Buncefield Incident." The Author should be given as "EEMUA" and date as "2017".
4. It is understood that no warranty is given in relation to the accuracy or completeness of information contained in the guidance except that it is believed to be substantially correct at the time of publication.

TABLE OF CONTENTS

Abbreviations

ACOP Approved Code of Practice
ALARP as low as reasonably practicable
AIChE American Institution of Chemical Engineers
AMN all measures necessary
API American Petroleum Institute
APJ absolute probability judgment
ARAMIS European Commission on Accidental Risk Assessment Methodology for Industries
ASM abnormal situation management
ATG automatic tank gauging

BAT best available technology
BPCS basic process control system
BPCF basic process control function
BSTG Buncefield Standards Task Group

CA Competent Authority
CAP-EPLG chemical and pipelines emergency planning liaison group
CBA Chemical Business Association
CCPS (US) Center for Chemical Process Safety
CIA Chemical Industries Association
CIRIA Construction Industry Research and Information Association
CM conditional modifier
CMS competence management system
COMAH Control of Major Accident Hazards Regulations
CSB (US) Chemical Safety Board

DCS distributed control system
DETR Department of the Environment, Transport and the Regions
DSEAR Dangerous Substances and Explosive Atmospheres Regulations 2002
DRA dynamic risk assessment

EA Environment Agency
ECC emergency control centre
EEMUA Engineering Equipment Materials Users' Association
EPC Error Producing Condition
EPRR emergency preparedness and response report
ERP emergency response plan

FMEA failure modes and effects analysis
FMP fatigue management plan
FRS Fire and Rescue Service

HAZID hazard identification
HAZOP hazard and operability study
HCI human–computer interface
HEART human error assessment and reduction technique
HEP human error probability
HFL highly flammable liquids
HSC Health and Safety Commission
HSE Health and Safety Executive
HSI human-system interface
HSL Health and Safety Laboratory

ICT incident control team
IPL independent protection layers
ISGOTT International Safety Guide for Oil Tankers and Terminals

LAH level alarm high
LAHH level alarm high-high
LOPA layer of protection analysis

MAPP major accident prevention policy
MATTE major accident to the environment
MIIB Buncefield Major Incident Investigation Board
MIMAH methodology for identification of major accident hazards
MOC management of change
MTTR mean time to repair

NIA Nuclear Industry Association
NOS National Occupational Standard
NRW Natural Resources Wales
NVQ National Vocational Qualification

OECD Organisation for Economic Co-operation and Development
ORR Office of Rail Regulation

PFD probability of failure on demand
PHA process hazard analysis
PPE personal protective equipment
PSA process safety analysis
PSF performance shaping factor
PSLG Process Safety Leadership Group
PSMS process safety management system

QRA quantitative risk analysis

RBI risk-based inspection
RCS risk control system
ROV remotely operated valve
ROSOV remotely operated shut-off valve
RVP reed vapour pressure

SCADA supervisory control and data acquisition
SEPA Scottish Environment Protection Agency
SIC site incident controller
SIF safety instrumented function
SIL safety integrity level
SIS safety instrumented system
SG specific gravity
SMC site main controller
SMS safety management system
SRAG safety report assessment guide
SRS safety requirement specification
SVQ Scottish Vocational Qualification

THERP technique for human error rate prediction
TRC tank rated capacity
TSA Tank Storage Association
TWI The Welding Institute

UKPIA United Kingdom Petroleum Industry Association
UKOPA United Kingdom Onshore Pipeline Operators' Association

VCE vapour cloud explosion

Section 1 – Introduction and Scope

The purpose of this guidance is to summarise the good practice for all establishments subject to the Control of Major Accident Hazards Regulations (COMAH) arising from learning from the investigation into the Buncefield incident in 2005, and the subsequent work by the Process Safety Leadership Group (PSLG) and the Chemical and Downstream Oil Industry Forum (CDOIF).

The PSLG Final Report following Buncefield (*1)* was focused on the manufacture and storage of fuels and its guidance was specifically drafted for that industry. PSLG led, developed and promoted improvements to safety and environmental controls at fuel storage sites, including:

- demonstrating effective leadership within the sector;
- developing organisational and technical solutions;
- sharing and learning from incidents and good practice;
- driving forward research;
- monitoring compliance with the Buncefield Major Incident Investigation Board (MIIB) and the Buncefield Standards Task Group (BSTG) recommendations and,
- making further recommendations where appropriate

The PSLG Final Report was therefore a landmark document for the fuel storage industry. However much of the guidance that was developed by the PSLG working group process and which led to the Final Report has relevance for a much wider part of major hazard industry than just fuel storage. This guidance should be helpful to industry in understanding the standards expected, and the valuable lessons to be learned from previous incidents. In recognition of this, CDOIF established a Working Group to review the PSLG Final Report and to make the guidance with generic cross-industry application more accessible to the broader major hazard industry.

The guidance in this document is the result of that process. The CDOIF Working Group approach was to use the good practice already set out in the PSLG Final Report, and to present it for the wider COMAH community, rather than to develop or write new standards. Nevertheless, it has been necessary to reflect more recent developments in process safety, and where relevant additional work or guidance has been completed since the PSLG Report, this has been included or referenced.

Document structure

The structure of the guidance in this document follows the hierarchy of the leadership and management of process safety for major hazard sites, and hence follows the following basic format:

- Introduction and scope
  - Introduction
  - Document structure
  - Scope and application
- The prevention of major accidents through Leadership and Organisation
  - Introduction;
  - Corporate governance for process safety
  - PSLG Process Safety Guidelines
  - High Reliability organisations
  - Positive safety culture
- Process Safety Management
  - Process Safety Management
  - Organisational Issues and Human Factors
- Maintaining integrity of equipment
  - Competency
  - Internal / External inspection
- Preventing loss of containment
  - Management of instrumented protective systems
  - Operator responsibilities and human factors

  - Isolation of equipment in emergency
- Emergency planning and response

Appendices contain further detail. Furthermore, if duty holders wish to see more detail than is presented in this document, they may wish to refer back to the original PSLG Report.

Scope and application

This guidance was originally relevant to establishments to which the Control of Major Accident Hazards (COMAH) Regulations 1999 (as amended) applied. Although primarily aimed at COMAH establishments, the guidance focuses on generic lessons applicable to most businesses handling hazardous substances; as such, parts of this guidance may also be useful for other installations which are not covered by the COMAH regulations.

Towards the end of the preparation of this guidance the COMAH Regulations were updated, and came into force from 1 June 2015. While the PLSG report upon which this document is based has not been updated, the references and nomenclature in this this guidance have been changed where appropriate. In particular, please note the following changes to nomenclature:

COMAH 1999	**COMAH 2015**
Top tier	Upper tier
On-site emergency plan	Internal emergency plan
Off-site emergency plan	External emergency plan

Note also that the original CDOIF working group was unable to complete this document; it was adopted and released by EEMUA, after their members reviewing the work felt it was of value to industry.

Section 2 –The Prevention of Major Accident Hazards Through Leadership and Organisation

Introduction

Parts 5 and 6 and Appendix 7 of the PSLG report related to Operation with High Reliability Organisations, Delivering High Performance through Culture and Leadership and laid down Principles of Process Safety Leadership. This Section summarises the leadership and organisational arrangements that should be in place to develop a high reliability organisation which will aid the prevention of major accidents.

Effective health, safety and environment performance in an organisation starts at the top; members of the board have both collective and individual responsibility for health and safety, including the management of major hazards. Directors and board members need to act to ensure they are leading process safety, alongside their other functions, for the following reasons:

- Protecting the health and safety of employees or members of the public who may be affected by business activities is an essential part of risk management and must be led by the board.
- Failure to include health and safety, and specifically process safety leadership, as a key business risk in board decisions can have catastrophic results. The causes of many high-profile incidents over the years have been rooted in failures of leadership.
- Health and safety law places duties on organisations and employers, and directors can be personally liable when these duties are breached: members of the board have both collective and individual responsibility for health and safety.

Corporate Governance for process safety

In June 2012 the Organisation for Economic Cooperation and Development (OECD) published new guidance on process safety leadership – “Corporate Governance for Process Safety – Guidance for Senior Leaders in High Hazard Industries”. The OECD Guidance is consistent with information on process safety leadership in the PSLG Final Report, but supersedes and refreshes it. This short, succinct guidance is in 3 parts:

- Business case for effective process safety management;
- Essential elements of corporate governance for process safety;
- Self-assessment tool for senior leaders.

The **essential elements** for process safety governance are addressed in the guidance under 5 headings, and set out the key behaviours of leaders to promote process safety leadership:

Leadership and culture: Leaders create an open environment where they:

- Keep process safety on their agenda, prioritise it strongly and remain mindful of what can go wrong.
- Encourage people to raise process safety concerns, or bad news to be addressed.
- Take every opportunity to be role models, promoting and discussing process safety.
- Delegate appropriate process safety duties to competent personnel whilst maintaining overall responsibility and accountability.
- Are visibly present in their business and at their sites, asking appropriate questions and constantly challenging the organisation to find areas of weakness and opportunities for continuous improvement.
- Promote a ‘safety culture’ that is known and accepted throughout the enterprise.

Risk Awareness: Leaders broadly understand the vulnerabilities and risks and they:

- Know the importance of process safety throughout the life cycle – whether it is the design, operation, and maintenance phases of their manufacturing facilities, or storage, logistics and decommissioning at those locations.
- Understand the critical and different layers of protection that are in place between a hazard and an accident and seek to strengthen those layers continually.
- Ensure appropriate and consistent management systems for analysing, prioritising and managing the risk, including strong management of change processes for people, technology and facilities.
- Personally involve themselves in risk assessing proposed budget reductions for process safety impacts and provide incentive schemes which don't encourage production at the expense of process safety risk.
- Take responsibility for emergency planning for the range of consequences from a process safety incident including the worst credible case scenario.
- Know the hazards and risks at installations where there are hazardous substances.

Information: Leaders ensure data drives process safety programmes, and they:

- Ensure that the organisation analyses audit and assessment results.
- Monitor site and corporate level process safety key performance indicators and near misses.
- Have metrics which help to monitor the health of the process safety culture and management systems.
- Actively share experiences and learning within their own organisation and within other high hazard sectors and ensure appropriate, high quality follow-up.
- Establish safety management systems and monitor/review their implementation; seek continuous improvement.

Competence: Leaders assure their organisation's competence to manage the hazards of its operations, they:

- Understand which questions to ask their people and know which follow-up actions are necessary.
- Ensure there are competent management, engineering and operational personnel at all levels.
- Ensure continual development of process safety expertise and learning from new regulation and guidance.
- Provide resource and time for expertise-based hazard and risk analyses, effective training and comprehensive scenario planning for potential accidents.
- Defer to the expertise of personnel, and do not dismiss expert opinions. They provide a process or system to ensure company leaders get expert process safety input as a critical part of the decision making process for commercial projects or activities.
- Ensure the organisation monitors and reviews the process safety competency of contractors and third parties.
- Are capable of openly communicating critical aspects of process safety with all internal and external audiences.

Action: Leaders engage in articulating and driving active monitoring and plans, they:

- Assure practices are consistent with corporate process safety policies.
- Safety measures should be incorporated at the earliest conceptual and engineering design stages of an installation to enhance the intrinsic (inherent) safety of the installation wherever practicable.
- Incorporate process safety considerations into major capital investments, long range planning and integration of mergers or acquisitions.
- Ensure process safety risk mitigation plans and emergency response plans are developed and maintained for all sites within their business and at an organisation-wide level, with appropriate levels of competent resources available to execute the plans.
- Ensure implementation of process safety risk mitigation plans and reviews of progress versus the plans at site and corporate level.

- Monitor that corrective actions are applied and closed out promptly following audits and after thorough root cause investigations of all incidents or potentially high consequence near misses.

Directors and boards need to examine their own behaviours, both individually and collectively, against the guidance - and, if they see that they fall short of the standards it sets, to change what they do to become more effective leaders in managing health, safety and environment and the development of high reliability organisations. The OECD Corporate Governance guidance will help organisations find the best ways to lead and promote health, safety and environment management, and therefore meet its legal obligations.

PSLG Principles of Process Safety Leadership

In 2009 industry across major hazard sectors represented on PSLG signed up to a set of 'Principles of Safety Leadership' following discussions between the CBA, the PSLG and the HSE. Notwithstanding the more recent OECD Corporate Governance guidance outlined above, the PSLG Principles are still relevant and contain some valuable pointers to how businesses can ensure effective leadership of process safety.

The PSLG Principles agreed are as follows:

- Clear and positive safety leadership is at the core of managing a major hazard business and is vital to ensure that risks are effectively managed;
- Safety leadership requires Board level involvement and competence. For companies with Boards located outside the UK then the responsibility to deliver this leadership rests with the most senior UK managers;
- Good safety management does not happen by chance and requires constant active engagement;
- Board level visibility and promotion of safety leadership is essential to set a positive safety culture throughout the organisation;
- Monitoring safety performance based on both leading and lagging indicators is central to ensuring business risks are being effectively managed;
- Publication of safety performance information provides important public assurance about the management of risks by an organisation;
- Sharing best practice across industry sectors, and learning and implementing lessons from relevant incidents in other organisations, are important to maintain the currency of corporate knowledge and competence.

The principles below are the basic framework of the process.

1) Safety accountabilities should be defined and championed at Board level
   - Board members, senior executives and managers should be accountable for safety leadership and performance. This should be embodied in:
     - the organisation's Safety, Health & Environment policies;
     - job descriptions; and
     - the overall company culture
2) At least one Board member should be conversant in safety management
   - This is to allow them to effectively advise the Board of the status of safety risk management within the organisation and of the safety implications of Board decisions
3) Appropriate resources should be made available to ensure a high standard of safety management throughout your organisation
   - Staff with safety management responsibilities should have or need to develop an appropriate level of competence. This is often achieved by a combination of external training and internal 'on the job' experience.
4) Organisations should have developed a programme for the promotion of safety
   - The Board representative and members of senior management who are actively engaged with direct employees and contract staff should underline the importance of

safety leadership, develop and support the maintenance of a positive safety culture within an organisation

5) Systems and arrangements should be in place to ensure the active involvement of the workforce in the design of safety controls and in the review of safety performance.
   - Employee 'buy in' to the safety culture of the organisation is essential, people work with systems they can relate to rather than those that are 'foisted upon them'.

6) Business risks, relating to safety, should be assessed and reviewed regularly.
   - Are risk assessments reviewed regularly, remedial action taken where appropriate and is this documented?
   - Does the organisation have a documented 'business continuity' plan in place to cover all eventualities?

7) "Leading" and "lagging" safety indicators should be in use within an organisation.
   - Companies should have in place metrics for process safety alongside other metrics such as financial and production metrics.
   - Metrics should be a combination of leading indicators which give indications of potential safety issues and that SMS controls are in place as well as lagging indicators which measure outputs of performance. These are primarily utilised by major hazard or COMAH sites but can be of benefit to all levels of business to identify and monitor critical activities that could lead to a major accident.

8) An organisation should actively engage with others within the sector and elsewhere to share good practice and information on safety incidents that may benefit others.
   - Companies should have mechanisms and arrangements in place to incorporate learning from others within their safety management programmes.

9) Systems and arrangements should be in place to ensure the retention of corporate knowledge relating to safety management.
   - Such arrangements should include information on the basis of the safety design concept of the plant and processes, plant and changes, and any past incidents that impacted on safety integrity and the improvements adopted to prevent a recurrence.

High Reliability Organisations

A High Reliability Organisation has been defined as one that delivers its product relatively error-free over a long period of time. Two key attributes of high reliability organisations are that they:

- have a chronic sense of unease, i.e. they lack any sense of complacency. For example, they do not assume that because they may not have had an incident for ten years, one won't happen imminently;
- make strong responses to weak signals, i.e. they set their threshold for intervening very low. If something doesn't seem right, they are very likely to stop operations and investigate.

Achieving a high reliability organisation depends on integrating human and organisational factors including the roles of operators, supervisors and managers. The following factors are important for delivery of effective process safety leadership within a high reliability organisation.

- **Leadership**, by:
  - giving safety a high priority in the organisation's business objectives;
  - having high visibility of management's commitment to safety;
  - delivery of effective safety management systems.
- **Effective process safety management**:
  - Hazard identification and appropriate layers of protection;
  - Instrumentation, including alarm systems, that allow front-line staff, particularly control room operators, to reliably detect, diagnose, and respond to potential incidents;
  - Delivery of effective safety management systems.
  - Effective management of change, including organisational change as well as changes to plant and processes.
  - Measurement of process safety performance.
- **Organisational issues:**
  - Clear understanding and definition of roles and responsibilities, and assurance of competence in those roles.

