A Management Overview of Safety Management Systems and Processes for High-Hazard Industries

This note provides a very brief, very high-level overview of some of the key safety management processes, techniques and tools that should be in place for high-hazard industries. It is intended that the processes presented are more-or-less generic to any high-hazard industry, including nuclear, oil and gas, and petrochemical process plant.

Safety management processes include:

- Personnel recruitment, competence assurance and training
- Safe working arrangements
- Design engineering and safety functional requirements
- Technical safety and technical risk assessments
- Engineering design change (including temporary modifications)
- Software design
- Accident and incident investigation
- Emergency planning

Each of these processes is addressed in more detail below. Other important safety management processes that are not included here include operating and maintenance procedures, Project Quality Assurance arrangements, the control of subcontractors, and security arrangements (including Information Technology security).

Senior management's role is not just to ensure that appropriate management arrangements are in place - there is also a crucial role in high-hazard industries for senior managers to send clear and unambiguous messages to personnel at all levels about the importance of safety. This must mean more than just repeating the tired old cliché 'safety is our top priority'; senior managers have to live the values, and be seen to send consistent messages at all times. This is especially important at times when budgets are under review: safety has to maintain its importance, and senior management have to be quite clear about this in all they say and do.

THE HEALTH, SAFETY AND ENVIRONMENTAL MANAGEMENT SYSTEM

All of the management systems listed above are important; there are no 'optional' items, although extra items may be appropriate. In an effective organisation, these items are captured within a Health, Safety and Environmental Management System – the HSE-MS – and are kept under regular review (Figure 1). The HSE-MS consists of enabling arrangements such as Leadership and Organisation, Competence Assurance and Training, Work Planning, Audits, Corrective Action Tracking, and Security, as well as the details of Health, Safety and Environment management arrangements.

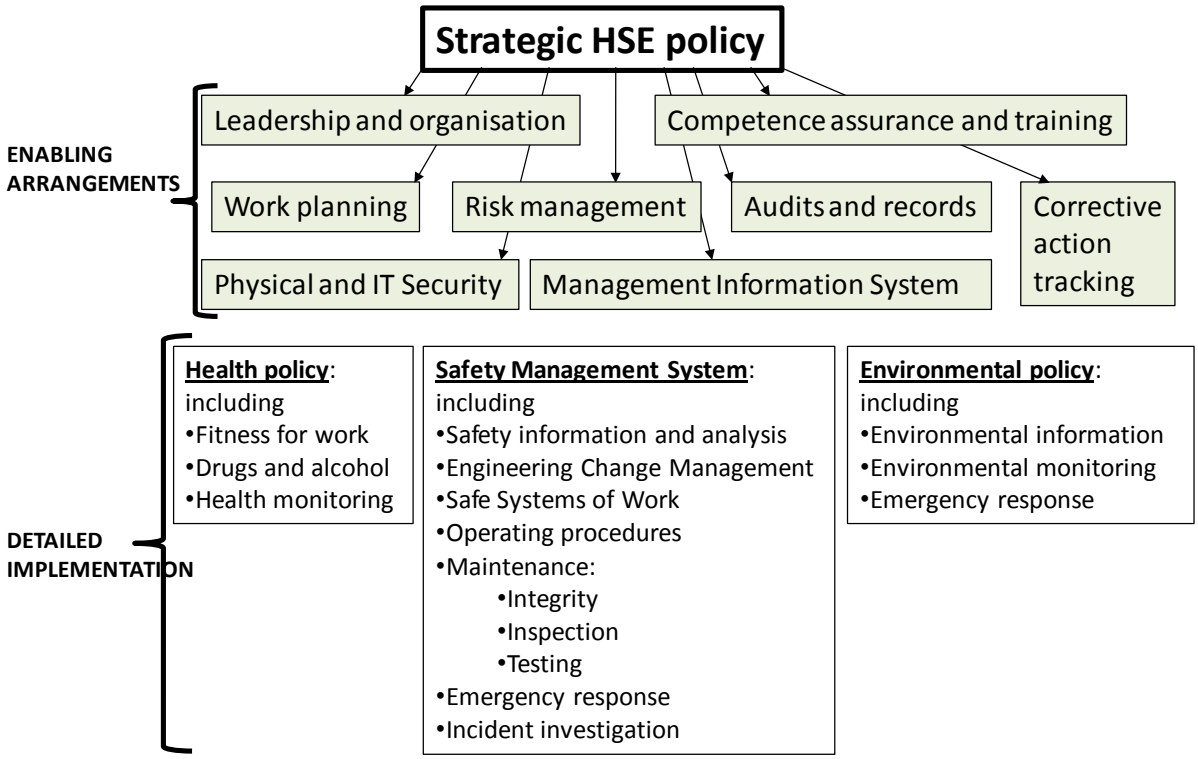

Fig 1 Key elements of a company's Health, Safety and Environmental Management System (HSE-MS)

The HSE-MS includes the Safety Management System (SMS). The SMS addresses worker safety and major accident risk and controls. Hence the SMS includes, for example, safe working arrangements (including the Permit to Work arrangements), the technical safety justification of the plant, the Quality Assurance arrangements for design engineering and site construction work, and the arrangements for ensuring that there are sufficient suitably qualified and experienced people. The SMS will also include arrangements for carrying out periodic reviews of the technical safety justification - the 'Safety Case' (Figure 2).

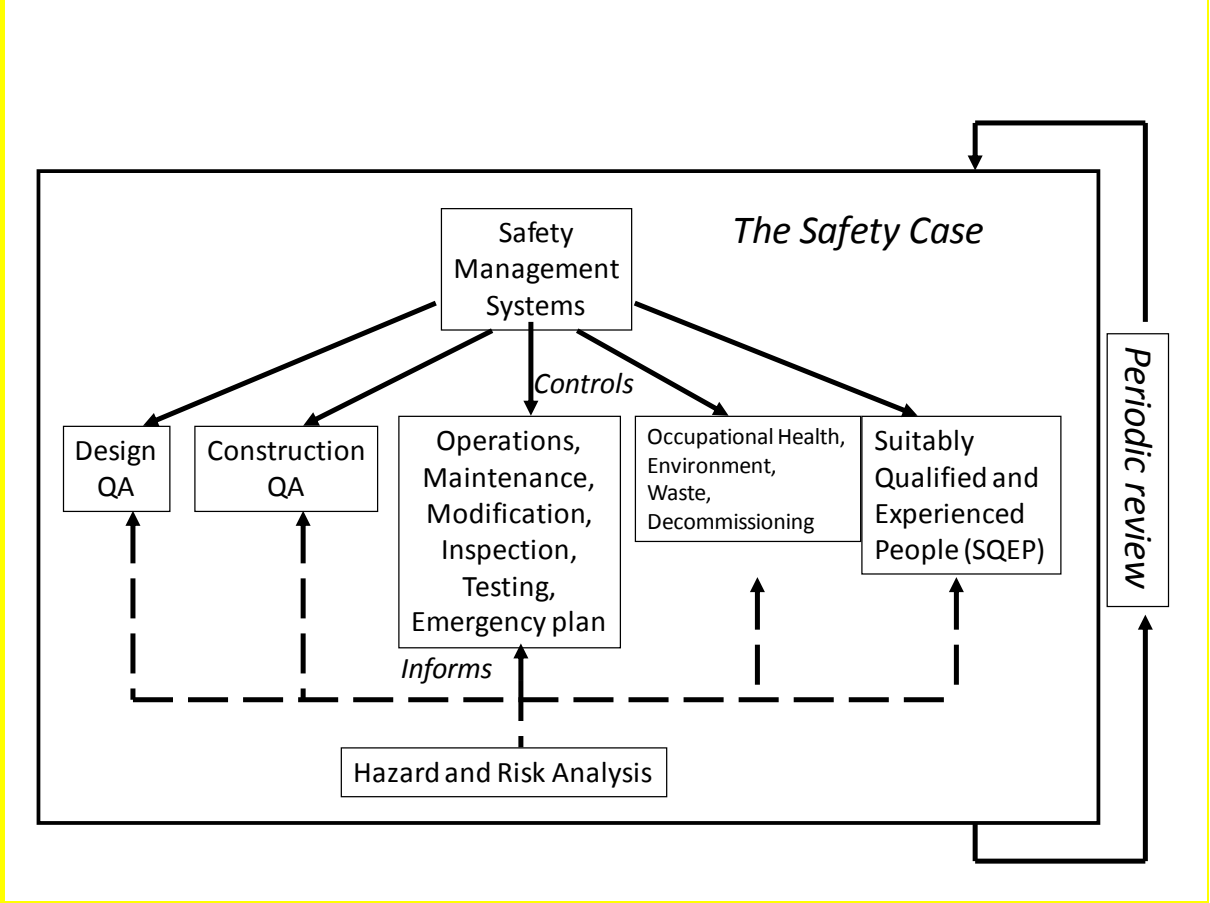

Fig 2 Safety Management System (SMS) and the Safety Case

PERSONNEL RECRUITMENT AND TRAINING

Ultimately, all safety comes down to people doing the right things, which means that recruitment, training, and succession planning arrangements need to be reviewed and maintained from a safety perspective. Companies need to recruit, develop and retain suitably qualified and experienced people (sometimes known as SQEPs).

In recruitment and training, risk-takers do not make good employees in front-line roles in the operations and maintenance for high-hazard industries. Situations where individuals are placed in the position of having to make risk-related decisions under time pressure can lead to accidents. Staff selection processes and training need to ensure that any risk-taking tendencies are firmly discouraged in front-line roles. All personnel need to be reminded regularly that delays because of safety concerns are alright; it must always be perfectly acceptable for employees to check 'up the line' whether a situation is safe, and to double check elsewhere if they are unhappy with the answer received.

SAFE WORKING ARRANGEMENTS

Wherever there is a potential for a major accident on hazardous plant, safe working arrangements are necessary. These require conscientious, diligent people working through procedures which are designed to minimise risk, either to the individual doing a job or to the plant itself.

These procedures begin by having clear statements of how certain activities will be carried out on site. The range of activities addressed will typically include: Welding; Confined space working; Scaffolding; Radiography; Working at height; and underwater work. There should also be clear definitions regarding the availability of essential or safety-related plant – for example, emergency shutdown systems, fire detection equipment, fire suppression equipment, or backup electricity supplies. These types of procedures and definitions may be given names such as 'Operating Rules' or 'Site Safety Policies' (Figure 3, top right.)

Next, there has to be controlled means of introducing new work into the work planning system. Plant defects must be logged and tagged, to ensure they are not forgotten about. Urgent work must be given priority. Non-urgent work must be scheduled for a suitable later time. Work to be done in scheduled shutdowns (both routine maintenance and inspection activities and non-urgent defect repair work) must be carefully planned, often long in advance, to ensure that the planned shutdown takes place in the most efficient way possible (Figure 3, top left).

For each job, there should be clear definition and scope of work, a method statement, an isolation and de-isolation procedure where necessary, and a Job Risk Assessment. The Job Risk Assessment addresses the hazards of the specific job, and should be done by people who are familiar with the plant and the type of work (Figure 3, centre). The output from this process is the Permit to Work for doing the specific job.

Next, the necessary isolations are completed and an isolation certificate is issued. The isolations are all locked and keys put in a locked cabinet, with the key held by the person in charge of doing the work. At that point, a pre-job brief can be given to the workers doing the job, and they complete the work. Afterwards, the plant is de-isolated, and the Permit to Work is withdrawn (Figure 3, bottom).

This seems like an awful lot of paperwork and effort, sometimes to do even a simple task. However, bitter experience has shown that this sort of thoroughness is essential to avoid accidents.