  - Appropriate staffing, shift work arrangements and working conditions to prevent, control and mitigate major accident hazards.
  - Setting and implementing a standard for effective and safe communication at shift and crew change handover.
  - Organisational change, and management of contractors.
- **Learning from experience:**
  - Investigation of incidents and near misses.
  - Availability of records for periodic review.
- **Communication:**
  - A positive safety culture requires effective channels for top-down, bottom-up and horizontal communications on safety matters.
- **Involvement of staff:** Active employee participation is a positive step towards controlling hazards. In particular:
  - ownership for safety, particularly with provision of safety training;
  - safety specialists should play an advisory or supporting role;
  - it should be easy to report safety concerns;
  - feedback mechanisms should be in place to inform staff about any decisions that are likely to affect them.
- **A just and open culture:** Companies or organisations with a blame culture over-emphasise individual blame for human error at the expense of correcting defective systems:
  - organisations should develop a no-blame culture that encourages reporting of near-misses and highlights areas for process safety improvement, rather than fear of blame for errors;
  - those investigating incidents should have a good understanding of the mechanism for human error;
  - management should demonstrate care and concern for employees;
  - employees should feel that they are able to report issues or concerns without fear of blame or possible disciplinary action.

The OECD Guidance referred to above sets out the essential elements of behaviour necessary for an organisation to demonstrate that it is leading process safety and working towards being a high reliability organisation, and the self-assessment tool incorporated in the guidance will enable leaders to monitor progress towards this.

Leadership and development of a positive safety culture

The importance to an organisation of a positive safety culture has been referred to above several times, including in the OECD Corporate Governance guidance and the PSLG Principles of Process Safety. Poor safety culture has been found to be a significant causal factor in major accidents across many sectors and over many decades, including incidents such as Texas City, Chernobyl, Bhopal, the Herald of Free Enterprise, and several major rail crashes.

The leadership of senior managers, and the commitment from the chief executive, is vital to the development of a positive safety culture. The Baker Panel Report following Texas City drew specific attention to the importance of:

- Process safety leadership at all levels of an organisation;
- Implementing process safety management systems; and
- Developing a positive, trusting and open safety culture.

CSB's Investigation Report (2) into the Texas City Refinery Explosion also identified safety culture as a key issue requiring leadership of senior executives. It was particularly critical of the lack of a reporting and learning culture, and of a lack of focus on controlling major hazard risk.

Guidance

The safety culture of an organisation has been described (HSG48) (3) as the shared values, attitudes and patterns of behaviour that give the organisation its particular character.

The term 'safety climate' has a very similar meaning to safety culture. Put simply, the term safety culture is used to describe behavioural aspects (what people do), and the situational aspects of the company (what the company has). The term safety climate is used to refer to how people feel about safety in the organisation (HSG48, Safety culture Human Factors Briefing Note No 763) (3).
When implementing guidance on leadership and safety culture, duty holders should ensure that:

- Clear goals and objectives are set, and made visible by leadership throughout the organisation;
- Expectations are translated into procedures and practices at all levels;
- These procedures and practices are commensurate with the risk, consequence of failure, and complexity of the operation;
- All hazards are considered when implementing these expectations – personal and process safety, security and environmental;
- The workforce actively participates in the delivery of these expectations;
- All members of the workforce are – and believe they are – treated fairly in terms of their responsibilities, accountabilities, access to leaders, rewards and benefits;
- There is open communication and consultation across all levels of the organisation;
- Relevant metrics are set and performance assessed at appropriate intervals to determine the effectiveness of leadership across the organisation;
- Lessons from incidents/near misses are shared across the organisation.
- When the organisation uses the services of others these principles should be used, commensurate to the task they perform.

The Baker Panel Report (4) includes a questionnaire used for a process safety culture survey, i.e. it is about process safety, and not personal safety, and could be adapted as required for a review of safety culture/climate.

The CSB Investigation Report (2) includes an analysis of safety culture, in relation to the Texas City explosion, and recommendations for improvement.

Reducing error and influencing behaviour HSG48 (3) summarises the organisational factors associated with a health and safety culture, and proposes a step-by-step approach to improving this culture.

HSE's Human Factors Toolkit Briefing Note 7 (5) is a concise briefing note providing a useful summary of the characteristics of a healthy safety culture.

"Leadership for the major hazard industries" (INDG277) (6) provides very useful guidance for executive directors and other senior managers reporting to board members. It is divided into four sections:

- Health and safety culture.
- Leadership by example.
- Systems.
- Workforce.

HSE's Research Report RR367 (7) provides a review of safety culture and safety climate literature. It is a comprehensive research report that highlights key aspects of a good safety culture. "Involving employees in health and safety" (HSG217) (8) provides more detailed guidance on employee involvement.

Summary

Duty holders should ensure that their executive management provides effective leadership of process safety to develop a positive, open, fair and trusting process safety culture. A review of the characteristics of their leadership and process safety culture should be carried out. The review should:

- be owned at a senior level within the company;
- be developed as appropriate for each site;
- apply to all parties operating at each site and

- lead to the development of action plans to ensure that a positive process safety culture is developed and maintained.

Process Safety Management and Organisational Issues

The Buncefield report identified some key issues relating to Process Safety Management, some with strong links to Organisational and Human Factors Issues. This section provides the key guidance for those Process Safety Management and Human Factors and Organisational issues.

Process Safety Management

Process safety management involves a particular type of risk management – identifying and controlling the hazards arising from process activities, such as the prevention of leaks, spills, equipment malfunctions, over-pressures, excessive temperatures, corrosion, metal fatigue, and other similar conditions. Process safety programmes focus on, among other things, the design and engineering of facilities; hazard assessments; management of change; inspection, testing and maintenance of equipment; effective alarms; effective process control; procedures; training and competence of personnel; and human factors.

One of the recommendations of the Baker Panel Report (4) following the Texas City Refinery explosion was that companies should establish and implement an integrated and comprehensive process safety management system that systematically and continuously identifies, reduces and manages process safety risks at its US refineries. The CSB Investigation Report (2) made similar recommendations. The principles embodied in this report are recognised by HSE as 'good practice.

Guidance

The Center for Chemical Process Safety (CCPS) of the American Institution of Chemical Engineers (AIChE) on its website (9) gives guidelines on the arrangements that should be in place for effective Process Safety Management. This guidance for risk based process safety identifies good practice on process safety management. It is structured as follows:

- Commitment to process safety:
  - process safety culture;
  - process safety competency;
  - stakeholder outreach.
  - workforce involvement;
  - compliance with standards;
- Understand hazards and risk:
  - hazard identification and risk analysis.
  - process knowledge management.
- Manage risks:
  - operating procedures;
  - management of change;
  - emergency management.
  - operational readiness;
  - safe work practices;
  - training and performance assurance;
  - contractor management;
  - conduct of operations
- Learn from experience:
  - auditing;
  - management review and continuous improvement
  - measurement and metrics;
  - incident investigation;

The key elements of PSM and learning as related to the Buncefield incident are addressed in more detail in the next section.

The HSE internal document Process Safety Management Systems (10) also identifies principles of process safety management. Although intended for process safety management of offshore installations, many of the principles are equally applicable onshore. Key points are:

- There is no single 'correct' model of a process safety management system; some companies have separate safety management systems for different sites, whereas others may adopt a more functional approach.
- Some companies give greater emphasis than others to corporate procedures. Each should adopt arrangements that are appropriate for its business and culture.
- In principle, different standards and procedures could be used within each of the sites or functions. In practice, however, systems need to be developed within the constraints of the corporate SMS, and there will inevitably be areas of overlap.
- There is no legal requirement for a company to have a policy statement that is specific to process safety management, but it is recognised good practice, and helps to define the management requirements.
- A good policy statement, or supporting documentation, would indicate the organization's approach to process safety management. This would include commitment to matters such as:
    - principles of inherent safety;
    - a coherent approach to hazard and risk management;
    - communication of the hazard and risk management process;
    - ensuring competence, and adequacy of resources;
    - recognition of the role of human failure – particularly unintentional human failure – on process safety;
    - assurance that the reliability of process safety barriers that depend on human behaviour and performance are adequately assessed;
    - working within a defined safe operating envelope;
    - careful control of changes that could impact on process safety;
    - maintaining up to date documentation;
    - maintenance and verification of safety critical systems;
    - line management monitoring of safety critical systems and procedures;
    - setting of process safety performance indicators;
    - independent audits of management and technical arrangements;
    - investigation and analysis of incidents to establish root causes;
    - reviewing process safety performance on a regular (e.g. annual) basis;
    - continuous improvement, with regularly updated improvement plans;
    - principles of quality management, e.g. ISO 9000 (11)

The COMAH Regulations (12) require duty holders to set out a Major Accident Prevention Policy (MAPP). This would be the logical place to record policies relating to process safety management. Duty holders also need to ensure that they have effective arrangements to implement each element of the policy.

Summary

Duty holders should ensure they have implemented an integrated and comprehensive management system that systematically and continuously identifies, reduces and manages process safety risks, including risk of human failure.

Key Process Safety Learning and Principles Arising from the Buncefield Incident

The Buncefield investigation report (1) identified a number of key areas of learning with respect to Process Safety Management. A summary of the key points and systems which companies should specifically consider is detailed below. The sections mirror those from the relevant CCPS guidance. Sections within the CCPS guidance which are not relevant to the learning from Buncefield are excluded.

Commitment to process safety:

Leadership with respect to Process Safety and setting a process safety culture has already been discussed above.

i. process safety culture;
ii. process safety competency;
iii. stakeholder outreach;
iv. workforce involvement; and,
v. compliance with standards.

Active employee participation is a positive step towards controlling process safety (and other) hazards. In particular arrangements should be in place such that all employees feel:

- ownership for safety, particularly with provision of safety training;
- that safety specialists should play an advisory or supporting role;
- that it should be easy to report safety concerns; and,
- that feedback mechanisms should be in place to inform staff about any decisions that are likely to affect them.

This should be supported with a just and open culture since companies or organisations with a blame culture over-emphasise individual blame for human error at the expense of correcting defective systems. To support this:

- those investigating incidents should have a good understanding of the mechanism for human error;
- management should demonstrate care and concern for employees; and
- employees should feel that they are able to report issues or concerns without fear of blame or possible disciplinary action.

Understand hazards and risk:

Hazard identification, layers of protection, and assessment of their effectiveness
Developing appropriate process safety controls and performance indicators involves identifying the risk control systems in place for each scenario, and determining which of these are important to prevent or control the various challenges to integrity (HSG254 Developing process safety indicators) (13). It is therefore essential to be able to provide an overview of:

- the potential major accidents and what can go wrong;
- the barriers to prevent major accidents (i.e. layers of protection); and
- risk control systems in place to control these risks.

Various techniques are in use within the industry to systematically give an overview of the layers of protection and to evaluate their effectiveness.

Guidance on hazard identification and risk assessment
One of the principles of COMAH is that the duty holder should develop and implement procedures to systematically identify and evaluate hazards arising from their activities in both normal and abnormal conditions (L111) (12). These procedures should address human factors with the same rigour as engineering and technical issues, and should be described in the SMS. There should also be systematic procedures for the definition of measures to prevent major accidents and mitigate their consequences.

Techniques used within the industry to help make decisions about the measures necessary include:

1. bow-tie diagrams;
2. layer of protection analysis;
3. fault/event trees; and,
4. tabular records of the hierarchy of control measures.

Summary

Duty holders should ensure that they have suitable techniques to demonstrate and assess their layers of protection for prevention and mitigation of major accident scenarios.

Manage risks:

Management of plant and process changes.

Experience (for example the Flixborough disaster in 1974) (14) has shown management of change (MOC) to be an essential factor in the prevention and control of major accidents. This section discusses plant and process changes. Management of organisational change is discussed under 'Organisational change and management of contractors'

Duty holders should adopt and implement management procedures for planning and control of all changes in plant, processes and process variables, materials, equipment, procedures, software, design or external circumstances which are capable of affecting the control of major accident hazards. This approach should cover permanent, temporary, and urgent operational changes, including control of overrides/inhibits, as well as changes to the management arrangements themselves.

Guidance

The Guide to the COMAH Regulations L111 (12) summarises the range of changes that should be subject to management of change control procedures.

Each site should have guidance to help its personnel to determine the difference between like-for-like replacement and a change. This should cover items such as:

- valves;
- piping and flanges;
- vessels/tanks;
- rotating machinery;
- instrumentation;
- software;
- process materials;
- operational changes;
- maintenance procedures;
- purchasing changes; and,
- equipment relocation.

Guidance on Management of Change for COMAH establishments is given in the HSE's Safety Report Assessment Manual (15)

MOC processes which align to current good practice may be further improved using the UKPIA self-assessment tool, which provides a suitable methodology for advancing an organisation's MOC processes to achieve excellence in process safety. (16)

Summary

Duty holders should ensure they have suitable guidance for their staff about what constitutes a plant or process change, and that they have suitable arrangements in place for management of the range of permanent, temporary, and urgent operational changes.

Emergency Management

The management of the Buncefield Incident resulted in a major review of emergency preparedness arrangements that should be in place for COMAH sites. The arrangements are summarised in section 5 of this report which also includes links to the supporting documentation that has been developed by the task group formed to address this topic.

Organisational change and management of contractors

Effective management of change, including organisational change as well as changes to plant and processes, is vital to the control of major accident hazards. This section deals with organisational change, particularly change involving contracting out of core business activities. Management of changes to plant and processes is discussed above.

Organisational changes that can adversely affect the management of major hazards include various types of internal restructuring, re-allocation of responsibilities, changes to key personnel, and contractorisation. Failure to manage organisational change adequately has been found to be a factor in major accidents.

In high-hazard industries policies regarding use of contractors or outsourcing need to be clear. If safety-critical work is to be contracted out then the company should ensure that it remains an 'intelligent customer'. In other words, it should retain adequate technical competence to judge whether, and ensure that, work is done to the required quality and safety standards.

Guidance

A guide to the Control of Major Accident Hazard Regulations 1999 L111 (12) summarises the range of changes, including changes to people and the organisation, which should be subject to management of change control procedures.

HSE's Information Sheet Organisational change and major accident hazards CHIS7 (17) sets out a framework for managing organisational changes, and is recommended for high-hazard industries. Principles for the assessment of a licensee's intelligent customer capability and Contractorisation are documents used internally by HSE's Nuclear Directorate to assess and inspect contractorisation and intelligent customer issues. (18)

Managing contractors HSG159 (19) is a guide for employers in managing contractors in the chemical industry.

The use of contractors in the maintenance of the mainline railway infrastructure is an HSC review of contractorisation (20) in the railways (primarily) and other high hazard industries, including nuclear, offshore, and onshore chemicals.

Health and safety management systems interfacing provides a methodology for interfacing/integrating safety management systems between clients and contractors.

CHIS7 (17) describes the types of organisational change that can affect the management of major accident hazards. These include:

- business process engineering;
- de-layering;
- introduction of self-managed teams;
- multi-skilling;
- outsourcing/contractorisation;
- mergers, demergers and acquisitions;
- downsizing;
- changes to key personnel;
- centralisation or dispersion of functions; and,

- changes to communication systems or reporting relationships.

The main focus of CHIS7 (17) is on changes at operational and site level and it is specifically about major accident prevention. It sets out a three-step framework for managing change, as follows:

Step 1 – Getting organised for change
Step 2 – Assessing risks
Step 3 – Implementing and monitoring the change.

Contractorisation, and intelligent customer capability

A principle, well known within the nuclear industry, is that duty holders should maintain the capability within their own organisations to understand, and take responsibility for, the major hazard safety implications of their activities. This includes understanding the Safety Case for their plant and the limits under which it must be operated. It is known as 'intelligent customer capability'. (See Principles for the assessment of a licensee's intelligent customer capability and Contractorisation (18))

As an intelligent customer, the management of the facility should know what is required, should fully understand the need for a contractor's services, should specify requirements, should supervise the work and should technically review the output before, during and after implementation. The concept of intelligent customer relates to the attributes of an organisation rather than the capabilities of individual post holders.

CHIS7 (17) extends this principle more widely to high hazard industries, stating that, if you contract out safety-critical work, you need to remain an 'intelligent customer'.

An organisation that does not have intelligent customer capability runs the risk of:

- not understanding its safety report, and operating unsafely;
- not having appropriate staff to adequately deal with emergencies;
- procuring poor safety advice, or wrongly implementing advice received;
- not recognising that significant plant degradation or safety critical events are arising, or not addressing them correctly;
- not identifying the requirements for safety-critical projects, modifications or maintenance, or carrying them out inadequately; or,
- employing inadequate contractors or agency staff.

A duty holder who proposes to contractorise should have organisational change arrangements in place to review the proposal and demonstrate that safety will not be jeopardised. Choices between sourcing work in-house or from contractors should be informed by a clear policy that takes due account of the potential major accident implications of those choices. The approach to identifying and managing core competencies and sustaining an intelligent customer capability should be set out in the safety management system.