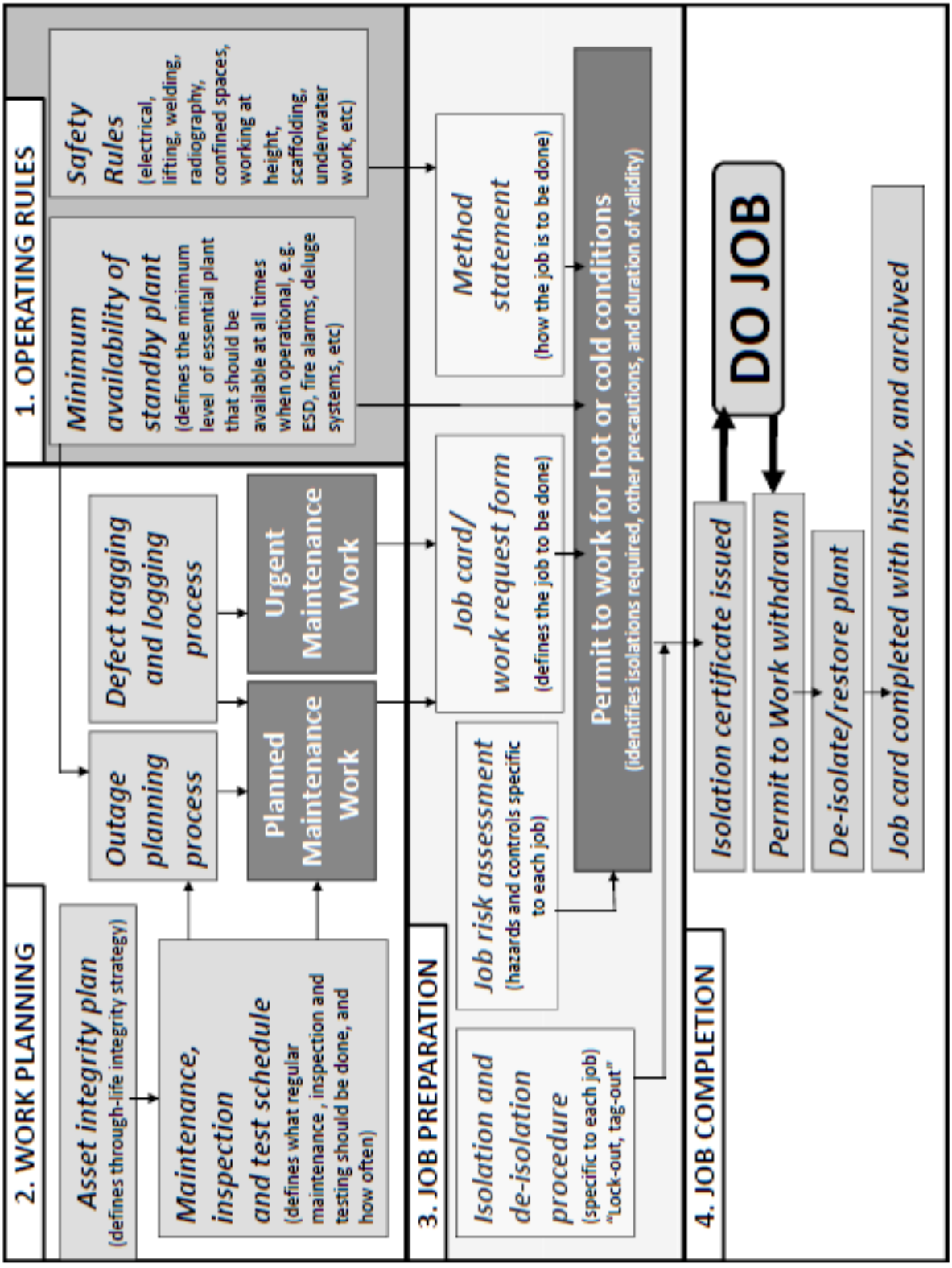

Fig 3 Safe working arrangements and Permits to Work

DESIGN ENGINEERING AND SAFETY FUNCTIONAL REQUIREMENTS

Design Engineering as applied to high-hazard plant begins with a design concept which develops in an iterative way until a 'frozen' design specification is available; at that point, detailed design can begin. This process is sometimes called Front End Engineering Design or FEED.

In broad terms, the process for producing a specification for a safe design involves Hazard Identification (HAZID), which asks 'What sort of accidents do we need to worry about?', followed by detailed analysis to identify the magnitude of potential accidents. From a safety perspective, a most important step is the clear and robust definition of the safety functional requirements, that is, the requirements for the control and protection systems on the completed plant. The history of accidents involving design failures show that very often a root cause is that some of the safety functional requirements were inaccurately or inadequately defined.

Thereafter the designers have to identify the necessary barriers and controls for the identified hazards and safety functional requirements. (A barrier or a control which prevents a hazard is called a Safety Critical Element (SCE).) The barriers and controls will typically consist of a mixture of mechanical barriers, Instrumentation and Control (I&C) systems, and fire-fighting systems, combined with administrative controls. Functional requirement specifications for all the necessary SCEs are then included in the overall design specification.

Operability and maintainability studies may be necessary before a final design specification can be issued. Input from experienced operations and maintenance engineers will be required.

The flowchart in Figure 4 presents an idealised view of the conceptual design process.

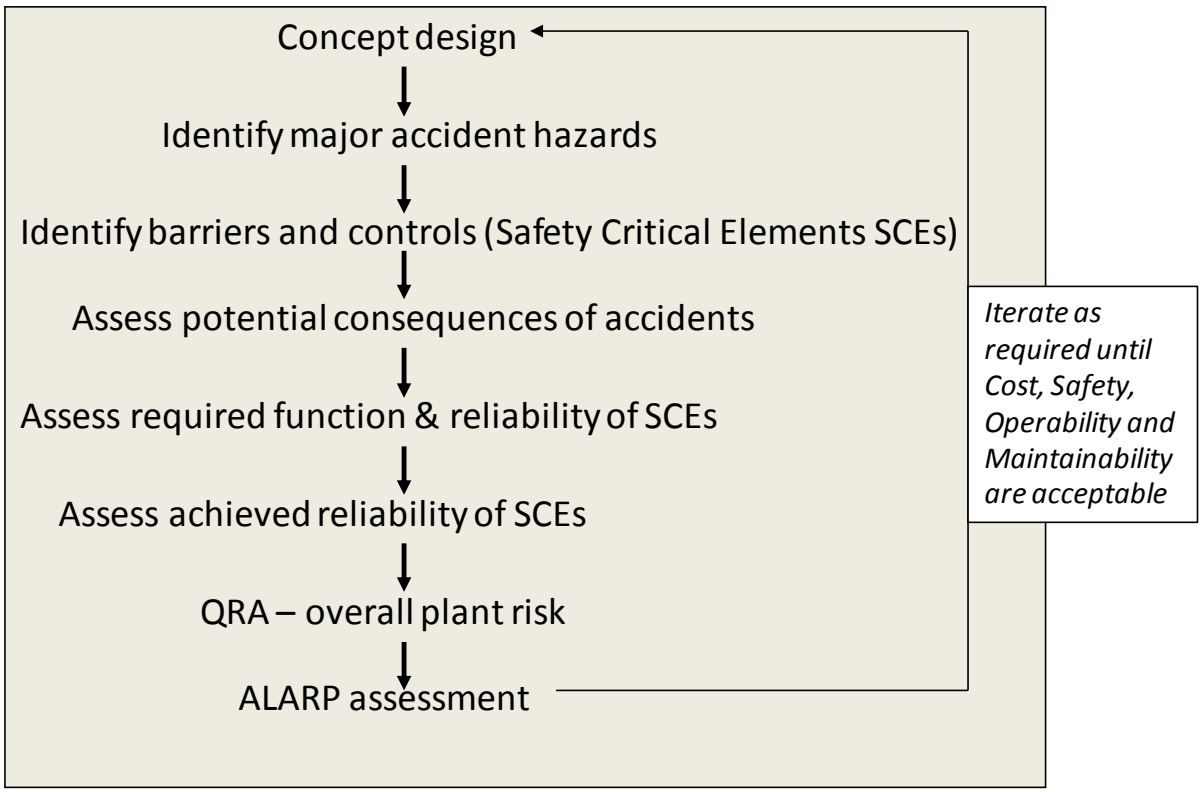

Fig 4 Safety aspects of Front End Engineering Design (FEED)

QRA = Quantified Risk Assessment

ALARP = As Low as Reasonably Practicable

TECHNICAL SAFETY AND TECHNICAL RISK ASSESSMENTS

The principal objective of technical safety assessments is to demonstrate that the risk associated with plant operations is 'As Low As Reasonably Practicable' (ALARP). First, the assessed frequency of major accidents has to be better than the applied 'tolerable risk' threshold. Thereafter, there must be a balance between the cost of further risk reduction, and the assessed frequency of major accidents causing fatalities.

In addition to the requirements of Front End Engineering Design, technical safety and risk assessments are needed at other stages of a plant's lifecycle, for example to justify plant modification work or as part of periodic plant safety reviews. The range of jargon that has developed around technical safety and risk analysis can be quite bewildering for the ingénue: a wide range of acronyms are used, and it is quite common to attend meetings with experts where it seems like entire sentences can be constructed from acronyms. This section gives an extremely brief overview of technical safety and risk assessment methodologies – a quick reference guide, if you like, for non-experts who have found themselves caught up in a blizzard of acronyms.