The guidance (Principles for the assessment of a licensee's intelligent customer capability and Contractorisation) (18) makes no reference to the concept of 'contracting-in' an intelligent customer resource e.g. for the evaluation of other contractors. Wherever practicable, this resource should be in-house.

Managing contractors HSG159 (19) is aimed at small to medium sized chemicals businesses and primarily focuses on ensuring safe working practices of contractors when on site to do specific jobs. It does contain a checklist to help duty holders to gain an overview of health and safety in managing contractors, and this contains statements that would infer some requirement for intelligent customer capability, such as:

- staff know their responsibilities for managing contractors on site;
- staff responsible have enough knowledge about the risks and preventative measures for all jobs involving contractors; and
- staff responsible know what to look for when checking that contractors are working safely, and know what action to take if they find problems.

Management systems interfacing

HSG159 (19) also includes a checklist of items (organised under the headings of: Policies; Organising; Planning and implementing; Monitoring; Reviewing and Learning) to give an overview of a client's arrangements for managing contractors.

This checklist deals with relevant elements of a safety management system (SMS) that need to be considered when engaging contractors. It doesn't deal specifically with how the SMS of the client might interface with that of the contractor, but it is a useful starting point.

On major hazard sites, the more the contractor becomes involved with managing core business activities of the site, the more important it becomes for formal interfacing/integration of the SMS of the client with that of the contractor.

Principles for the assessment of a licensee's intelligent customer capability (18) states that 'where complex management arrangements and several duty holders contribute to complying with the requirements, HSE will usually expect a duty holder to describe the arrangements for 'interfacing' with others'. However, it provides no further guidance on how this might be done.

The UK offshore industry has developed guidance (21) for interfacing health and safety management systems between duty holders involved in shared activities. The guidance deals with all the elements of an SMS including issues such as:

- identifying minimum training needs and competencies;
- identifying responsibilities for training and competence;
- agreement of criteria and mechanisms for handling changes;
- responsibility for hazard identification and risk assessment of changes; and,
- identifying key safety performance indicators.

The extent to which the guidance needs to be applied is a function of the risk associated with the shared activities. Thus, before developing SMS interfacing arrangements, a risk assessment must be undertaken by the parties involved. This may be a simple matter of making a judgement about the degree of hazard and duration of activity.

It would seem to be potentially useful (with minor tailoring) for onshore application, particularly where a significant element of core business activity is contracted out (e.g. maintenance).

Retention of corporate memory

The duty holder also needs to have adequate arrangements for retention of corporate memory. Principles for the assessment of a licensee's intelligent customer capability discusses requirements for retention of corporate memory in the context of the nuclear industry, and CHIS7 (17 and 18) briefly refers to it in the wider context of organisational change and major accident hazards.

The most common circumstances under which the loss of corporate memory could occur are:

- Staff turnover: The accumulated knowledge of the experienced staff, which is often extensive, can be lost when knowledge is not transferred from the outgoing to the incoming staff.
- Unavailability of information: This occurs when information is not recorded, or not archived appropriately, or when information is not provided through pre-job briefing. Of particular importance is the availability of the as-built design knowledge that changes over the life of the facility.
- Ineffective use or application of knowledge: Despite the existence of information within the organisation, individuals may not be aware or may not understand they had access to information.

To counter the above, duty holders should develop succession plans to respond to situations involving staff movements and have in place formal arrangements for knowledge archiving and transfer of information.

Summary

Duty holders should ensure that:

- there is a suitable policy and procedure for managing organisational changes;
- there is a suitable policy and procedure for retention of corporate memory;
- should ensure that it retains adequate technical competence and 'intelligent customer' capability when work impacting on the control of major accident hazards is outsourced or contractorised; and,
- suitable arrangements are in place for management and monitoring of contractor activities. in addition to retaining intelligent customer capability, they consider using industry guidance for SMS interfacing where core business is contracted out.

Learn from experience:

Audit and Management Review.

The terms 'audit' and 'review' are used for two different activities (see L111 (12) and HSG65 (22)). In addition to the routine monitoring of performance (i.e. active monitoring) the duty holder should carry out periodic audits of the SMS as a normal part of its business activities.

An audit is a structured process of collecting independent information on the efficiency, effectiveness, and reliability of the total SMS. It should lead to a plan for corrective action. In this context 'independent' means independent of the line management chain.

Reviews are a management responsibility. They need to take account of information generated by the measuring (active and reactive monitoring) and auditing activities, and how to initiate remedial actions.

The requirements for audit and review are well established. The main issue is to ensure that process safety is adequately included in audit and review programmes.

Guidance on auditing

Auditing provides an independent overview to ensure that appropriate management arrangements (including effective monitoring) are in place, together with adequate risk control systems and workplace precautions.

Various methods can achieve this. AIChE guidelines (Guidelines for auditing process safety management systems (23) and Guidelines for technical management of chemical process safety (24)) draw a distinction between process safety auditing, and process safety management systems (PSMS) auditing.

The focus of process safety auditing is the identification and evaluation of specific hazards (e.g. inspecting hardware and finding the absence of a relief device, or an independent trip system). PSMS auditing, however, involves assessment of the management systems that ensure ongoing control (e.g. the management systems in place to ensure that pressure relief devices have been designed, installed, operated, and maintained in accordance with company standards).

Both types of audit are important. The process safety audit addresses a particular hazard found at a specific time. It could lead to correction of the hazard without addressing the underlying reason why the hazardous condition came to exist. The PSMS audit addresses the management systems intended to preclude the creation of hazards.

The audit programme should include a selection of range of controls in place for preventing or mitigating the risk of major accidents. These include, but are not limited to:

- commitment to process safety management;
- risk assessment procedures;
- effectiveness of process safety barriers;
- definition of roles and responsibilities;
- ensuring competence;
- assessment of staffing arrangements;
- management of fatigue associated with shift work;
- safety-critical communications, including shift handover;
- management of organisational change;
- management of contractors;
- retention of intelligent customer capability;
- retention of corporate memory;
- operational planning, and consignment transfer procedures;
- safety-critical operating procedures;
- provision of information;

- document control procedures;
- control of overrides/inhibits of safety-critical instrumentation systems;
- alarm systems;
- inspection and maintenance of safety-critical systems;
- permit to work and isolation arrangements;
- detection measures for loss of containment;
- integrity of secondary and tertiary containment measures;
- control of ignition sources;
- fire protection measures;
- management of plant and process changes;
- maintenance of records;
- active monitoring arrangements;
- reactive monitoring arrangements;
- setting and reviewing of process safety performance indicators;
- investigation procedures/analysis of underlying causes;
- sharing of lessons learned;
- emergency procedures/testing of emergency plans; and,
- review arrangements/improvement plans.

Such audits are formal and infrequent. Duty holders may decide to audit a small range of activities on a more frequent basis (e.g. yearly), or a more extensive range on a less frequent basis (e.g. 3–5 years). The duty holder should decide the range and scope of its audit programme, taking into account such factors as audits/inspections imposed by others (e.g. the CA, parent companies or joint venture partners, insurers, trade associations), and the extensiveness of the active monitoring programme.

Audits that focus primarily on ‘compliance’ (i.e. verifying that the right systems are in place rather than ensuring that they deliver the right safety outcome) are not sufficient.

Guidance on review

Reviewing should be a continuous process undertaken at different levels in the organisation. An annual review should be the norm, but duty holders may decide on a system of intermediate reviews at, for example, department level. The result should be specific remedial actions which establish who is responsible for implementation, with deadlines for completion.

Issues to be considered in the review process include:

- the major accident prevention policy;
- audit programme achievement and findings;
- active monitoring records and findings;
- process safety performance indicators;
- incident/near miss history;
- relevant lessons from incidents etc elsewhere;
- analysis of root/basic causes of incidents and near misses;
- issues from safety committees;
- tracking of safety actions;
- risk assessment status, including reviews against changing standards; and,
- changes of legislation.

Retention of relevant records is necessary for the periodic review of the effectiveness of control measures, and the root cause analysis of those incidents and near misses that could potentially have developed into a major incident.

The following records are considered to be particularly relevant:

- operational plans;
- incidences of high level alarm activation;
- incidences of high-high level/trip activation;

- maintenance/proof testing for high level trip and alarm systems;
- faults discovered on high level alarm or protection systems;
- stock records to demonstrate compliance with a stock control policy;
- plant/process changes;
- organisational changes;
- approval/operation of inhibits/overrides of safety systems;
- competence/training records;
- shift work/overtime records;
- shift handover records;
- permits to work;
- risk assessments;
- method statements, and,
- active monitoring records.

Summary

Duty holders should adopt and implement audit plans defining:

- the areas and activities to be audited, with a particular focus on process; safety/control of major accident hazards;
- the frequency of audits for each area covered;
- the responsibility for each audit;
- the resources and personnel required for each audit;
- the audit protocols to be used;
- the procedures for reporting audit findings; and
- the follow-up procedures, including responsibilities.

Duty holders should ensure that they have implemented suitable arrangements for a formal review of arrangements for control of major accident hazards, including:

- the areas and activities to be reviewed, with a particular focus on process safety/control of major accident hazards;
- the frequency of review (at various levels of the organisation);
- responsibility for the reviews;
- the resources and personnel required for each review;
- procedures for reporting the review findings; and
- arrangements for developing and progressing improvement plans.

Duty holders should identify those records needed for the periodic review of the effectiveness of control measures, and for the root cause analysis of those incidents and near misses that could potentially develop into a major incident. The records should be retained for a minimum period of one year.

Availability of records for periodic review

Retention of relevant records (see earlier list) is necessary for the periodic review of the effectiveness of control measures, and the root cause analysis of those incidents and near misses that could potentially have developed into a major incident.

Guidance

The following records are considered to be particularly relevant:

- Operational plans.
- Incidences of high level alarm activation.
- Incidences of high-high level/trip activation.
- Maintenance/proof testing for high level trip and alarm systems.
- Faults discovered on high level alarm or protection systems.
- Stock records to demonstrate compliance with a stock control policy.
- Operational plans.
- Plant/process changes.
- Organisational changes.
- Approval/operation of inhibits/overrides of safety systems.
- Competence/training records.
- Shift work/overtime records.
- Shift handover records.
- Permits to work.
- Risk assessments.
- Method statements.
- Active monitoring records.

Summary

Duty holders should identify those records needed for the periodic review of the effectiveness of control measures, and for the root cause analysis of those incidents and near misses that could potentially develop into a major incident. The records should be retained for a minimum period of one year.

Measurement and metrics

Measuring performance to assess how effectively risks are being controlled is an essential part of a health and safety management system (see L111 (12) and HSG65 (22)). Active monitoring provides feedback on performance before an accident or incident, whereas reactive monitoring involves identifying and reporting on incidents to check the controls in place, identify weaknesses and learn from mistakes.

The presence of an effective personal safety management system does not ensure the presence of an effective process safety management system. The Report of the BP U.S. Refineries Independent Safety Review Panel (the 'Baker Panel report'), following the Texas City refinery explosion in 2005 (4), found that personal injury rates were not predictive of process safety performance at five US refineries.

Used effectively process safety indicators can provide an early warning, before catastrophic failure, that critical controls have deteriorated to an unacceptable level. The use of process safety performance indicators fits between formal, infrequent audits and more frequent inspection and safety observation programmes. It is not a substitute for auditing, but a complementary activity.

The main reason for measuring process safety performance is to provide ongoing assurance that risks are being adequately controlled. In order to measure safety performance, many duty holders have incorporated leading and lagging indicators, also known as 'metrics' or 'key performance indicators', into their safety management systems. Managers use these metrics to track safety performance, to compare or benchmark safety performance.

Many organisations rely on auditing to highlight system deterioration. However, audit intervals can be too infrequent to detect rapid change, or the audit may focus on 'compliance', i.e. verifying that the right systems are in place rather than ensuring that systems are delivering the desired safety outcome (see HSG254 (13)).

Many organisations do not have good information to show how they are managing major hazard risks. This is because the information gathered tends to be limited to measuring failures, such as incident or near misses. System failures following a major incident frequently surprise senior managers, who believed the controls were functioning as designed (see HSG254 (13)).

Guidance

Active monitoring

Active monitoring is primarily a line management responsibility (see HSG65 (22)). It should be distinguished from the requirement for 'independent' audits, which are a separate activity. HSG65 refers to auditing as the structured process of collecting independent information on the efficiency, effectiveness, and reliability of the total health and safety management system, and drawing up plans for corrective action.

Active monitoring should include inspections of safety-critical plant, equipment and instrumentation as well as assessment of compliance with training, instructions and safe working practices.

Active monitoring gives an organisation feedback on its performance before an incident occurs. It should be seen as a means of reinforcing positive achievement, rather than penalising failure after the event. It includes monitoring the achievement of specific plans and objectives, the operation of the SMS, and compliance with performance standards. This provides a firm basis for decisions about improvements in risk control and the SMS.

Duty holders need to decide how to allocate responsibilities for monitoring at different levels in the management chain, and what level of detail is appropriate. In general, managers should monitor the achievement of objectives and compliance with standards for which their subordinates are responsible. Managers and supervisors responsible for direct implementation of standards should

monitor compliance in detail. Above this immediate level of control, monitoring needs to be more selective, but provide assurance that adequate first line monitoring is taking place.

Various forms and levels of active monitoring include:

- examination of work and behaviour;
- systematic examination of premises, plant and equipment by managers, supervisors, safety representatives, or other employees to ensure continued operation of workplace risk precautions;
- the operation of audit systems; and,
- monitoring of progress towards specific objectives, e.g. training/competence assurance objectives.

Many of these topics are not specific to process integrity, but are equally applicable to all areas. Topics of particular relevance to process integrity include:

- change control;
- process safety study (e.g. HAZOP or PSA) close out;
- control of process plant protection systems/inhibits etc;
- control of alarms/alarm system status;
- operating procedures, including consignment transfer procedures and stock reconciliation procedures;
- shift handover procedures;
- management of fatigue and shift work;
- maintenance of safety-critical systems; and,
- control of contractors.

They should also include other key systems that are equally relevant to preventing a major incident, such as:

- workplace risk assessments;
- permit to work systems;
- isolation standards;
- controls at high pressure/low pressure interfaces; and,
- control of relief devices etc.

Reactive monitoring

Reactive monitoring involves identifying and reporting on incidents to check the controls in place, identify weaknesses and learn from mistakes (see L111 (12) and HSG65 (22)). It includes:

- identification and analysis of injuries/causes of ill health;
- identification and analysis of other incidents, near misses, and weaknesses or omissions in performance standards;
- assessing incident/near miss potential;
- investigation and identifying remedial actions to deal with root causes;
- communication of lessons learned;
- tracking of remedial actions arising from incidents/near misses etc.; and,
- contributing to the corporate memory.

Process safety performance indicators

HSE guidance HSG 254 - Developing process safety indicators: A step-by-step guide for chemical and major hazard industries (13) outlines six main stages needed to implement a process safety management system. It provides a methodology for leading and lagging indicators to be set in a structured way for each critical risk control system within the process safety management system.

OECD has also developed Guidance on Safety Performance Indicators to assess the success of chemical safety activities (25).

The Chemical Business Association and UK Warehouse Association, in conjunction with HSE, have developed and published Safety Performance Leading Indicators guidance to assess activities within warehouses and SME premises (26).

Leading indicators are a form of active monitoring focused on a few critical risk control systems to ensure their continued effectiveness. They require a routine systematic check that key actions or activities are undertaken as intended. They can be considered as measures of process or inputs essential to deliver the desired safety outcome.

Lagging indicators are a form of reactive monitoring requiring the reporting or investigation of specific incidents and events to discover weaknesses in that system. These incidents represent a failure of a significant control system that guards against or limits the consequences of a major incident.

The six key stages identified in the guidance are:

Stage 1 Establish the organisational arrangements to implement the indicators.
Stage 2 Decide on the scope of the measurement system; consider what can go wrong and where.
Stage 3 Identify the risk control systems in place to prevent major accidents. Decide on the outcomes for each and set a lagging indicator.
Stage 4 Identify the critical elements of each risk control system (i.e. those actions or processes that must function correctly to deliver the outcomes) and set leading indicators.
Stage 5 Establish the data collection and reporting system.
Stage 6 Review.

Summary

Duty holders should ensure that a suitable active monitoring programme is in place for key systems and procedures for the control of major accident hazards.

Duty holders should develop an integrated set of leading and lagging performance indicators for effective monitoring of process safety performance.

Investigation of incidents and near misses.

As technical systems have become more reliable, the focus has turned to human causes of accidents. The reasons for the failure of individuals are usually rooted deeper in the organisation's design, decision-making, and management functions.

HSG48 (3) gives several examples of major accidents where failures of people at many levels (i.e. organisational failures) contributed substantially towards the accident. Human factors topics of relevance to process integrity include:

- ergonomic design of plant, control and alarm systems;
- style and content of operating procedures;
- management of fatigue and shift work;
- shift/crew change communications; and
- actions intended to establish a positive safety culture, including active monitoring.

Investigation procedures should address both immediate and underlying causes, including human factors.

Guidance

HSG65 (22) is a suitable reference on investigation of incidents and near misses. Not all events need to be investigated to the same extent or depth. Duty holders need to assess each event (for example using a simple risk-based approach) to identify where the most benefit can be obtained. The greatest effort should concentrate on the most significant events, as well as those that had the potential to cause widespread or serious injury or loss.

HSG65 Appendix 5 describes one approach that may be used as a guide for analysing the immediate and underlying causes of effects. Various other approaches are also available, and widely used within the industry. These include various in-house or proprietary systems.

Other suitable references include Human factors in accident investigations (27) and Guidance on investigating and analysing human and organisational factors aspects of incidents and accidents (28).

Summary

Duty holders should ensure they have suitable procedures for:

- identifying incident/near miss potential;
- investigating according to the identified potential;
- identifying and addressing both immediate and underlying causes;
- sharing of lessons learned; and,
- tracking of remedial actions.

Organisational issues

As discussed above the investigation into the Buncefield incident identified a number of organisational and human factors related issues which contributed to the incident. This section summarises the issues arising, the arrangements that should be in place, and provides reference to the relevant good practice from where more guidance can be obtained.

Roles, responsibilities and competence

Clear understanding and definition of roles and responsibilities, and assurance of competence in those roles, are essential to achieve high reliability organisations for the control of major accident hazards. Companies should assess competency requirements for all personnel (including contractors) involved in the management of Major Accident Hazard risks.

Problems have been found in the past, with competence assessment in the UK hazardous industries sector. A review of practices in 2003 indicated that there was a wide variation in standards (29). In some cases companies had developed systematic approaches, and made explicit links to the COMAH risk assessment. Others relied on unstructured on-the-job reviews. The gas plant fatal explosion in Longford, Australia in 1998 (30) is an example of a major incident in which organisational changes and a lack of skills or knowledge led to errors that contributed to the incident.

Organisational changes such as multi-skilling, delayering or downsizing, in which staff are expected to take on a wider range of responsibilities with less supervision, increase the need to assure competence. Duty holders have a responsibility to ensure their medical (including mental) and physical fitness standards are suitable for the risks involved (see Human Factors Briefing Note No 7 Training and competence (5)). Fitness may be impaired through, for example, drink, drugs or fatigue.

Guidance on roles and responsibilities

COMAH guidance L111 (12) identifies a range of personnel for which the roles, responsibilities, accountability, authority, and interrelation of personnel should be identified. They include all those involved in managing, performing or verifying work in the management of major hazards, including contractors.

However, whatever the make-up of the operating function, the precise roles and responsibilities of those involved in it need to be clearly defined, either in job descriptions or elsewhere. This is an essential step for the identification of training needs, and assurance of competence.

Industry guidance on human–computer interfaces and alarm systems is covered in the EEMUA guidance (2007) ‘Alarm systems - A guide to design, management and procurement’ (31). This also discusses the role of the control room operator, and notes how this has changed as control systems have developed and become more sophisticated. The main source of guidance on supervision is Successful health and safety management (HSG65) published by HSE (22). This establishes the importance of supervision, stating that adequate supervision complements the provision of information, instruction and training to ensure that the health and safety policy of an organisation is effectively implemented and developed. Good supervision regimes can form a powerful part of a proper system of management control. It is for the duty holder to decide on the appropriate level of supervision for particular tasks. The level depends on the risks involved as well as the competence of employees to identify and handle them, but some supervision of fully competent individuals should always be provided to ensure that standards are being met consistently.

Organisation of supervision arrangements should ensure:

- an appropriate span-of-control;
- that supervisors are accessible and have the time to actively supervise (i.e. they are not overloaded with administration and meetings); and,
- that supervisors have appropriate inter-personal skills and competence to be effective in the supervisory role.

Duty holders should monitor risk control systems. HSG65 (22) is clear that organisations need to decide how to allocate responsibilities for monitoring at different levels in the organisation, and what level of detail is appropriate. Managers and supervisors responsible for direct implementation of standards should monitor compliance in detail.

Guidance on competence

HSE Briefing Notes No 2 (32), CTI and Energy Institute Briefing Note No. 7 (33) provide useful summaries of requirements for competence management. The Office of Rail Regulation Guide Developing and Maintaining Staff Competence (34) is a particularly useful text on competence management. The principles of this have been incorporated into Competent Authority inspections at COMAH establishments.

Competence is a combination of practical and thinking skills, experience and knowledge. It means the ability to undertake responsibilities and to perform activities to a recognised standard on a regular basis. Training and development seek to create a level of competence for the individual or team, sufficient to allow individuals or teams to undertake the operation at a basic level. Over time, as practical experience grows, operations can be carried out at a more complex level. Training is required not just for normal operation but also for abnormal/upset and emergency conditions etc.

Training alone is not sufficient. Duty holders need to recognise the difference between merely recording a person's experience and training, and assessing their competence (see RR086) (29).

The purpose of a competence management system is to control, in a logical and integrated manner, a cycle of activities that will assure competent performance. The aim is to ensure that individuals are clear about the performance expected of them, that they have received appropriate training, development and assessment, and that they maintain or improve their competence over time.

A key issue is to make sure that on-the-job training is sufficiently well structured, and that the training and assessment is by competent people. In practice this relies heavily on the quality of the procedures for safety-critical tasks. A key piece of evidence for this would be a well-structured plan for training and assessment.

Ongoing assurance of competency (e.g. through refresher training), is also important, as is validation of the understanding of the training provided.

The guidance on maintaining competence includes requirements for monitoring, and reassessing, the performance of staff to ensure performance is being consistently maintained and developed. Guidance is also given on updating of the competence of individuals in response to relevant changes.

The integrity of the competence management system will only be maintained if it is regularly checked against the design, and improvements made when needed. Some form of verification and audit of the system should be undertaken. Verification should support the assessors, check the quality of the competence assessments at a location and individual level, including the competence of the managers operating the system, and ensure the assessment process remains fit for purpose. Audit should inspect the whole competence management system and judge compliance against the defined quality assurance procedures.

A key issue for duty holders to consider is the competence of staff in relation to the control of major accident hazards, and how this is identified, assessed and managed. Major accident hazard competency needs to be appropriately linked to the major accident hazard and risk analysis and key

procedures. The aim is to assure competence in safety critical tasks, and associated roles and responsibilities.

Competency in major accident hazard prevention is necessary at all levels in the organisation, not just the front line. There should be standards set for competency at all levels, and these should be process/job specific.

The research report Competence Assessment for the Major Hazard Industries RR086 (29) is also a very useful reference for COMAH sites. This aims to provide:

- an authoritative view of what comprises good practice in the field of competence assessment in relation to control of major accident hazards; and
- a model of good practice.

The National or Scottish Vocational Qualification (NVQ/SVQ) system can provide some general and some site-specific competencies, but they are not usually linked to major accident hazards. Duty holders of COMAH sites need to adjust their systems to make this link. Although considerable prominence is given to the S/NVQ option, it is recognised that there are other competence assurance systems, including in-house systems, which are also effective.

Process Safety Training Standards

Since 2011 a project has been operational (PSM Project) to develop process safety training standards, on which accredited courses can be based. The PSM Project is a collaborative initiative led by industry but also involving the regulators, trade unions, skills bodies (National Skills Academy and Cogent) and consultant service providers. Standards have been produced for 3 levels – Process Safety Leadership, Management, and Operations. Using this specifically-targeted training, and crucially, embedding it in the business and culture of the organisation, is one way COMAH sites can help demonstrate competence in process safety and the drive for continuous improvement.

Summary

Duty holders should ensure that they have clearly identified the roles and responsibilities of all those involved in managing, performing, or verifying work in the management of major hazards, including contractors in particular, defined the roles and responsibilities of managers and supervisors.

Duty holders should ensure that they have implemented a competence management system, linked to major accident risk assessment, to ensure that anyone whose work impacts on the control of major accident hazards is competent to do so.

Staffing, shift work arrangements, and working conditions

Staffing, shift work arrangements and working conditions are critical to the prevention, control and mitigation of major accident hazards.

Inadequate staffing arrangements were a factor in the explosion at Longford, Australia in 1998 (30). Some high hazard organisations in the UK were setting staffing levels based on steady-state operations.

Staffing levels should be sufficient to react effectively to foreseeable events and emergencies. Duty holders should be able to demonstrate that there are sufficient alert, competent personnel to deal with both normal operation and hazardous scenarios arising from abnormal events. Contract Research Report CRR 348/2001 (37) was commissioned by the HSE to provide a method to demonstrate that staffing arrangements are adequate for hazardous scenarios as well as normal operations.

Fatigue has been cited as a factor in numerous major accidents including Three Mile Island in 1979, Bhopal in 1984, Challenger Space Shuttle in 1986, Clapham Junction in 1988, Exxon Valdez in 1989, and Texas City in 2005 (HSG256 (36), the US Chemical Safety and Hazard Investigation Board's Investigation Report, Refinery Explosion and Fire (2)). Sleepiness is also thought to be the cause of

one in five accidents on major roads in the UK with shift workers being second after young men for risk ('Vehicle accidents related to sleep'). Shift work arrangements, and working conditions, should be such that the risks from fatigue are minimised.

Guidance on safe staffing arrangements

CRR 348/2001 (35) gives a practical method for assessing the safety of staffing arrangements and is supplemented by a user guide: Safe Staffing Arrangements – User Guide for CRR 348/2001 Methodology (37). Other methodologies could also be used, provided they are robust.

The CRR 348/2001 method provides a framework for duty holders to assess the safety of their staffing arrangements with focus on assessing the staffing arrangements for capability to detect, diagnose and recover major accident scenarios. It is a facilitated team based approach taking several days for each study and using control room and field operators as team members.

The method has three key elements:

- definition of representative scenarios (preparation for study);
- physical assessment of the ability of staff to handle each scenario by working through eight decision trees for each scenario (approximately two hours per scenario); and,
- benchmarking of 11 organisational factors using 'ladders' – this is a general assessment by the team and not scenario based (approximately one hour per ladder).

Note that both CRR 348/2001 and associated User Guide are required for the method since the Guide gives an additional benchmarking ladder for assessing automated plant/equipment.

The effectiveness of the method is dependent on selecting a suitably experienced and competent team. The User Guide gives guidance on the team including suggested membership:

- facilitator (familiar with the method);
- scribe;
- three experienced operators (including control room and field operators); and,
- management, shift supervisors and technical specialists as required on a part-time basis.

The basis for the method can be found in HSG48 (3) as an assessment of individual, job and organisational factors. The physical assessment using the eight decision trees for each scenario focus on job factors:

- Decision trees 1–3 assess the capability of the operators to detect a hazardous scenario e.g. is the control room continuously manned?
- Decision trees 4 and 5 assess the capability of the operators to diagnose a hazardous scenario.
- Decision trees 6–8 assess the capability of the operators to recover a hazardous scenario including assessment of communications.

The general benchmarking uses the team to make judgements of performance against a series of graded descriptions (ladders) on 11 factors including:

- situational awareness (workload);
- alertness and fatigue (workload);
- training and development (knowledge and skills);
- roles and responsibilities (knowledge and skills);
- willingness to initiate major hazard recovery (knowledge and skills);
- management of operating procedures (organisational factors); and,
- automated plant and/or equipment (added by User Guide).

Guidance on safe shift work arrangements

An overview is given in Note 10 of HSEs Human Factors Toolkit (38). More comprehensive guidance is given in Managing shift work HSG256 (36), and in the oil and gas industry guide Managing Fatigue Risks in the Workplace. (39)

The introduction to Managing shift work HSG256 outlines the aim of the guidance to improve safety and reduce ill health by:

- making employers aware of their duty under law to assess any risks associated with shift work;
- improving understanding of shift work and its impact on health and safety;
- providing advice on risk assessment, design of shift work schedules and the shift work environment;
- suggesting measures to reduce the negative impact of shift work; and,
- reducing fatigue, poor performance, errors and accidents by enabling employers to control, manage and monitor the risks of shift work.

The main principle of the Health and Safety at Work Act is that those who create risk from work activity are responsible for the protection of workers and the public from any consequences. Generically, the risk arising from fatigue derives from the probability of sleepiness and the increased probability of error.

Consistent with this and Successful health and safety management HSG65 (22), HSG256 (36) details a systematic approach to assessing and managing the risks associated with shift work under the following five headings:

- **Consider the risks of shift work and the benefits of effective management.** For example, fatigue particularly affects vigilance and monitoring tasks particularly on night shifts.
- **Establish systems to manage the risks of shift work**. The need for senior management commitment is highlighted.
- **Assess the risks associated with shift work in your workplace.**
- **Take action to reduce these risks.** The guidance includes a number of useful tables giving non-sector specific examples of factors relating to the design of shift work schedules, the physical environment and management issues such as supervision.
- **Check and review your shift-work arrangements regularly**. Includes suggested performance measures such as the HSE Fatigue and Risk Index Tool and Epworth sleepiness scale.

HSG256 is a comprehensive and practical guide with appendices covering a summary of legal requirements and practical advice for shift workers along with a listing of assessment tools such as the HSE Fatigue and Risk Index Tool. HSG256 should be supplemented by any sector-specific guidance, e.g. the Energy Institute's "Improving alertness through effective fatigue management" (40), or the oil and gas industry guide "Managing Fatigue Risks in the Workplace" (39).

Managing fatigue risks in the workplace is intended primarily as a tool to assist oil and gas industry supervisors and occupational health practitioners to understand, recognise and manage fatigue in the workplace. It sets out to: explain the health and safety risk posed by fatigue; provide the necessary background information on sleep and the body clock; and describe the main causes of fatigue and provide strategies for managing the causes.
Implementation of a fatigue management plan (FMP) in accordance with established guidance is recommended. Managing fatigue in the workplace describes an FMP as a framework designed to maintain, and when possible enhance safety, performance, and productivity, and manage the risk of fatigue in the workplace. FMPs typically contain the components of:

- policy (including a requirement for auditing processes);
- training (to help identify signs and symptoms of fatigue, and to adopt coping strategies);
- tracking incidents/metrics; and
- support (including medical and wellbeing support).

Monitoring of actual shifts worked and overtime, on an individual basis, is a key practical point for duty holders and managers.

Shift handover

Continuing operations over shift handover has been a contributory factor in several previous major accidents, including Piper Alpha, Longford and Texas City. Reducing error and influencing behaviour HSG48 (3) discusses how unreliable communications can result from a variety of problems. It identifies some high-risk communication situations, and some simple steps that can be used to improve communications in the workplace.

HSE's Safety Alert review in early 2006 indicated that many sites had structured shift handover formats in place, but some relied on event-type logs or unstructured logs that did not clearly specify the type of information that needed to be communicated.

The minimum provision is a handover procedure that specifies simple and unambiguous steps for effective communications at shift and crew change. These include carefully specifying what information needs to be communicated, using structured easy-to-read logs or computer displays, ensuring key information is transmitted both verbally and in writing, and encouraging two-way communication.

Guidance

The handover procedure should be based on the principles described in HSG48 (3) or similar guidance available via the HSE website in Human factors: Safety critical communications. It should:

- carefully specify what key information needs to be communicated at shift and crew change, at key positions in the organisation. The requirements may well be different for different positions, but should consider issues such as:
  - product movements, both ongoing and planned;
  - control systems bypassed;
  - equipment not working or out of commission;
  - maintenance and permitry;
  - isolations in force;
  - trips defeated;
  - critical or high priority alarms activated and actions taken;
  - health, safety or environment incidents or events;
  - modifications; and,
  - personnel on site;
- use suitable aids, such as logs, computer displays etc. to provide a structured handover of key information, while aiming to cut out unnecessary information;
- capture key information that needs to be carried forward across successive shifts (e.g. equipment out of service);
- allow sufficient time for handover, including preparation time;
- ensure that key information is transmitted both verbally and in writing;
- encourage face-to-face, and two-way communication, with the recipient asking for confirmation, repetition, clarification etc. as appropriate; and,
- specify ways to develop the communication skills of employees.

The handover procedure should take account of situations that are known to be especially liable to problems, including:

- during maintenance, if the work continues over a shift change;
- during deviations from normal working;
- following a lengthy absence from work (either as a result of a regular long shift break, or individual absence); and,
- handovers between experienced and inexperienced staff.

Techniques that have been reported from the industry, and that duty holders may wish to consider in development of their procedures, include:

- use of electronic logs, with password systems for acceptance;
- systems to project electronic logs onto a screen (for team briefing);

- use of team briefings, e.g. with staggered shift changes between supervisors and operators;
- use of pre-printed paper logs in a structured format; or,
- use of white boards for recording systems that may be out of service for several shifts.