I have separated the techniques into two types: Qualitative methods are shown in Figure 5, and Quantitative or Semi-quantitative methods are shown in Figure 6.

HAZID was introduced in the discussion above about Front End Engineering Design (FEED). A group of suitably experienced people will meet to identify the range and likely magnitude of hazards associated with a hazardous plant. This can then lead to a Hazard and Effects Register, which identifies the hazards and their likely magnitudes, potential threats which could lead to the hazard becoming an accident, and (ultimately) suggested ways in which the hazard could be controlled.

Layers Of Protection Analysis (LOPA) is used to identify how many barriers are needed for a given hazard. It can be used during FEED to examine basic design alternatives and provide guidance to select a design that has lower initiating event frequencies, or a lower consequence, or for which the number and type of independent protection systems are "better" than alternatives. Ideally, LOPA could be used to design a process that is "inherently safer" by providing an objective method to compare alternative designs quickly and quantifiably.

In contrast, Hazard and operability Studies (HAZOP) are used for analysing the detailed design of process plants. HAZOP studies involve groups of experienced people, sometimes over many days or even weeks, sitting together and reviewing in detail the operation of process plant. The detailed process flow diagram is used as the basis for the discussion and key words are applied at each node in the flow chart to prompt discussion about what would happen if something went wrong.

Two other techniques, ESSA and EERA, are used to assess the effects of major accidents. Essential Systems Survivability Analysis (ESSA) is as its name implies; analysis is carried out to see whether essential systems such as Emergency Shutdown (ESD) or fire-fighting systems can survive, say, flood or localised fire. Escape, Evacuation and Rescue Analysis (EERA) is used in particular in offshore platforms where it is important to have diverse routes between any point on the platform and the emergency lifeboats (Totally Enclosed Motor Propelled Survival Craft, TEMPSC).

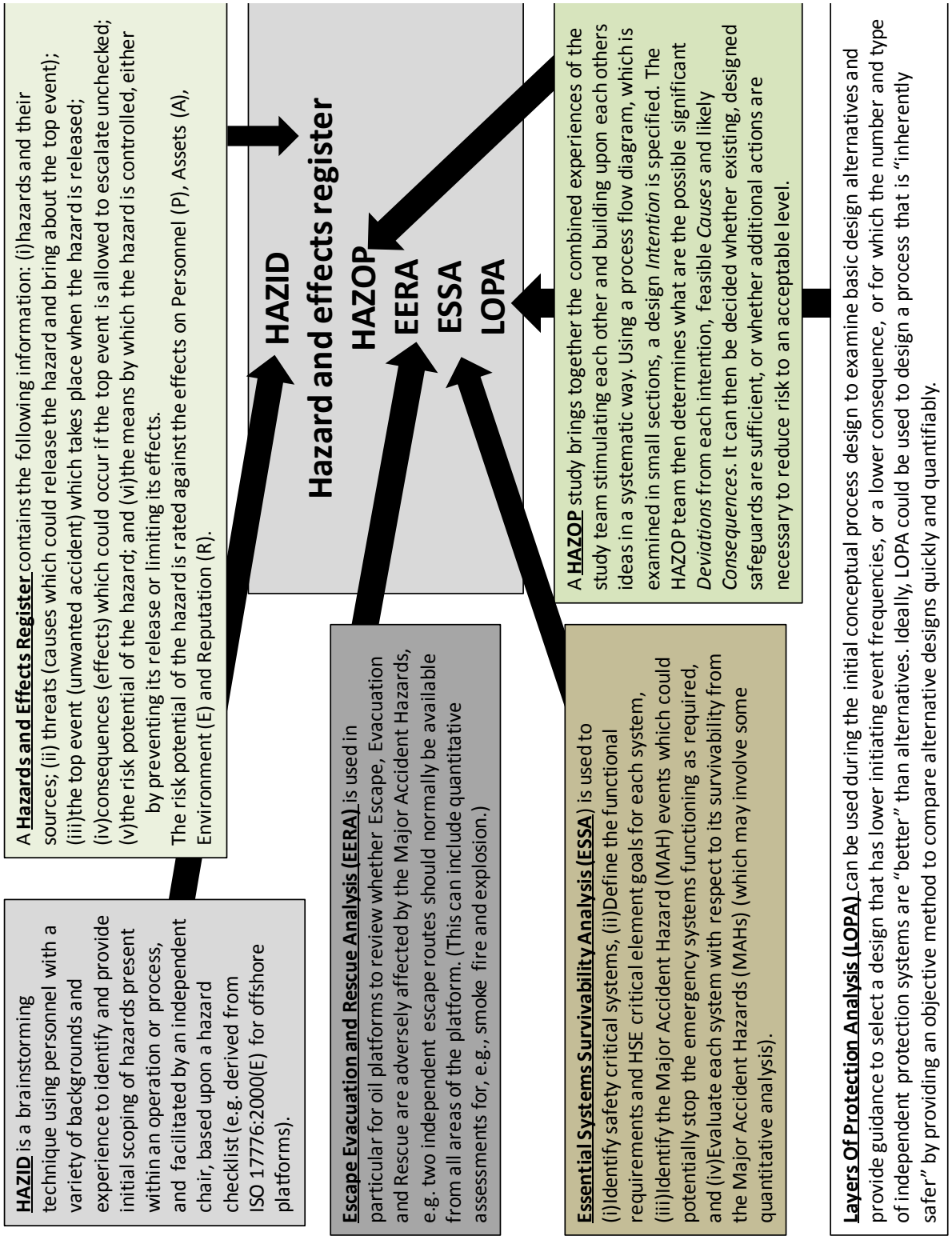

Fig 5 Some qualitative techniques used in technical safety and risk assessments.

Quantitative and semi-quantitative methods are summarised in Figure 6.

Safety Integrity Level (SIL) assessment is used during Front End Engineering Design to develop the reliability requirements for control and protection systems. This is normally done in accordance with international standards such as IEC 61508.

Fault trees, Failure Modes and Effects Analysis (FMEA), Failure Modes Effects and Criticality Analysis (FMECA) and event trees use logic, reliability data (component failure rates), and assessed system failure rates, combined with human error failure rates (using methodologies such as HEART or THERP) and other methodologies such as software reliability assessment, to develop estimates of plant accident frequencies.

In technical safety, risk is a function of accident frequency and accident consequences. 'Pure' Quantified Risk Assessment (QRA, also called Probabilistic Risk Assessment or PRA) typically uses mortality (that is, the number of assessed deaths in any given potential accident situation) as a measure of consequences. The overall risk for a variety of potential accidents at a particular process plant can be plotted against recognised risk criteria in a graph of accident frequency against mortality, to help make judgments about whether the plant is 'acceptably safe' or not.

Semi-quantitative risk assessment methods are less exacting about how accident frequency and consequences are calculated. For a large organisation with many hazardous facilities, it is normal for their risks to be judged against overall industry accident records. Figure 7 shows a typical (hypothetical) table of risk criteria for a large multinational company operating hazardous facilities. A table such as this can be used as an aid to judgment when prioritising capital expenditure for safety improvements across different types of facilities operating in different countries.