Duty holders must have the facilities and management arrangements necessary to ensure that the procedures set are indeed complied with. These include:

- arrangements to minimise distractions during handover;
- sufficient time set aside for handover to take place;
- instruction and training of employees in handover procedures; and,
- supervision, audit and review to ensure that the procedure is complied with and the necessary information is communicated and understood.

Safety-critical tasks, should generally be scheduled to avoid shift handover times.

Summary

Duty holders should set and implement arrangements for effective and safe communication at shift and crew change handover.

Upper tier COMAH sites should include a summary of the arrangements for effective and safe communication at shift and crew change handover in the next revision of the safety report.

Guidance on Control Room Design, Alarm systems and Ergonomics

Control room working conditions

Control room issues should focus on ensuring operators (both individually and as teams) can develop, maintain and communicate shared situation awareness.

It is well established that shift work and fatigue may affect safety (e.g. HSG48 (3), HSG256 (36)) and failure to provide suitable and sufficient breaks is a contributory factor. Guidance on rest and meal breaks is given in HSG256, which states that frequent short breaks can reduce fatigue, improve productivity and may reduce the risk of errors and accidents, especially when the work is demanding or monotonous.

Breaks are better taken away from the immediate workplace i.e. in this case, away from the control room and the immediate work station(s). It is recognised that there may need to be some flexibility in doing this, but the flexibility should not override the principle of allowing adequate rest and meal breaks away from the job.

EEMUA201 (41) notes that the overall environment of the control room can also contribute heavily to the effectiveness of control room staff. This includes, for example:

- different users of the control room;
- dividing into primary and secondary users;
- considering the needs of each set of users;
- ensuring there is no conflict between users;
- controlling access;
- environment;
- blast resistance;
- lighting;
- heating and ventilation;
- noise levels;
- furnishings and colour schemes;
- console design;
- safety requirements;
- fire prevention, control and emergency exits;
- other operational support requirements;
- meeting room/office facilities;
- PCs (if not incorporated into the console).

Summary

Duty holders should ensure they can demonstrate that staffing arrangements are adequate to detect, diagnose and recover any reasonably credible hazardous scenario.

Duty holders should develop a fatigue management plan, to ensure that shift work is adequately managed to control risks arising from fatigue.

Duty holders should review working conditions, in particular for control room staff, and develop a plan.

Information and system interfaces for front-line staff

Control room design and ergonomics, as well as effective alarm systems, are vital to allow front line staff, particularly control room operators, to reliably detect, diagnose, and respond to potential incidents. They should comply with recognised good practice appropriate to the scale of the operation.

Guidance on human-computer interfaces

In the past, most control rooms consisted of hard-wired equipment laid out on large metal panels and desks, which required the operator to patrol the panels, monitoring key plant variables, adjusting set-points and operating equipment. These have now commonly been replaced by computer screen based ('soft-desk') systems, through which the operator both views the plant and operates it. In the majority of such cases there is no hard-wired facility at all. This is known as a human-computer interface (HCI) (or human-system interface (HSI)).

EEMUA201 (41) discusses the changing nature of control centres, and how these changes have affected the role of the control room operator. It is the primary and authoritative industry guide to HCIs, and is intended to help those involved in the design, procurement, operation, management and maintenance of these systems. It includes material derived from cooperation with the US-based Abnormal Situation Management Consortium (ASM). ASM publications should be consulted where further information is required.

HCIs provide the vital means by which the operator obtains information on the state of the plant, enters operational data, and by which any automatic control action can be overridden and manual control of the plant be taken.

As plants have become more automated, the automatic system, rather than the operator, performs the majority of the control actions. The operator tends to have a more reactive role, devoting more time to analysing potential problems or dealing with shortfalls in performance. Major intervention by the operator is only required when the plant moves away from its normal operating parameters.

Therefore a modern HCI is required to perform satisfactorily for two very different situations. For most of the time the plant will be operating normally and the HCI must be designed to aid the operator maximise plant efficiency, but when an abnormal situation arises the HCI must aid the operator in returning the plant to normal operation as soon as possible.

Design of the system is crucial to the operator's role, including the number of screens, the design of displays, and the means of navigation around the system. The HCI to a process control system is critical in allowing an operator:

- to develop, maintain and use an accurate and up to-date awareness of the current and likely future state of the process; and
- to interact with the system quickly and efficiently under all plant conditions.

To achieve this, the following categories of operation, in order of importance, need to be considered:

- Category 1: Abnormal situation handling, including start-up and shutdown.
- Category 2: Normal operation.
- Category 3: Optimisation.
- Category 4: General information retrieval.

Many issues need to be taken into account, ranging from the detailed design of display formats, and the way these formats fit together in the hierarchy, through to the actual desk layout, number of screens, and the overall operational environment. This interface is the nerve centre of the operator's work, and its design is very much a human factors issue.

In order to design the HCI it is imperative that the operator's activities are well understood, and all the different operational circumstances considered. EEMUA201 (41) details a number of steps that should be taken including:

- task analysis, to capture the full remit of the operator's role;
- end-user involvement in the system design;
- ensuring that the number of screens allows for complete access to all the necessary; information and controls under all operational circumstances;
- ensuring that the design allows for a permanently viewable plant overview;
- providing continuous access to alarm indications; and,
- providing the capability to expand the number of screens.

The guide provides further advice on issues that have to be considered in taking these steps, including:

- the physical layout and number of screens;
- use of multi-windows;
- use of large screen displays;
- navigational requirements – based on a hierarchy of screens;
- information access;
- management of abnormal situations;
- automation;
- plant size;
- process complexity;
- staffing levels, and multi-unit operation; and,
- reliability/redundancy/system failure.

BS EN ISO 11064 (42) sets a standard for ergonomic design of control centres. It is divided into seven parts, as follows:

- Part 1: Principles for the design of control centres.
- Part 2: Principles for the arrangement of control suites.
- Part 3: Control room layout.
- Part 4: Layout and dimensions of workstations.
- Part 5: Displays and controls.
- Part 6: Environmental requirements for control centres.
- Part 7: Principles for the evaluation of control centres.

In the absence of a more up-to-date company standard, procedure or specification, projects should follow this standard and EEMUA201 (41) for new control rooms, and they can be usefully referred to for modifications and upgrades to existing ones, especially where there are known problems.

Part 1 sets up a generic framework relating to ergonomic and human factors in designing and evaluating control centres, with the view to eliminating or minimising the potential for human errors. It includes requirements and recommendations for a control centre design project in terms of philosophy and process, physical design and design evaluation. It can be applied to the elements of a control room project, such as workstations and overview displays, as well as to the overall planning and design of entire projects.

Other parts of BS EN ISO 11064 (42) deal with more detailed requirements in support of this framework, and may be considered as advanced references.

Guidance on alarm systems

Management of abnormal situations often concerns the effectiveness of the alarm system. Increased automation provides a relatively calm operating scenario when the plant is in a steady state. However, given the importance of alarms in times of upset, the display of alarm information has to be given high priority. Even if there are relatively few alarms on the system and the system is not a distributed control system (DCS) the same principles apply, to ensure a reliable response to alarms.

Duty holders should proactively monitor control systems, such as the tank gauge system, so that designated level alarms etc. do not routinely sound. (This does not exclude the use of properly managed variable alarms or warnings set below the established alarm levels).

The Energy Institute's Alarm handling (43), and HSE's Alarm handling and Better alarm handling (44) provide useful summaries of alarm handling issues with case studies.

EEMUA191 (31) covers the topic fully, and is referenced as good practice guidance in each of the above summaries. It identifies the following characteristics of a good alarm:

- Relevant: not spurious or of low operational value.
- Unique; not duplicating another alarm.
- Timely; not long before response needed, or too late.
- Prioritised; indicating importance to the operator.
- Understandable; message clear and easy to understand.
- Diagnostic; identifying the problem that has occurred.
- Advisory; indicative of action to be taken.
- Focusing; drawing attention to the most important issues.

EEMUA191 (31) provides a roadmap to direct different users to different parts of the guide, relevant to their particular needs. There are separate roadmaps for:

- where an alarm system is already in operation; and
- where an alarm system is in the conceptual phase.

For situations where an alarm system is already in operation, users are provided with guidance on how to review:

- the alarm system philosophy;
- the principles of alarm system design, especially:
  - the design process;
  - generation of alarms;
  - structuring of alarms;
  - designing for operability;
- implementation issues, especially:
  - training;
  - procedures;
  - testing;
- alarm system improvement.

Summary

Duty holders should ensure that their control room information displays, including human-computer interfaces and alarm systems, are reviewed in relation to recognised good industry practice.

Where reasonably practicable, duty holders should put plans in place to upgrade control room information displays, including human–computer interfaces and alarm systems, to recognised good industry practice.

Duty holders should ensure that modifications or development of new control rooms or HCIs comply with recognised industry good practice both in their design, and their development and testing.

SECTION 3 – MANAGING INTEGRITY OF EQUIPMENT

Part 3 of the PSLG report "Engineering against Escalation of Loss of Primary Containment" (46) included a discussion of the inspections systems that should be in place to ensure the integrity against loss of Primary Containment. This section summarises the principles from Part 3 into general guidance on the management of the integrity of equipment.

Guidance on periodic examination and testing

The most recent guidance on periodic examination and testing of plant and equipment forming the primary containment of hazardous substances is the document 'The mechanical integrity of plant containing hazardous substances', produced by EEMUA and SAFed in 2012 (EEMUA231, SAFed IMG1) (46). This publication does not introduce new standards, but comprehensively pulls together the existing best practice guidance on all aspects of integrity management of plant in hazardous substance duty.

Equipment integrity should be managed in accordance with the relevant good practice appropriate to the type of equipment (e.g. API510 for pressure vessels (47), EEMUA159 (48) and API653 (49) for storage tanks, API570 (50) for pipework). The relevant good practice held within these documents should form the basis of minimum industry standards for equipment integrity management and repair to prevent loss of primary containment. (General guidance for Pressure systems is given the Pressure Systems Safety Regulations and its associated ACOP (51)).

HSE guidance Integrity of atmospheric storage tanks (SPC/Tech/Gen/35) (52) highlights the factors to consider when operating storage tanks containing hazardous substances and includes reference to EEMUA159 (48) and API653 (49) and RR760 (53).

Competency

When assessing equipment integrity and conducting inspections competent personnel who are aware of and able to apply relevant equipment design codes where necessary should be used. Competent personnel may be directly employed or accessed on a contractual basis by the user. Assessors should be qualified in the relevant API/ASME codes appropriate to the equipment being inspected, and have completed appropriate training courses. The inspection organisation should be accredited e.g. by UKAS to ISO17020. This defines the standards required for competence of the inspection organisation and the procedures that should be in place.

Regular online operational checks can be undertaken by suitably trained personnel with the competencies required to carry out such checks properly.

Internal/out-of-service inspections

The relevant good practice described above, acknowledges the typical equipment failure modes e.g. corrosion, erosion, settlement, fatigue etc. for the equipment concerned and provides good guidance for early detection and measurement of symptoms that could lead to failure. The scope of any examination should take the potential failure modes into account.

Arrangements for vessel inspection should include any non-metallic vessels, such as plastic or glass-reinforced plastic (GRP), as well as metallic vessels and pipework. Although corrosion is not an issue with these vessels, there are other potential failure mechanisms and design-life issues that need to be properly managed. HSE Guidance PM75 (54) and PM86 (55) specifically apply to the inspection and maintenance of non-metallic vessels.

A written scheme of examination should be prepared by a competent person and is required for internal/out-of-service inspections on all equipment subject to inspection. The relevant good practice guides typically will give example checklists for inspection (e.g. EEMUA 159 (48), Appendix B2 provides an example of such a checklist.)

The relevant good practice documents provide guidance on inspection intervals by either fixed periodicity or by use of a risk-based methodology. The tables of fixed inspection intervals within such guidance can be used where there is little or uncertain history of equipment integrity available. A risk-based inspection (RBI) approach allows the use of actual corrosion rates and performance data to influence the most appropriate inspection interval. An example of such a risk assessment is also shown in CIRIA 598.30 (56).

Many companies have their own technical guidance on equipment inspection, maintenance, and engineering best practices, in addition to established RBI programmes. In such cases they are best placed to determine inspection frequencies informed by inspection history. HSE research report RR729 (Establishing the requirements for internal examination of high hazard process plant) (57) establishes relevant good practice covering RBI assessment of hazardous equipment.

The frequency, scope and techniques of internal/out-of-service inspections should be routinely reviewed and in the light of new information. Inspections may become more frequent if active degradation mechanisms are found. It is best practice to review the inspection frequency after each inspection to ensure any findings from the inspection are immediately addressed.

Particular attention should be given to insulated or lined equipment, as corrosion under insulation and external coating prior to insulation can have significant effects on equipment integrity. For corrosive products protective coatings may be applied internally. This may lengthen the inspection interval. To ensure quality control, particular attention should be paid during the application of coatings.

Thorough internal inspections can only be carried out by removing the equipment from service and cleaning. The potential deterioration mechanisms for a piece of equipment need to be considered in advance of an internal inspection, and appropriate techniques defined in the written scheme of examination to ensure any such potential defects are detected. Consideration of the scope of any such tests needs to be considered to ensure locations of the potential failures are thoroughly examined. For example, as a minimum for metallic tanks, a full-floor scan along with internal examination of the shell to annular/floor weld, annular plate and shell nozzles using non-destructive testing and visual inspection in line with good practice would be appropriate. For erosion it may be appropriate only to inspect the locations, such as bends in pipework, where erosion is more likely. Different techniques may be appropriate for non-metallic equipment.

External/in-service inspections

A written scheme of examination is also required for any external inspections. These examinations supplement thorough internal inspections and form part of the overall assessment of equipment history and fitness for purpose for future service. In some situations, e.g. pipework systems, external examination may be the only option. Relevant guidance such as EEMUA 159 (48) provides an example of considerations to be included in the Written Scheme of Examination. This must be prepared by a competent person.

Thorough internal inspections must be supplemented by external/in-service inspections. These inspections must be completed periodically, as this forms a part of obtaining the overall equipment history and assessing fitness for future service. In-service inspection frequency may be determined through RBI assessment or may be based on fixed intervals (see relevant guidance) based on the type of product and the type of equipment. Frequency of in-service inspections should be subject to review and may become more frequent if active degradation mechanisms are found or towards the end of predicted equipment life.

It is best practice to review the Written Scheme of Examination and the RBI assessment following an inspection

Routine operator checks, outside formal inspections, also support the maintenance of equipment integrity. Operators should check for any signs of potential problems e.g. visible signs of external corrosion, breaking down of coatings etc. or can undertake more formal checks. For example, guidance for routine operational checks of storage tanks is provided in EEMUA159 (48) and API653

(49) which suggests that such evaluation should include fixed roof venting, floating roof drainage and general operation.

All inspections and routine checks should be documented and appropriate action taken on any issues identified.

Deferring internal examinations

Deferral of the required inspection date must be risk assessed by a competent person. Where necessary, deferral decisions should be supported by targeted non-destructive testing. Deferral decisions must also consider previous inspection history and other relevant information including changes in operating conditions, etc. For pressure systems the Pressure Systems Safety Regulations (51) require that deferrals must be notified to HSE.

Particular attention should be given to equipment that has had no previous internal examination as the probability of failure will increase with every year that the recommended interval is exceeded. In such cases it is unlikely that risk assessment could justify a deferral as there is little data to base such a deferral on. It is the duty holder's responsibility to ensure that the risk of loss of containment is properly managed.

Remedial work

Equipment repair is a specialised activity, and should be performed only by those competent in equipment design, reconstruction and repair works, specific to the equipment concerned. Non-destructive testing should be carried out by personnel qualified to standards such as TWI's Certification Scheme for Welding and Inspection Personnel or Personnel Certificate of Non-Destructive Testing, or equivalent.

Having completed an inspection, repair and any additional testing, a new risk- or time-based inspection frequency should be determined, taking into account all relevant factors including the condition of the equipment, future service requirements, potential degradation mechanisms and failure consequences.

Ensuring risks are ALARP is a continuous improvement process. Good practice therefore requires a periodic assessment of existing equipment against current standards. As a minimum, existing equipment should comply with a relevant recognised design code at their date of manufacture. Where this is not the case, equipment should be assessed against an appropriate current design standard and remedial action should then be taken, as necessary, informed by the resulting gap analysis, to reduce risks ALARP.

Where major modifications or repairs are undertaken on existing equipment these should comply with a suitable recognised and current standard.

Section 4 – Preventing Loss of Containment

Parts 2 and 3 of the PSLG report (1) related to protecting against loss of primary containment using high integrity systems, and engineering against escalation of loss of primary containment. This section incorporates the basic principles from those two sections into the key principles for assessment of required protective systems and their ongoing maintenance for purpose. It also provides guidance on the use of ROSOVs to protect against escalation due to loss of containment.

Guidance on secondary and tertiary containment has been reviewed and updated following the work of PSLG. Current guidance (incorporating the work of PSLG and others) can be found in the CIRIA publication "Containment systems for the prevention of pollution (C736) (58). C736 is applicable to the containment of a wide range of flammable/combustible and environmentally hazardous inventories. It provides guidance for all sizes of site, from small commercial premises, which may contain a single tank, through to large chemical or petrochemical sites. Experience has shown that many incidents occur in warehouses and other storage facilities, and these are also covered.

Maintaining the integrity of plant, equipment and vessels used in the service of hazardous substances at COMAH sites will depend on an integrated approach to design, provision of protection systems, and inspections and maintenance. This approach to asset integrity is necessary both to meet legal requirements to prevent loss of containment and to ensure the consequential business risks are effectively managed. Operators may also need to address the issue of the levels of protection provided for existing plant and equipment and the extent to which they remain appropriate in the light of incident experience and 'near misses' both at the site and elsewhere.

There are various approaches to risk assessing processes and hazardous substance storage to determine an appropriate level of protection. Safety Integrity Level (SIL) assessment of instrumented systems is one method, however, alternatives based on recognised International standards, e.g. Layers of Protection Analysis (LOPA), are acceptable.

Safety Integrity Level – SIL

Before protective systems are installed there is a need to determine the appropriate level of integrity that such systems are expected to achieve, and where appropriate that they have sufficient independence to ensure safe operation.

Operators of COMAH sites should assess the need for instrumented protective systems to protect against major accident hazards such as overfill, over pressure and other potential failure modes for equipment. This assessment should take account of:

(a) the existence of nearby sensitive resources or populations;
(b) the nature and intensity of site operations;
(c) realistic reliability expectations for instrumented protective systems and
(d) the extent/rigour of operator monitoring.

Where such systems are necessary from the systematic assessment, duty holders should ensure the systems meet recognised international standards, for example BS EN 61511:2004 (59). This should lead, through risk assessment, to an appropriate Safety Integrity Level for all such identified protective systems.

For each risk assessment/SIL determination study, duty holders should be able to justify each claim, and data used in the risk assessment, and ensure that appropriate management systems and procedures are implemented to support those claims. For COMAH Upper Tier sites this will form part of the demonstration required within the safety report. For COMAH Lower Tier sites, this should be part of their safety management system represented in their Major Accident Prevention Policy (MAPP)

Of particular importance is the reliability and diversity of the independent layers of protection. To avoid common mode failures extreme care should be taken when claiming high reliability and diversity, particularly for multiple human interventions.

Layers of Protection Analysis (LOPA) is one recognised method of determining the robustness of measures to prevent major accidents, and whether high integrity systems to manage potential loss of containment are necessary. LOPA is a suitable methodology to determine SILs within the framework of BS EN 61511-1:2004 (59). Note that other methods are available, and are described in this standard.

Instrumented protective systems

Overfill and other safety instrumented protection systems, including instrumentation, devices, alarm annunciators, valves and components comprising the shutdown system, should be assessed. This includes the following considerations:

- design, installation, operation, maintenance and testing of equipment;
- management systems;
- redundancy level, diversity, independence and separation;
- fail safe, proof test coverage/frequency; and
- consideration of common causes of failures.

Note - although referred to as safety instrumented systems, in this guidance the term is intended to include protection against environmental as well as safety risks.

Systems providing a risk reduction of less than 10 are not in scope of BS EN 61511 (59). They may, however, still provide a safety function and hence are safety systems and can be a layer of protection. Such systems should comply with good practice in design and maintenance so far as is reasonably practicable.

The duty holders should review the risk assessment for their installations periodically and take into account new knowledge concerning hazards and developments in standards. Any improvements required by standards such as BS EN 61511:2004 (59) should be implemented so far as is reasonably practicable

Management of Instrumented Protective Systems

This guidance does not replace or detract from the requirements of standards including BS EN 61511:2004 (59), but is a summary of some of the main requirements that are relevant.

The suitability and continuing integrity of instrumented systems is essential to ensure the safety of an installation and in particular the primary containment system. The functional integrity of safety instrumented protection systems (SIS) is critical to primary containment. Protective systems may be in a dormant state without being required to operate for many years. For this reason, periodic testing is an essential element in assuring their continuing integrity.

BS EN 61511:2004 (59) requires that for all SIS implementing safety instrumented functions of SIL 1 or higher there is a management system in place for the whole of the lifecycle of the SIS, which will manage all appropriate measures.

Management of Safety Instrumented Systems (SIS)

A SIS management system should include the following elements specific to safety instrumented systems. The management system may be part of an overall site-wide safety management system but the following elements should be in place for each phase in the SIS lifecycle:

Safety planning, organisation and procedures

Safety planning should identify all the required tasks that need to be performed at various stages and allocate roles and responsibilities of people (departments, individuals, staff or contractors) to perform those tasks.

The organisation and planning should be documented and reviewed as necessary when changes occur throughout the operational life of the system.

Responsibilities and competence

The roles and responsibilities associated with the SIS (such as design, operation, maintenance, testing etc.) should be documented and communicated. This should include a description of the tasks and who is responsible for performing the tasks.

People with responsibilities should be competent to perform their tasks consistently to the required standard. The required knowledge, understanding and skills for the competences can be wide ranging and depend on the role and the type of task, and these may be for design, engineering, system technology, hazard and safety engineering, regulations, management, leadership, maintenance and testing.

Performance Evaluation

Arrangements should be in place to evaluate the performance and validation of a safety instrumented system. This should include validation that the system design meets the requirements of BS EN 61511:2004 (59) and the system operation fulfils the design intent.

Failures of the system or of any component should be investigated and recorded along with any modifications and maintenance performed. The details of any demands on the system, and system performance on demand, should be recorded including data on any spurious trips, any revealed failures of the system or its components and, in particular, any failures identified during proof testing.

Records of all these events should be kept for future analysis. Records may be paper or electronic.

Operation, maintenance and testing

Arrangements should be in place for the operation, maintenance and system testing and inspection for the whole system and subcomponents. Written procedures should be agreed by those the duty holder has identified as responsible and competent for these functions. Procedures and competency arrangements should be based on adequate consideration of human failure potential in carrying out inspection, maintenance and testing activities.

The initial test interval should be determined by the calculation of probability of failure on demand during the design process, and this should be assessed and amended periodically based on real operational data.

Functional safety assessment

Functional safety is the part of the overall safety arrangements that depends on a system or equipment operating correctly in response to its inputs (BS EN 61508 (60)). Procedures for functional safety assessment and auditing should be in place. A functional safety assessment is an independent assessment and audit of the functional safety requirements and the safety integrity level achieved by the SIS.

At least one functional safety assessment should be performed on each system, typically at the design stage before the system is commissioned. The functional safety assessment process should be performed by an assessment team which includes at least one competent person independent of the project design team. A functional safety assessment should be performed and revalidated after any modifications, mal-operation or failure to deliver the required safety function (a spurious trip which caused the safety system to action its functions successfully would not be considered a failure). The depth and scope of the functional safety assessment should be based on the specific circumstances, including the size of the project, complexity, SIL and the consequences of failure. Further guidance is given in BS EN 61511:2004 Section 5 (59).

Modifications

Where changes or modifications to an SIS are planned then the changes should be subject to a management of change process. The procedure should identify and address any potential safety implications of the modification. Software changes and system configuration changes should also be subject to a management of change process.

Documentation

The associated documentation should be maintained, accurate and up-to-date with all necessary information available to allow operation and lifecycle management.

The documentation should include but not be limited to process and instrumentation diagrams, system design and testing requirements, and a description of maintenance activities for the various components of the SIS from sensors to final elements inclusive. Documentation of the design should include risk assessment for SIL determination, design specification, factory acceptance testing, installation specification, and commissioning tests.

Operator Response Times to SIS

Where operators are involved in Safety Instrumented Protective Systems their ability to respond in a timely manner is critical to the overall effectiveness of the systems.

High Integrity systems – SIL 2 and above – should be designed to give the required integrity independent of any operator response.

Where operator response is important care is needed when estimating the likely time for operators to respond to an incident. Consideration should be given to the detection, diagnosis, and action stages of response.

Detection covers how an operator will become aware that a problem exists. Assessment of alarm priorities and frequencies, the characteristics of the operator and console displays, as well as operators' past experience of similar problems on sites, are all useful aspects to review operational problems that appear over a period of time, and where the information available to the operators can be uncertain, are particularly difficult to detect. When control rooms are not continually staffed, the reliable detection of plant problems needs careful consideration.

Diagnosis refers to how an operator will determine what action, if any, is required to respond to the problem. Relevant factors to think about include training and competence assurance, the availability of clear operating procedures and other job aids, and level of supervision. The existence of more than one problem can make diagnosis more difficult.

Action covers how a timely response is carried out. Key aspects include: the availability of a reliable means of communicating with other plant operators; the time needed to locate and operate a control (close a valve, stop a pump); the need to put on personal protective equipment (PPE); the ease of operating the control while wearing PPE; and how feedback is given to operators that the control has operated correctly. Occasionally there may be circumstances where operators may hesitate if shutting down an operation might lead to later criticism.

A 'walk-through' of the physical aspects of the task with operators can provide useful information on the minimum time needed to detect and respond to an incipient incident. However, allowance needs to be made for additional delays due to uncertainty, hesitation or communications problems. This will need to be added to the minimum time to produce a realistic estimate of the time to respond.

Operator responsibilities and human factors

Monitoring and control of levels, and protection systems, may depend on operators taking the correct actions at a number of stages in the operating procedure. Using overfill of a storage tank as an example these actions may include, but not be limited to:

- calculation of spare capacity;
- correct valve line up;
- cross-checks of valve line up;
- manual dipping of tanks to check automatic tank gauging (ATG) calibration;
- confirmation that the correct tank is receiving the transfer;
- monitoring level increase in the correct tank during filling;
- checks for no increase in level in static tanks;
- closing a valve at the end of a transfer;
- response to level alarm high (LAH); and
- response to level alarm high-high (LAHH).

Some of these actions are checks and therefore improve safety; some however are actions critical to safety. The probability of human error increases in proportion to the number of contiguous, critical actions required, so the human factors associated with operator responsibilities need careful consideration. A useful guide is Reducing error and influencing behaviour HSG48 (3) Further information and guidance on human factors in process safety operations is given in this document.

Improved level instrumentation components and systems

When selecting components and systems for safety instrumented protection systems designers should ensure adequate testability and maintainability to support the required reliability and take account of the safety benefits available in modern components and systems, such as diagnostics. Designers should also take account of the potential advantages of the use of non-invasive systems compared with systems using components inside vessels. Data retrieval and display systems with software features which assist operator monitoring during critical operations should be considered for more complex systems.

Designers and duty holders should review how they currently control and log override actions, where SIS are taken out of service for a limited period of time. In general, they should consider:

- the need for any overrides – when they may be needed, who should have access to them and their duration;
- the possible impairment of effective delivery of a safety instrumented function created by an override against any safety risks that an inability to override could result in. Such reviews should consider both normal operation and the response to abnormal/emergency situations;
- if current logs would allow the effective identification and review of when overrides are in operation or have been operated.

Duty holders should identify those records needed for the periodic review of the effectiveness of control measures, and for the root cause analysis of those incidents and near misses that could potentially have developed into a major incident. The records should be retained for a minimum period of one year.

Monitoring Process Safety Performance

Duty holders should measure their performance to assess how effectively risks are being controlled. Active monitoring provides feedback on performance and a basis for learning to improve before an accident or incident, whereas reactive monitoring involves identifying and reporting on incidents to check the controls in place, identify weaknesses and learn from failures.

Isolation of Equipment in an Emergency

Fire-safe shut-off valves

Each pipe connected to a piece of equipment is a potential source of a major leak. In the event of an emergency it is important to be able to safely isolate the contents of the equipment. Isolation valves should be fire-safe, i.e. capable of maintaining a leak-proof seal under anticipated fire exposure.

Fire-safe shut-off valves should be fitted close to the equipment on both inlet and outlet pipes. Valves should either conform to an appropriate standard (BS 6755-214 (61) or BS EN ISO 1049715 (62)), equivalent international standards or be of an intrinsically fire-safe design, i.e. have metal-to-metal seats (secondary metal seats on soft-seated valves are acceptable), not be constructed of cast iron and not be wafer bolted.

Remotely operated shut-off valves (ROSOVs)

Operators of COMAH sites should asses the need for ROSOVs in accordance with the methodology detailed in HSG244 (63).
In an emergency, rapid isolation of vessels or process plant is one of the most effective means of preventing loss of containment, or limiting its size. A ROSOV is a valve designed, installed and maintained for the primary purpose of achieving rapid isolation of plant items containing hazardous substances in the event of a failure of the primary containment system (including, but not limited to, leaks from pipework, flanges and pump seals). Valve closure can be initiated from a point remote from

the valve itself. The valve should be capable of closing and maintaining tight shut off under credible conditions following such a failure (which may include fire).

Remotely operated shut-off valves (ROSOVs) for emergency isolation of hazardous substances: Guidance on good practice HSG244 (63) provides guidance on how to assess the need to provide ROSOVs for emergency isolation. It has been written for a wide range of circumstances and as a result the section dealing with ROSOV failure modes requires additional interpretation.

A review of the ROSOV assessments showed that assessments did not always fully address the risks in the structured manner required by HSG244 (63), but rather simply asserted that the provision of ROSOVs was not reasonably practicable. Others did not fully apply the primary and secondary selection criteria. Of those that did properly follow the steps in HSG244 it was concluded that:

- where the case-specific risk assessment indicated a ROSOV was required where currently only manual valves existed, then there was a worthwhile improvement to be gained by fitting a ROSOV;
- where the case-specific risk assessment indicated a ROSOV should be provided where currently a ROV (which would not fail safe) existed, it was not reasonably practicable to upgrade to a fail-safe device. But additional risk reduction could be achieved by ensuring that the cables are fire protected, and a rigorous regime is in place for inspection and testing the operation of the valves and control systems.

Operators of COMAH sites should take into account the learning from this review in assessing the need for ROSOVs.

Section 5 - Emergency planning and response

This section takes Appendix 6 “Emergency Planning Guidance” in the PSLG report (1) and applies it as guidance for all COMAH establishments.
The reference “Competent Authority guidance for inspectors on emergency arrangements for COMAH establishments” (68) was produced jointly by the CA, industry, emergency planners and other organisations following recommendations made in the Buncefield MIIB emergency preparedness for, response to and recovery from incidents (EPRR) report. In response to these recommendations, this improved guidance was developed on producing on and offsite emergency plans and the integration of COMAH with other emergency planning requirements established under the Civil Contingencies Act.

Emergency Planning

A summary of emergency planning guidance is given in the route map in Appendix 6 in the PLSG report (1).

Emergency response arrangements

This section covers good practice relating to internal emergency response arrangements and the interface between internal and off-site emergency response arrangements. An overview of emergency planning requirements can be found in Appendix 6.

Principles

All sites in scope of the COMAH regulations – including both lower tier and upper tier COMAH sites - should prepare in writing a suitable internal emergency plan as required by the COMAH Regulations. For lower-tier COMAH sites the plan should be prepared as part of the MAPP.

The emergency plans should consider the response to and mitigation of the worst case credible scenarios for a site. This should consider escalation of an initial event into a more widespread incident. The plan should cover the on-site consequences of such an event and the assistance available in the form of off-site mitigating actions (reference should be made to HSG191 (64) paragraph 115 for examples of such off-site mitigating actions).

As part of the overall internal emergency plan the operator should develop Incident specific emergency response pre-plans. These should be developed for the worst case credible scenarios to specifically cover emergency team tactics and equipment etc. needed to deal with a specific incident. In the event of a fire this may include allowing a controlled burn, and the management of firewater.

The incident-specific emergency response pre-plans should consider emergency management requirements in response to, and mitigation of, a multiple event e.g. fire fighting requirements for a multiple tank fire, or an explosion leading to the release of toxic material. The pre-plan should cover the on-site consequences of such an event and the assistance available in the form of off-site mitigating actions. Any pre-plan deemed necessary to deal with such an event must be capable of operating effectively even in the event of a preceding incident which might compromise the ability to utilise the emergency response equipment available e.g. the release of a toxic material which might prevent operator response without Breathing Apparatus to make isolations.

The overall internal emergency response plan should be tested on a schedule. Site-specific guidance should be produced as to what is required to exercise fully the emergency response arrangements.

During preparation of the internal emergency plan, the operator should consult with the local authority emergency planning unit, the relevant environment agency (EA, NRW or SEPA) and the local emergency services, particularly the local Fire and Rescue Service, on the content of the internal emergency plan to ensure the off-site response available is adequate to deal with the incident.

The operator should provide all information (relating to the site) required by the COMAH Regulations (12) to the local emergency planning unit to allow the external plan arrangements to dovetail with the internal emergency plan.
The operator should keep the internal emergency plan up to date and should ensure that any significant changes are communicated to the local authority and other concerned agencies.