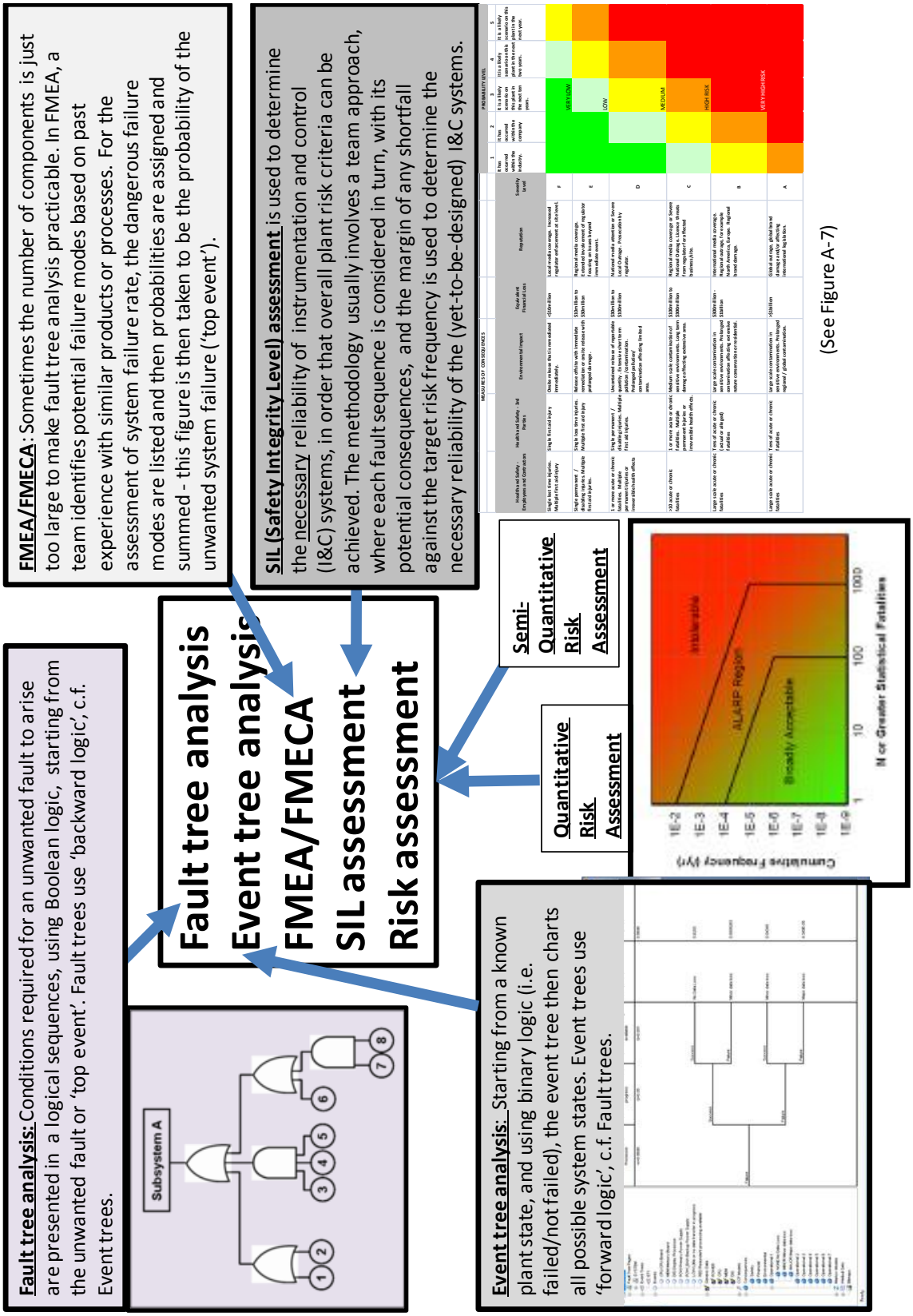

Fig 6 Quantitative and semi-quantitative methods used in technical safety and risk analysis

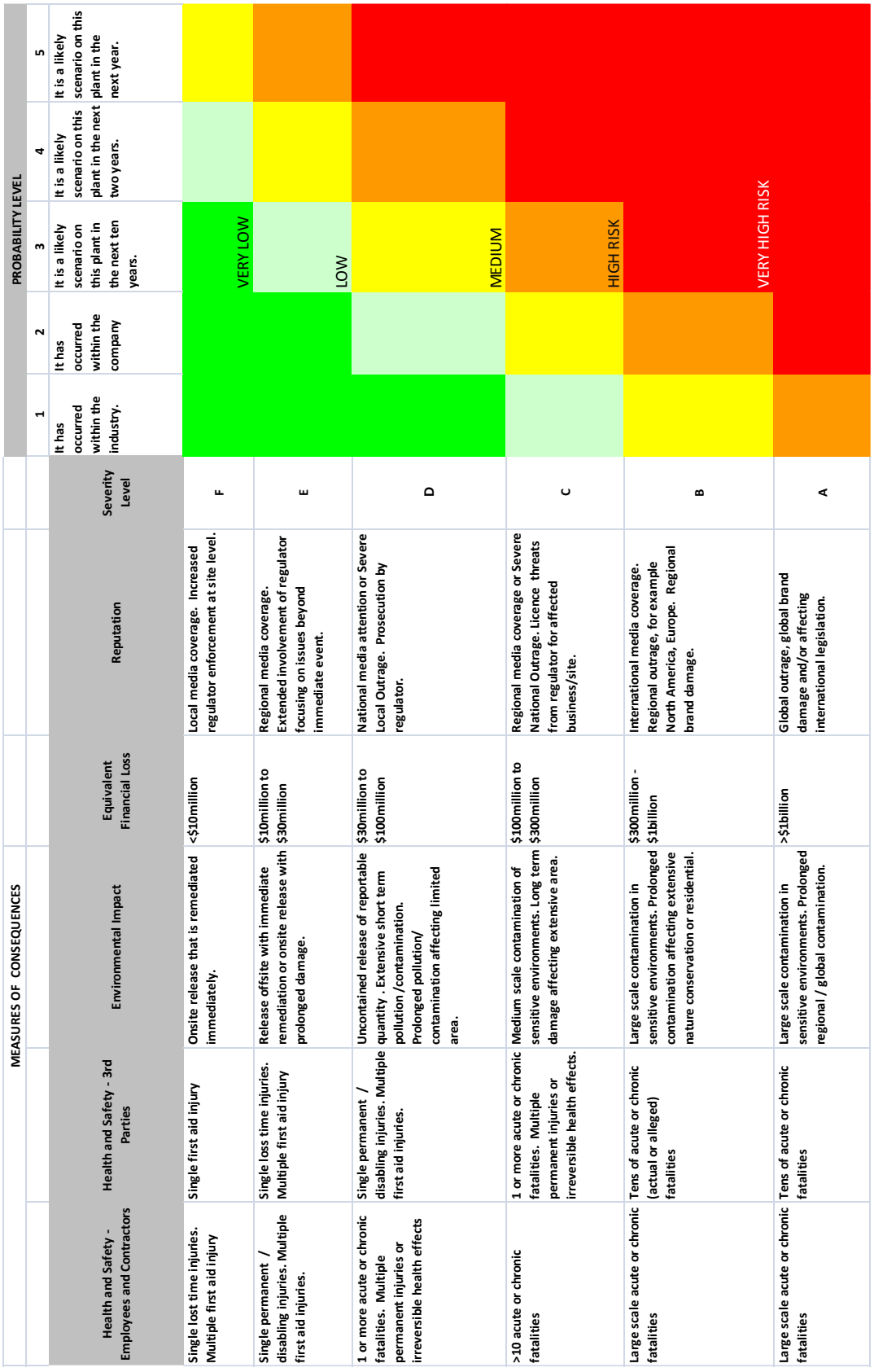

Fig 7 A typical table of risk criteria for a large multinational company operating hazardous facilities, as might be used in prioritising safety-related capital spending across different facilities in various countries

ENGINEERING CHANGES

Engineering changes require thorough and careful consideration – just as much as the original design. The amount of care, attention and independent review will depend on the perceived potential risk associated with the change. Hence, modifications are usually classified according to the risk that would arise if the modification were "inadequately conceived or executed"; in other words, how bad would the risk become if the modification was fundamentally flawed. Where the risk arising from this classification is 'high', there may be a requirement for independent assessment.

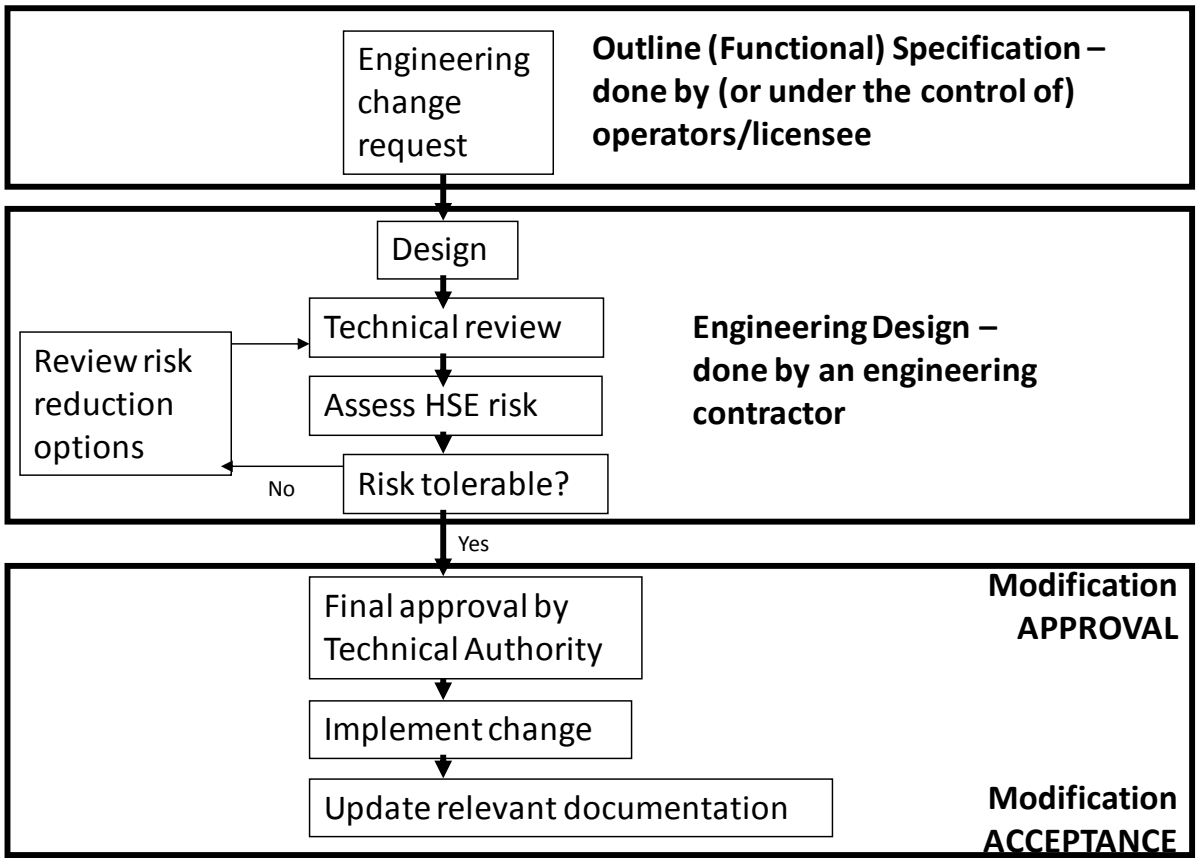

Fig 8 Typical process for Engineering Change

Another category of Engineering Change, which is particularly prone to abuse unless managed carefully, is Temporary Modifications or Overrides. Ideally, these should never be required, but in the real world they are inevitable, so there have to be robust means of ensuring that temporary changes are given careful consideration, and that the temporary arrangement is regularised at the earliest possible opportunity. Figure A-9 shows some of the main factors that have to be taken into consideration when designing a temporary modification process.