The operator should ensure the internal emergency plan is functionally tested at least every three years. Site-specific guidance should be produced as to what is required to exercise the plan. The testing of the internal emergency plan should involve the testing of any incident specific emergency pre-plans.

Trained, knowledgeable and competent personnel must be involved in the exercise and testing of the onsite emergency plan (including the testing of the incident specific emergency pre-plan (the incident specific emergency response plan being a sub-set and one specific aspect of the overall internal emergency response plan). Personnel must be able to perform the tasks they will be expected to fulfil during an incident.

Whenever the onsite emergency plan is reviewed/tested or if there has been a material change in an aspect of an emergency arrangement, the operator should inform all contributors to the plan of any changes to arrangements and verify that the arrangements are still adequate. All contributors to the plan should be encouraged to inform the site operator proactively of any material changes affecting their contribution.

Internal emergency plan

A template for an internal emergency plan can be found in Appendix 6. It is envisaged that sites will complete this template and that it will then act as a high-level document providing an overview of the site's arrangements. Underpinning this document will be a series of detailed plans relating to specific incidents.

Emergency planning and preparation

This topic comprises of two elements; firstly, the actions that should be put in place before an event occurs and secondly, actions that should be carried out once an event has occurred. These arrangements should be agreed by all parties involved, including off-site responders.

Planning is essential to defining incident specific emergency response pre-plans by determining what resources are needed to manage a specific incident e.g. to extinguish a fire, disperse a toxic release or manage a controlled burn; and how to deliver the required resources and manage firewater to prevent environmental impact.

Scenario-based incident-specific emergency response pre-plans can identify incident control resources required for accidental release, spillages and fire and emergency response. They can also provide guidance on control and deployment of the necessary resources and importantly, can be used as a tool to exercise against, thus closing the loop from preparation to planned and exercised response.

For firefighting emergency response pre-plans then EI 19 Fire precautions at petroleum refineries and bulk storage installations (65) is considered to be 'relevant good practice' under COMAH, and operators should consider how this applies. The steps laid down here also provide some guidance on principles on assessment of water requirements for dealing with toxic releases and to allow assessment of fire water runoff.

For fires it may be appropriate to allow a controlled burn rather than to extinguish it. A scenario specific emergency pre-plan should consider the need for a controlled burn. However, this decision may be affected by conditions on the day. Guidance on the use of controlled burn is available in the Environment Agency's PPG 28 (66) and the Fire and Rescue Service's Manual on environmental protection (67).

Emergency Response Incident Management

The following actions need to be carried out and arrangements for these should be described in the onsite emergency plan:

- Operators should contact the local authority Fire and Rescue Service in accordance with the pre-incident management agreement between the operator and the Fire and Rescue Service.
- The local authority Fire and Rescue Service should rendezvous at a predetermined holding point for the company concerned.
- Fire and Rescue Service Incident Commander should formally liaise with the company on-scene commander (and site fire officer if applicable), obtaining information regarding the incident, whether or not people are involved, the resources in place and the hazards and risks associated with the particular event. These persons will form the incident control team (ICT) along with any others required by the circumstances.
- Establish immediate priorities and the potential for escalation. Local scenario-specific emergency response pre-plans (ERPs) for the plant or area should at this time be made available to, and be used by, the ICT.
- Lines of supervisory authority and the means of communication should be clearly established within the ERPs to assist in effective reporting and incident control.
- The ICT must ensure the safety of all personnel. This team should have:
  - completed a dynamic risk assessment (DRA) and if there has been time, a written record needs to be handed to the Fire and Rescue Service IC on their arrival;
  - arranged for the DRA to be recorded and constantly reviewed. The DRA also needs to be communicated and the tactical mode declared, implemented and recorded;
  - ensured that safety officers are appointed with their responsibilities clearly established.
- The ICT should also:
  - establish the incident command position;
  - determine the operational objectives and the incident plan, including tactical and strategic considerations;
  - identify from the ERPs, the equipment, material and resources required, coordinating effort into sourcing equipment and materials to the incident;
  - obtain additional support/equipment/resources if required (via mutual aid partnerships if in existence);
  - implement the mutually agreed strategy by bringing resources on-site from the rendezvous point at this stage;
  - monitor and review the implemented plan for ongoing potential hazards and the continued effectiveness of the plan at predetermined intervals. If the plan cannot be followed or if a deviation is required from it at any time then a DRA must be carried out, communicated to all concerned and recorded;
  - establish welfare arrangements for all at incident scene; and
  - ensure that media issues are addressed.

Guidance for planning emergency arrangements

The event that operators should plan for, with respect to emergency arrangements, is that of the worst case credible scenario allowing for reasonable escalation of an initial incident (e.g. a multiple tank fire following an explosion as happened at Buncefield, or the release of a toxic material following an explosion). Emergency arrangements will need to be capable of operating effectively following such an event (e.g. should survive reasonable overpressures following an explosion (1), or not be affected by a release of toxic or corrosive chemicals).

The methodology below is for duty holders to evaluate the potential impact of an incident on the emergency arrangements at their site. These arrangements will include fixed equipment such as fire

pumps and hydrants as well as foam stocks, site ingress and egress points for off-site emergency resources, control rooms and critical equipment.

Duty holders should carry out individual site assessments based on the following methodology:

- identify the critical equipment and resources necessary to respond to credible incident scenarios following a significant incident;
- for those resources identified, plot the location on a site plan of those that are installed at the facility or provided as part of a mutual aid or common user scheme;
- apply the consequence circles from an incident;
- assess the effects of the consequences of the incident (thermal radiation, overpressure, release of toxic or corrosive materials) on all items of critical equipment and resources within the designated area;
- decide whether the equipment or resource would remain usable or not (note: apply the precautionary principle and if in doubt treat as unusable);
- assess the effects of the consequences of an incident on Occupied Buildings which may be critical to management of an emergency e.g. plant control rooms, the Emergency Control Centre.
- for each item of critical equipment or resource that is likely to be damaged in the event of an incident, the facility should consider:
    - moving the equipment outside the area likely to be affected;
    - duplicating the equipment by providing an alternative outside the area;
    - providing protection in the form of blast shielding (note: if site power and control systems are lost there may be little advantage in protecting pumps or other equipment that cannot be used);
    - reducing the consequence of the damage. For example, if a fire pump is lost in a blast, but an underground hydrant system is still usable, then additional inlet points for mobile pumps from open water could restore operation of the system;
    - using off-site emergency equipment and resources, e.g. by providing mobile equipment from the Fire and Rescue Service or mutual aid scheme;
    - for access and egress points used by the emergency services, provide alternate routes in case the main roads and gates are affected by the incident.

The results of the assessment should be documented and incorporated into the internal and external emergency plans. These results should be used to plan the emergency arrangements for the site. Any dependency on mutual aid or external resources should be agreed, and these arrangements regularly tested and reviewed. The template for completion of the internal emergency plan for COMAH sites is provided in Appendix 6. The template can be completed and used as the basis for the internal emergency plan. This approach may be of benefit to lower-tier COMAH sites.

The blank template can be used as a checklist against which to verify an existing internal emergency plan.
Each emergency plan should be specific to an individual site. Duty holders should review their internal emergency plan to ensure that there are enough people with the right training and competence to deal with an emergency.

The following factors should be considered:

- Have all the risks been identified for the site with respect to the credible emergency scenarios?
- Have response plans been developed to deal with these risks?
- Do the response plans identify actions and resources needed especially people?
- Do the response plans identify escalation measures including the resources needed to action the plan?
- Are there sufficient resources to action these plans? This can be done by a gap analysis of the staff and other resources. Consider the following:
    - Time: Can staff be released in an emergency? Have they time to do all that they need to under the plan?
    - Tools: Do staff have access to the correct equipment/information?

- Ability: Can they use the equipment/understand the information and do what they need to properly?
- Sustainability (for longer duration scenarios): Are suitably competent relief staff available to maintain the emergency plan over a realistic response period.

This can be summarised as 'does the site at all times have enough staff who are able to do what they need to in the time available to make the plan work?'

Each member of staff should be competent to implement the emergency plan. Competency should be checked during training and testing of emergency plans. Can each person do what they need to – if not train and evaluate? Refresher training is vital to maintain competence and there needs to be realistic testing to ensure that staff demonstrate competence. Duty holders should record all reviews, analysis, training and testing.

Table 1 is derived from the Energy Institute guidance in EI 19 (65). It provides an example of the competencies required by a typical emergency response team member. The areas where competencies are necessary have been identified by analysing the tasks that the person will fulfil as their part in the plan. The same process can be applied to all tasks and the competencies required identified.

It is essential to consider tasks such as drainage, firewater management, pollution control and site recovery when deciding on training and competencies.

Table 1 Emergency response team member – example competency profile

Operations	**Maintenance**	**Procedures**	**Skills**
1.1 Inspect and test fire vehicles	2.1 Inspect and test site portable/mobile fire equipment	3.1 Execute assigned duties	4.1 Respond to emergencies
1.2 Inspect and test fire station communications	2.2 Inspect and test site fixed fire systems	3.2 Working safely	4.2 Fixed systems/fire tender work in incident area
1.3 Exercise emergency response	2.3 Inspect and test site fire hydrants		4.3 Carry out fire fighting or incident control operations
1.4 Fire prevention			4.4 Rescue personnel
			4.5 Reinstate resources
			4.6 Training and instruction

Source: EI 19 Annex E – an example ERT member competency profile based on four units.

Duty holders should evaluate the siting and protection of emergency response facilities, and put in place contingency arrangements either on or off site in the event of failure. This should include identifying and establishing an alternative emergency control with a duplicate set of plans and technical information.

EI 19 provides good practice guidance on protection of safety-critical equipment and resources. Fire protection and other critical emergency equipment and resources should be located in non-hazardous areas so far as is reasonably practicable. Duty holders should consider the consequence of a major incident to determine where to locate such items as they may constitute sources of ignition. Locate equipment and resources to enable access at all times during incidents. They should be capable of functioning despite the effects of fire and explosion, for example, fire pumps should be located at a safe distance away from any possible explosion/fire consequences.

Step 1 Duty holders should consider and list worst-case credible scenarios in terms of:

- hazard distances;
- over-pressures;
- radiant heat levels;
- potential for missile generation; and,

- toxic hazard distances.

The emphasis should be on the effects of 'worst-case credible' incident scenarios, as these identify the most vulnerable emergency equipment and resources. However, duty holders should consider specific issues that may arise from lesser incidents, e.g. different types of foam concentrate, critical emergency equipment located near relatively low-hazard operational areas etc.

Step 2 Identify critical emergency response equipment and resources vulnerable to the worst-case credible scenarios. Start by reviewing the list to identify critical equipment and resources that may be vulnerable in a major incident. Detailed site plans with significant hazard ranges marked on them may be used as an aid.

The templates provide a list of emergency response equipment and resources, drawn from industry guidance and codes. The list should not be seen as exhaustive. Duty holders should also consider unique features of their own sites and emergency response arrangements.

Step 3 In reviewing critical equipment and resources consider all necessary measures to manage the incident, i.e. drainage, firewater management, power supply, control centres, communications etc. Consider the requirements to deal with the more likely scenarios, not just the high impact–low probability events. Assess what the likely level of damage would be to vulnerable equipment and resources, in terms of Table 2:

Table 2

Functionality (Can the system still meet its intended role or function?)	**Availability (Is the system still available when it might be needed?)**	**Reliability (Can the system still work as intended when called upon?)**
- Total loss (e.g. loss of foam supplies) - Partial loss (e.g. water spray system pipework may be damaged so that it cannot give adequate coverage to all vessels exposed to radiant heat and/or flames? - No significant loss (the system can still function as intended)	- Total loss (e.g. fire pumps destroyed by blast) - Partial loss (e.g. emergency access may be obstructed from certain directions) - No significant loss (the system is still available for use)	- Total loss (e.g. severe bund wall damage) - Partial loss (e.g. damage to cabling may mean remote operation of valves is lost/unreliable, but manual operation may still be possible) - No significant loss (the system can still function when called upon)

Step 4. Where there are gaps against current good practice, as an alternative to upgrading the on-site facilities, duty holders may consider other contingency arrangements, for example, relocating mobile equipment and resources. Where further measures are necessary to provide an alternative to fixed equipment, it may be more appropriate to identify what external assistance may be available to provide sufficient contingency (e.g. local emergency services, mutual aid schemes). Emergency plans should be revised to take into account any possible loss of critical equipment and resources.

Additional measures to consider include:

- reducing the risk of the incident at source;
- increased redundancy, e.g. alternative fire pumps in different locations;
- increasing supplies;
- relocating resources;
- splitting supplies into different locations;
- manual back up for automated systems;
- resources that can be brought in by the emergency services;
- mutual aid schemes;
- contracts/agreements with specialist companies who can provide additional resources within a reasonable time period;

- duplicate copies of emergency information (hazard data, site plans, etc.). Information kept in different locations (on and off site) and different formats (hard copy and electronic);
- alternative emergency control centre off site;
- alternative emergency response tactics (e.g. consideration of controlled burn if firewater supplies are lost);
- revision of emergency plans, tactics and strategies; and,
- exercises to test the adequacy of contingency arrangements.

Should the duty holder rely on off-site fire and rescue services, the internal plan should clearly demonstrate that there are adequate arrangements in place between the parties.

The following guidance is aimed at sites whose current arrangements rely on the Fire and Rescue Service or other off-site responders to fulfil functions as part of their internal emergency plan. These arrangements should also include off-site Fire and Rescue Service response required to prevent/deal with a Major Accident to the Environment (MATTE).

Part 3 of this appendix provides a template for auditing the test of an external emergency plan. It can also be used as a basis for identifying those parts of an internal emergency plan that rely on off-site responders. The following are examples of areas where this is likely:

- Reliable relations between duty holders, the emergency services and other responders (e.g. the Environment Agency/HPA) are critical in the successful management of major emergencies and there should be scheduled liaison meetings held;
- if the external Fire and Rescue Service supplements on-site fire teams, the level of training and compatibility of breathing apparatus, fire fighting and other equipment must be established; and
- where an emergency plan has been produced by the Fire and Rescue Service for specific COMAH sites including rendezvous points and alternative access to the site.

The effectiveness of these arrangements should be exercised and evaluated.

When all instances of reliance on off-site responders have been identified, the adequacy of the joint arrangements should be demonstrated. Part 3 of this appendix can be used to audit a test of the emergency plan. Assumptions should be validated and emergency plans reviewed and updated as appropriate.

Part 1 of this appendix clearly defines the arrangements between the duty holder and the Fire and Rescue Service. These include but are not limited to:

- raising an alert and initial information;
- access points, suitable hard-standings for vehicles and rendezvous points;
- site information (water supplies, foam stocks, equipment details, drainage information, containment capability, evacuation arrangements, etc.);
- pre-fire plans clearly indicating firefighting capability, resources available and firewater management arrangements.

Duty holders should review their arrangements to communicate with people and establishments likely to be affected by a major accident to ensure that this information takes account of any additional major accident scenarios resulting from, for example, a large flammable vapour cloud.

Guidance on provision of information to the public is given in L111 (12) and HSG191 (64) .