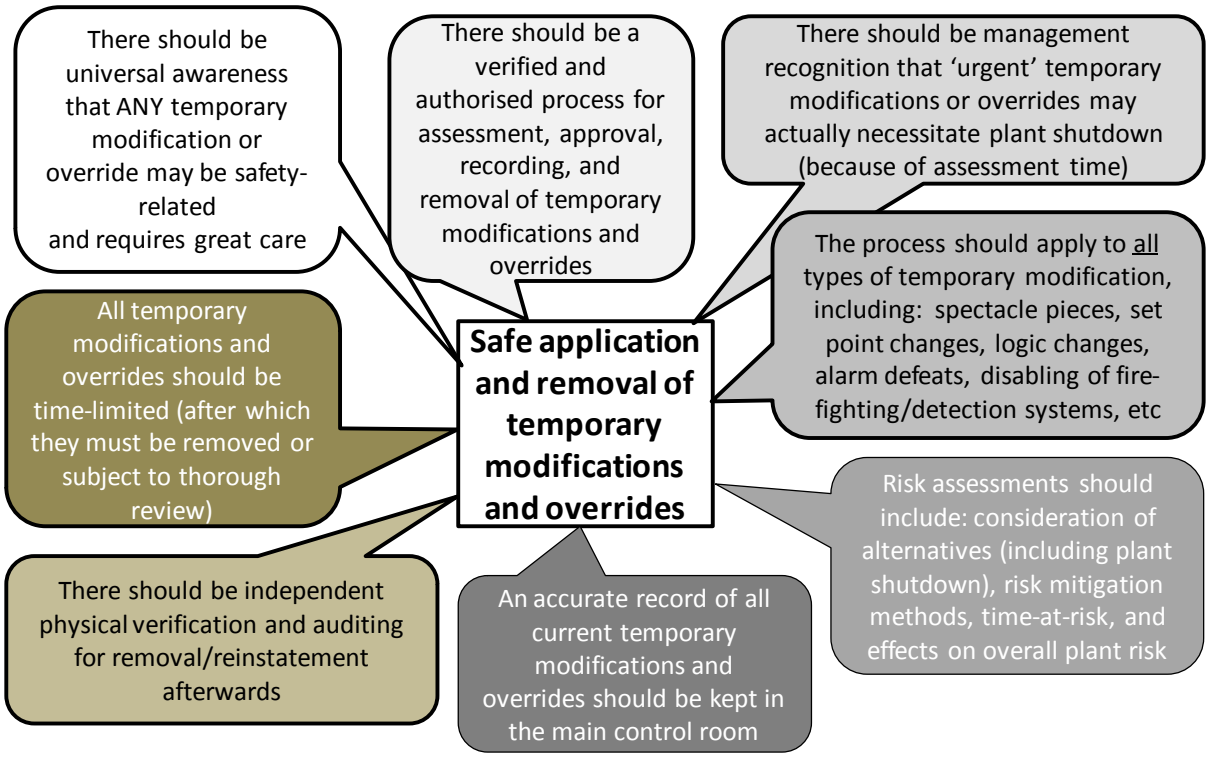

Fig 9 Some key requirements in a temporary modification process

An important concept here is configuration management; it is essential that operations management knows the exact plant state at any given time. Operations management must always be in full control of the plant state.

SOFTWARE DESIGN

All new industrial plant includes software-based automation, monitoring and protection systems. A major challenge is to ensure that plant design engineers communicate their requirements clearly and accurately to the software engineers (who do the software coding), and then to ensure by means of testing that the software produced has correctly implemented the requirements.

The problem here is that the software engineers doing the coding may not actually understand the safety and operational issues for the plant. Hence, the specification for the software engineers must be precise and unambiguous. This difficult interface between plant designers and software engineers have led to the 'V-model' where a great deal of effort is placed, first, to ensure that the detailed software specifications are correct, and then to ensure that the coverage of test procedures is such that all important safety and operational requirements are correctly implemented. This approach is detailed in the international standard IEC 61508. This process is commonly called 'software V&V', that is, 'verification and validation'.

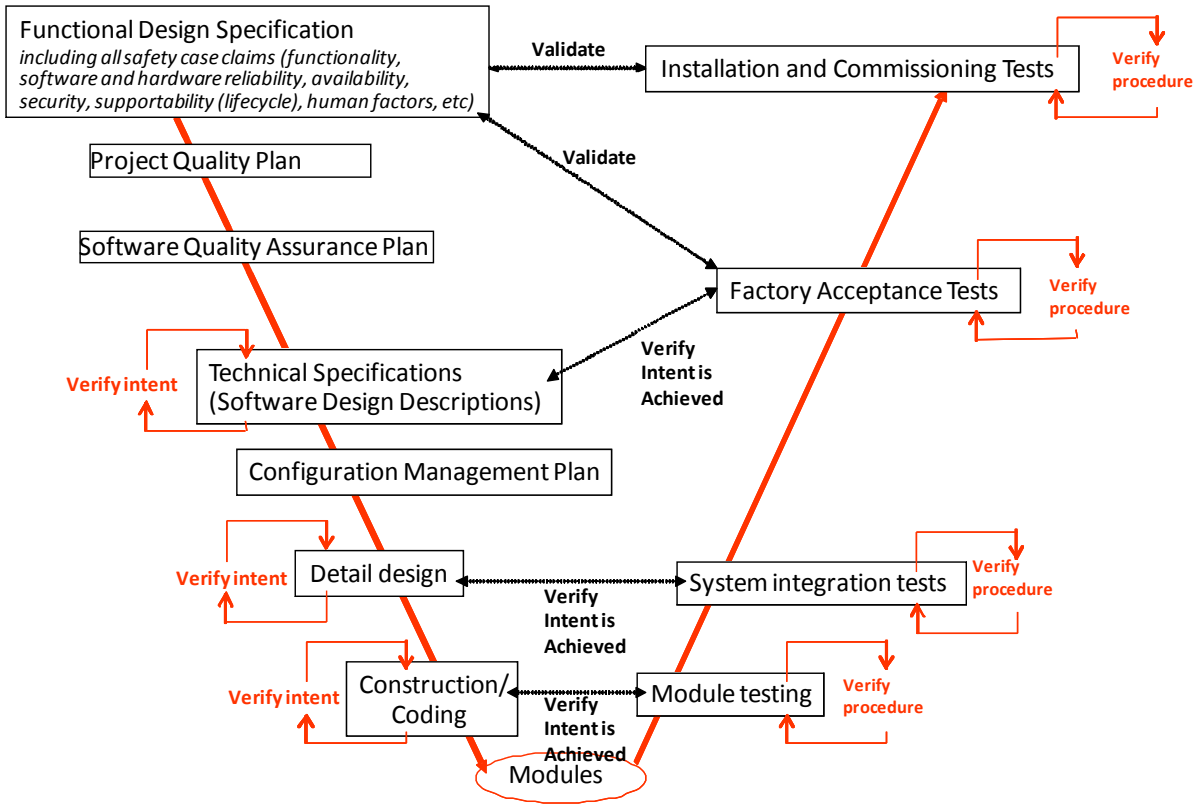

Fig 10 The V-model for design, production and testing of software-based automation, monitoring and protection systems

Safety-related software development projects require a number of key elements to be carefully established from the beginning. Although some of these are common with all major projects, others are quite specific to software projects. Figure 11 outlines the main elements.