REFERENCES

1. Buncefield Major Incident Investigation Board The Buncefield Incident 11 December 2005: The final report of the Major Incident Investigation Board Volume 1 HSE Books 2008 ISBN 978 0 7176 6270 8 www.buncefieldinvestigation.gov.uk
2. Investigation Report Refinery Explosion and Fire Report No 2005-04-1-TX US Chemical Safety and Hazard Investigation Report 2007. www.csb.gov/assets/document/CSBFinalReportBP.pdf
3. Reducing error and influencing behaviour HSG48 (Second edition) HSE Books 1999 ISBN 978 0 7176 2452 2
4. The Report of the BP US Refineries Independent Safety Review Panel January 2007 (The Baker Panel Report)
5. Safety Culture HSE Human Factors Briefing Note No 7 www.hse.gov.uk/humanfactors/comah/07culture.pdf
6. Leadership for the major hazard industries Leaflet INDG277(rev1) HSE Books 2004 (single copy free or priced packs of 15 ISBN 978 0 7176 2905 3)
7. A review of safety culture and safety climate literature for the development of the safety culture inspection toolkit RR367 HSE Books 2005 ISBN 0 7176 6144 X
8. Involving employees in health and safety: Forming partnerships in the chemical industry HSG217 HSE Books 2001 ISBN 978 0 7176 2053 1
9. The Center for Chemical Process Safety (CCPS) of the American Institution of Chemical Engineers (AIChE) on its website (9) (http://www.aiche.org/ccps/topics/elements-process-safety)
10. HSE internal document Process Safety Management Systems
11. BS EN ISO 9000 Quality Management Systems.
12. A guide to the Control of Major Accident Hazards Regulations 2015 (as amended). Guidance on Regulations L111 ISBN 978 0 7176 6605 8 http://www.hse.gov.uk/pubns/books/l111.htm
13. Developing process safety indicators: A step-by-step guide for chemical and major hazard industries HSG254 HSE Books 2006 ISBN 978 0 7176 6180 0
14. Health and Safety Executive, 'The Flixborough Disaster : Report of the Court of Inquiry', HMSO, ISBN 0113610750, 1975.
15. HSE's Safety Report Assessment Manual (http://www.hse.gov.uk/comah/sragtech/techmeasplantmod.htm).
16. UKPIA Guidance is available at http://www.ukpia.com/process-safety/tools/self-assessment-tools.aspx
17. Organisational change and major accident hazards Chemical Information Sheet CHIS7 HSE Books 2003 www.hse.gov.uk/pubns/comahind.htm
18. Licensee core and intelligent customer capabilities. Office for nuclear regulation NS-TAST-GD-049 http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-049.pdf
19. Managing contractors: A guide for employers. An open learning booklet HSG159 HSE Books 1997 ISBN 978 0 7176 1196 6
20. Contractorisation – aspects of health and safety in the supply train. RR112 http://www.hse.gov.uk/research/rrpdf/rr112.pdf
21. Guidance for managing shiftwork and fatigue off shore. http://www.hse.gov.uk/offshore/infosheets/is7-2008.htm
22. Successful health and safety management HSG65 (Second edition) HSE Books 1997 ISBN 978 0 7176 1276 5

23. AIChE guidelines (Guidelines for auditing process safety management systems http://www.aiche.org/ccps/publications/books/guidelines-auditing-process-safety-management-systems-2nd-edition
24. AIChE Guidelines for technical management of chemical process safety http://www.aiche.org/ccps/publications/books/guidelines-implementing-process-safety-management-systems
25. OECD Guidance on Safety Performance Indicators http://www.oecd-ilibrary.org/environment/oecd-guidance-on-safety-performance-indicators_9789264019119-en
26. Chemical Business Association guidance on Safety Performance Leading Indicators http://www.chemical.org.uk/regulatoryissues/healthandsafety/safetyperformanceleadingindicatorsspli.aspx
27. Human factors in accident investigations HSE www.hse.gov.uk/humanfactors/comah/hfaccident.htm
28. Guidance on investigating and analysing human and organisational factors aspects of incidents and accidents Energy Institute May 2008 ISBN 978 0 85293 521 7 www.energyinst.org.uk/humanfactors/incidentandaccident
29. Competence assessment for the hazardous industries RR086 HSE Books 2003 ISBN 0 7176 2167 7
30. Hopkins A Lessons from Longford: The Esso Gas Plant Explosion CCH Australia Ltd 2000 ISBN 978 1 86468 422
31. EEMUA 191 Alarm Systems – A Guide to Design, Management and Procurement Publication 191 (Second edition) Engineering Equipment Materials User's Association 2007 ISBN 978 0 85931 155 7
32. Competence HSE Human Factors Briefing Note No. 2 www.hse.gov.uk/humanfactors/comah/02competency.pdf
33. Training and Competence EI Human Factors Briefing Note No 7 Energy Institute 2003 www.energyinst.org.uk/humanfactors/bn
34. Developing and maintaining staff competence Railway Safety Publication 1 (Second edition) Office of Rail Regulation (ORR) www.rail-reg.gov.uk/upload/pdf/sf-dev-staff.pdf
35. Assessing the safety of staffing arrangements for process operations in the chemical and allied industries CRR348 HSE Books 2001 ISBN 0 7176 2044 1
36. Managing shift work: Health and safety guidance HSG256 HSE Books 2006 ISBN 978 0 7176 6197 8
37. Safe Staffing Arrangements – User Guide for CRR348/2001 Methodology: Practical application of Entec/HSE process operations staffing assessment methodology and its extension to automated plant and/or equipment Energy Institute 2004 ISBN 0 85293 411 4 www.energyinst.org.uk/humanfactors/staffing
38. Fatigue HSE Human Factors Toolkit: Note 10. www.hse.gov.uk/humanfactors/comah/10fatigue.pdf
39. Managing Fatigue Risks in the Workplace. http://www.hse.gov.uk/humanfactors/topics/specific2.pdf
40. Fatigue Human Factors Briefing Note No 5 Energy Institute 2006 www.energyinst.org.uk/
41. EEMUA 201 Process Plant Control Desks Utilising Human-Computer Interfaces – A Guide to Design, Operational and Human Interface Issues Publication 201 (Second edition) Engineering Equipment Materials User's Association 2009 ISBN 978 0 85931 167 0
42. BS EN ISO 11064: Parts 1-7 Ergonomic design of control centres British Standards Institution
43. Alarm handling Human Factors Briefing Note No 2 Energy Institute 2003 http://publishing.energyinst.org/topics/process-safety/leadership/human-factors-briefing-notes-no.-2-alarm-handling

44. Better alarm handling in the chemical and allied industries Chemical Information Sheet CHIS6 HSE Books 2000 www.hse.gov.uk/pubns/comahind.htm
45. PSLG report Safety and Environmental standards for fuel storage sites. http://www.hse.gov.uk/comah/buncefield/fuel-storage-sites.pdf
46. The mechanical integrity of plant containing hazardous substances', produced by EEMUA and SAFed in 2012 (EEMUA231, SAFed IMG1) http://www.eemua.org/Products/Publications/Digital/EEMUA-Publication-231.aspx
47. API510 Pressure vessel inspection code: In-service inspection, rating repair and alteration.
48. EEMUA Publication 159 Above ground flat bottomed storage tanks - a guide to inspection, maintenance and repair http://www.eemua.org/Products/Publications/Print/EEMUA-Publication-159-Ed4.aspx
49. API653 Above ground storage tank inspection
50. API570 Piping inspection code: In-service inspection, rating repair and alteration for piping systems.
51. Pressure Systems Safety Regulations Approved Code of Practice. Safety of pressure systems http://www.hse.gov.uk/pubns/priced/l122.pdf
52. HSE Integrity of Atmospheric storage tanks. SPC/Tech/Gen/35 http://www.hse.gov.uk/foi/internalops/hid_circs/technical_general/spctechgen35.htm
53. Mechanical integrity management of bulk storage tanks. RR760 http://www.hse.gov.uk/research/rrpdf/rr760.pdf
54. HSE Guidance Glass reinforced plastic vessels and tanks. PM75 http://www.hse.gov.uk/pubns/guidance/pm75.pdf
55. HSE Guidance Thermoplastic tank integrity management PM86 http://www.hse.gov.uk/pubns/guidance/pm86.pdf
56. Chemical storage tank systems – good practice CIRIA 598.30 http://www.ciria.org/ItemDetail?iProductCode=C598D&Category=DOWNLOAD
57. HSE Research Report RR729 Establishing the requirements for internal examination of high hazard process plant http://www.hse.gov.uk/research/rrpdf/rr729.pdf
58. Containment systems for the prevention of pollution (C736) : Secondary, tertiary and other measures for industrial and commercial premises, CIRIA C736, ISBN: 978-0-86017-740-1, (2014). This is available free to download from https://www.ciria.org/Resources/Free_publications/c736.aspx
59. BS EN 61511:2004 Functional safety instrumented systems for the process industry.
60. BS EN 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems.
61. BS 6755 Testing of valves
62. BS EN ISO 10497 Testing of valves. Fire type-testing requirements
63. Remotely operated shutoff valves (ROSOVs) for emergency isolation of hazardous substances: Guidance on good practice HSG244 http://www.hse.gov.uk/pubns/books/hsg244.htm
64. Emergency Planning for major Accidents. HSG191 http://www.hse.gov.uk/pubns/priced/hsg191.pdf
65. Fire precautions at petroleum refineries and bulk storage installations Energy Institute Model code of safe practice Part 19. http://publishing.energyinst.org/__data/assets/file/0013/51403/Pages-from-MCSP-Pt.-19.pdf
66. Environment Agency Guidance: Using controlled burn during fires PPG 28: prevent pollution. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/290140/pmho1005bjit-e-e.pdf

67. Environmental Protection Handbook for the Fire and Rescue Service http://www.ukfrs.com/Information%20and%20Research/Environment%20Agency%20and%20DCLG%20environmental%20handbook.pdf
68. Competent Authority guidance for inspectors on emergency arrangements for COMAH establishments http://www.hse.gov.uk/comah/inspectors-emergency-arrangements-comah-establishments.pdf

OTHER USEFUL PUBLICATIONS

Control of Major Accident Hazard Regulations 1999
The safety report assessment manual Open document under 'Code of Practice on Access to Government Information' HSE www.hse.gov.uk/comah/sram/s2-7.pdf
Major accident prevention policies for lower-tier COMAH establishments Chemical Information Sheet CHIS3 HSE Books 1999 www.hse.gov.uk/pubns/comahind.htm
Assessing Compliance with the Law in Individual Cases and the Use of Good Practice HSE ALARP Suite May 2003 www.hse.gov.uk/risk/theory/alarp2.htm

Health and safety management (general)
Management of health and safety at work. Management of Health and Safety at Work Regulations 1999. Approved Code of Practice and guidance L21 (Second edition) HSE Books 2000 ISBN 978 0 7176 2488 1
Managing health and safety: An open learning book for managers and trainers HSE Books 1997 ISBN 978 0 7176 1153 9 (out of print)
Formula for health and safety: Guidance for small and medium-sized firms in the chemical industry HSG166 HSE Books 1997 ISBN 978 0 7176 0996 3
HID CI / SI Inspection Manual Open document under 'Code of Practice on Access to Government Information' HSE 2001
www.hse.gov.uk/foi/internalops/hid/manuals/pmenf05.pdf Chapters on 'Risk Control Systems' including RCS 11 Assessing Auditing on pages 184–187

Process safety management (general)
Guidelines for Risk Based Process Safety Center for Chemical Process Safety 2007 ISBN 978 0 470 16569 0
Guidelines for Implementing Process Safety Management Systems Center for Chemical Process Safety 1994 ISBN 978 0 8169 0590 4
Guidelines for Auditing Process Safety Management Systems Center for Chemical Process Safety 1993 ISBN 978 0 8169 0556 8
Guidelines for Technical Management of Chemical Process Safety Center for Chemical Process Safety 1989 ISBN 978 0 8169 0423 5
Plant Guidelines for Technical Management of Chemical Process Safety Center for Chemical Process Safety 1992 ISBN 978 0 8169 0499 0
Process safety management systems SPC/TECH/OSD/13 OSD Internal Document HSE www.hse.gov.uk/foi/internalops/hid/spc/spctosd13.pdf
Guidance on safety performance indicators OECD http://www2.oecd.org/safetyindicators

Human factors (general)
Human factors integration: Implementation in the onshore and offshore industries RR001 HSE 2002 www.hse.gov.uk/research/rrhtm/rr001.htm

The promotion of human factors in the onshore and offshore hazardous industries RR149 HSE Books 2003 ISBN 0 7176 2739 X
Mutual misconceptions between designers and operators of hazardous installations RR054 HSE Books 2003 ISBN 0 7176 2622 9
Development of human factors methods and associated standards for major hazard industries RR081 HSE Books 2003 ISBN 0 7176 2678 4

Leadership and safety culture

Managing Human Error Number 156 Parliamentary Office of Science and Technology June 2001 www.parliament.uk/post/pn156.pdf
Health and Safety Climate Survey Tool (electronic publication) HSE Books 1998 ISBN 978 0 7176 1462 2

Key performance indicators

Developing process safety indicators: A step-by-step guide for chemical and major hazard industries HSG254 HSE Books 2006 ISBN 978 0 7176 6180 0
Guidance on safety performance indicators OECD
http://www2.oecd.org/safetyindicators

Staffing, shift work arrangements, and working conditions

The development of a fatigue/risk index for shift workers RR446 HSE Books 2006 www.hse.gov.uk/research/rrhtm/index.htm
Horne JA and Reyner LA 'Vehicle accidents related to sleep: A review' Occupational and Environmental Medicine 1999 56 (5) 289–294
Improving alertness through effective fatigue management Energy Institute, London September 2006 ISBN 978 0 85293 460 9 www.energyinst.org.uk/

Management of change

Organisational change and transition management HSE Human Factors Toolkit: Specific Topic 3 www.hse.gov.uk/humanfactors/comah/specific3.pdf
'Assessing Risk Control Systems – RCS5 Management of Plant and Process Change' in HID CI/SI Inspection Manual HSE 2001 pages 135–145 www.hse.gov.uk/foi/internalops/hid/manuals/pmenf05.pdf
Guidelines for the Management of Change for Process Safety CCPS 2008 ISBN 978 0 470 04309 7

Competence

Competence HSE Human Factors Briefing Note No. 2
www.hse.gov.uk/humanfactors/comah/02competency.pdf
Competence assurance HSE Core Topic 1
www.hse.gov.uk/humanfactors/comah/core1.pdf
'Assessing Risk Control Systems – RCS12 Assessing Competence' in HID CI/SI Inspection Manual HSE 2001 pages 188–191
www.hse.gov.uk/foi/internalops/hid/manuals/pmenf05.pdf
Cogent National Occupational Standards Bulk Liquid Operations Level 2
Cogent National Occupational Standards Downstream Operations Level 3

Management of contractors

Backs for the future: Safe manual handling in construction HSG149 HSE Books 2000 ISBN 978 0 7176 1122 5

'Assessing Risk Control Systems – RCS7 Selection and Management of Contractors' in HID CI/SI Inspection Manual HSE 2001 pages 150–155
www.hse.gov.uk/foi/internalops/hid/manuals/pmenf05.pdf
Contractorisation Technical Assessment Guide T/AST/052 HSE 2002
www.hse.gov.uk/foi/internalops/nsd/tech_asst_guides/tast052.pdf
Principles for the assessment of a licensee's 'intelligent customer capability' Technical Assessment Guide T/AST/049 Issue 002 23/10/2006 HSE 2006
www.hse.gov.uk/foi/internalops/nsd/tech_asst_guides/tast049.pdf and Draft Revision of T/AST/049 (also replacing T/AST/052) 20 Mar 2009)
The use of contractors in the maintenance of the mainline railway infrastructure: A report by the Health and Safety Commission May 2002 HSC 2002
www.rail-reg.gov.uk/upload/pdf/contrail.pdf
Health and Safety Management Systems Interfacing 2003 download available from Step Change in Safety website http://stepchangeinsafety.net/stepchange/
The Client Contractor National Safety Group Safety Passport www.ccnsg.com/

Safety-critical communications and written procedures

Interface Management – Effective Communication to Improve Process Safety CCPS AIChE 2004
www.aiche.org/uploadedFiles/CCPS/Publications/SafetyAlerts/CCPSAlertInterface.pdf
International Safety Guide for Oil Tankers and Terminals (ISGOTT) (Fifth Edition) International Chamber of Shipping 2006 ISBN 978 1 85609 292 0
'Effective Shift Communication' – extract from Reducing error and influencing behaviour HSG48 (Second edition) HSE Books 1999 ISBN 978 0 7176 2452 2 (reprinted 2003) pages 38–39
Human factors: Safety critical communications HSE
www.hse.gov.uk/humanfactors/comah/safetycritical.htm
Safety-critical communications Human Factors Briefing Note No 8 HSE
www.hse.gov.uk/humanfactors/comah/08communications.pdf
Reliability and usability of procedures Core Topic 4 HSE
www.hse.gov.uk/humanfactors/comah/core4.pdf
Revitalising Procedures HSE www.hse.gov.uk/humanfactors/comah/procinfo.pdf
Improving compliance with safety procedures: Reducing industrial violations HSE Books 1995 HSE Books 1995
www.hse.gov.uk/humanfactors/comah/improvecompliance.pdf
'Assessing Risk Control Systems – RCS3 Operating Procedures' in HID CI/SI Inspection Manual HSE 2001 pages 114-125
www.hse.gov.uk/foi/internalops/hid/manuals/pmenf05.pdf

Storage and transfer (general)

The storage of flammable liquids in tanks HSG176 HSE Books 1998 ISBN 978 0 7176 1470 7
The bulk transfer of dangerous liquids and gases between ship and shore HSG186 HSE Books 1999 ISBN 978 0 7176 1644 2
Safe use and handling of flammable liquids HSG140 HSE Books 1996 ISBN 978 0 7176 0967 3
Procedures for offloading products into bulk storage at plants and terminals RC 106 Chemical Industries Association 1999 ISBN 978 1 85897 087 5
www.cia.org.uk/newsite/

Control and alarm systems

Out of control: Why control systems go wrong and how to prevent failure HSG238 HSE Books ISBN 978 0 7176 2192 7

Alarm handling HSE Human Factors Briefing Note No 9 HSE www.hse.gov.uk/humanfactors/comah/09alarms.pdf