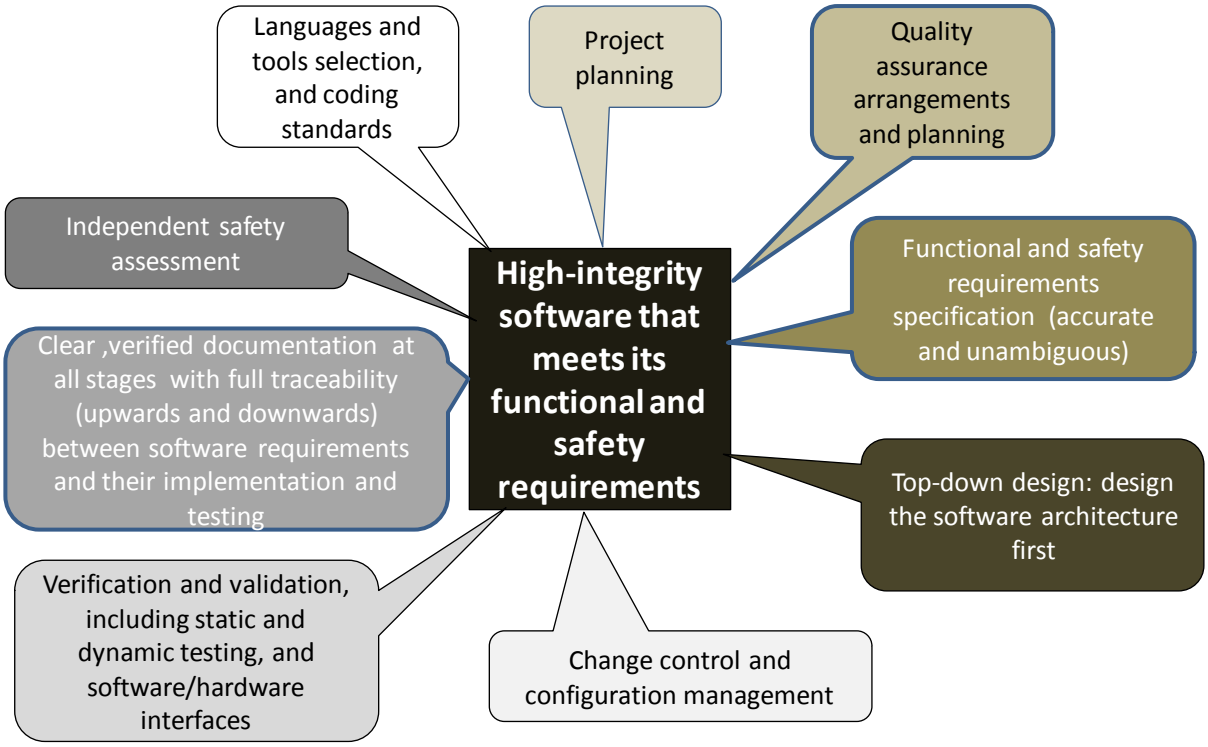

Fig 11 The main elements of a safety-related software development project

ACCIDENT AND INCIDENT INVESTIGATIONS

Data on accidents and incidents show that, for every major accident, there may be dozens or even hundreds of minor incidents which might have escalated into a worse situation. It is important that the organisation tries to learn from minor incidents and anomalies to ensure no repetition and to avoid possible escalation into something worse. Hence, the management of high-hazard plant should have processes in place to review incidents, learn the important lessons, identify the root causes, implement the necessary changes promptly, and educate all the relevant people about the changes.

A typical flowchart for a root cause analysis process is shown in Figure 12.

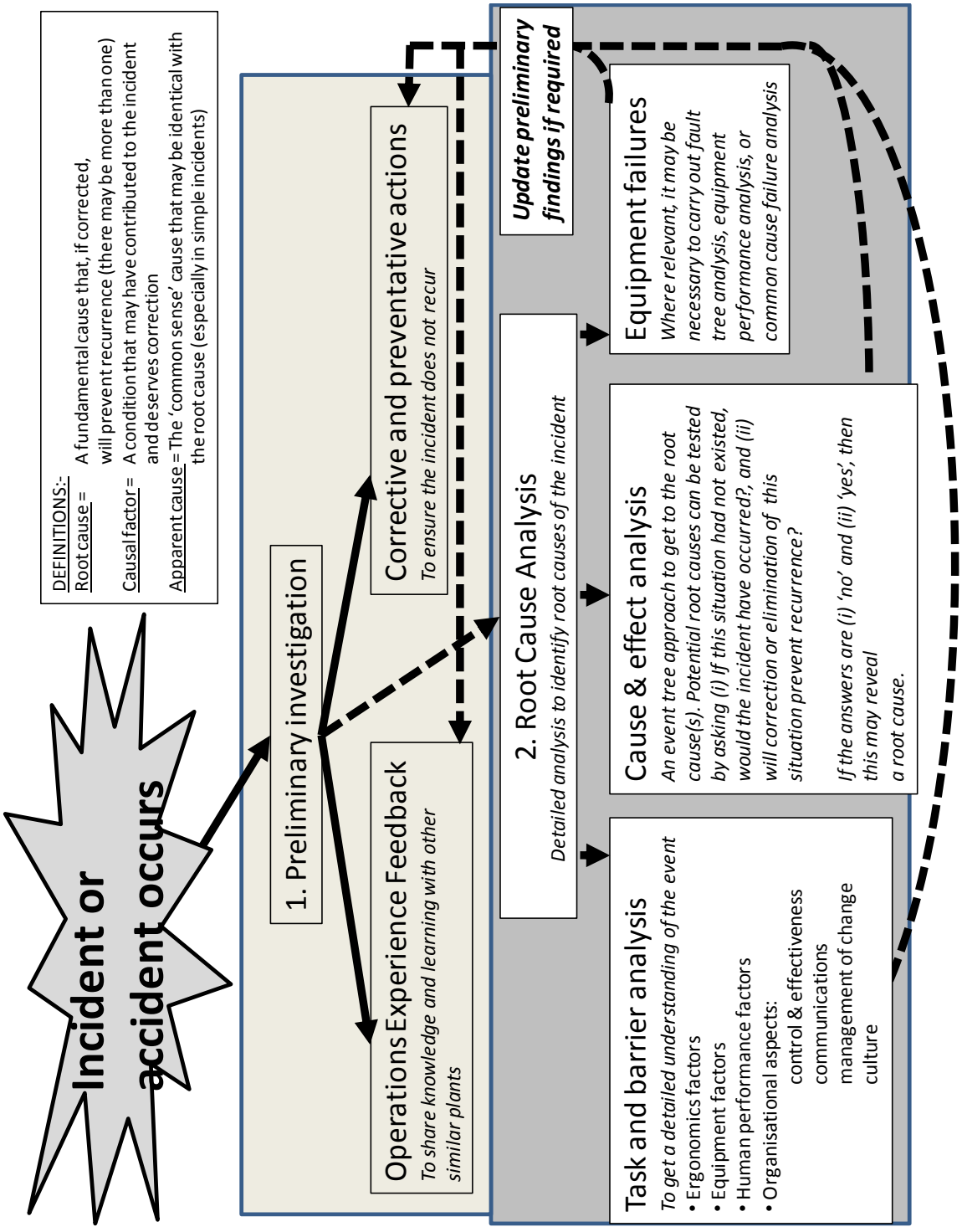

Fig 12 Accident and incident investigation and root cause analysis

EMERGENCY PLANNING

Typical outline scopes and objectives of the emergency planning arrangements for hazardous facilities are given below.

Nuclear Power Stations, Petrochemical and Chemical Plants

Basic objectives of Emergency Plan:

1. Muster and headcount to identify any missing persons.
2. Recovery and treatment of injured personnel.
3. Evacuation of non-essential station staff.
4. Termination or mitigation of the incident.
5. Surveys of surrounding area to establish extent of contamination.
6. Minimise radiation exposure/toxin uptake to the general public by (where appropriate):
    - Evacuation within a defined emergency planning zone.
    - Issuing potassium iodate tablets (for iodine-131 release)
    - Other prophylactic medication as may be appropriate
7. Advice to regional authorities (police, fire, health authorities, etc).
8. Receipt of casualties (who may be contaminated).
9. Communications to the media.

Gasmasks or BA sets should be available to site personnel as required to permit ordered evacuation. There should be regular realistic exercises, which include regional authorities, to ensure personnel are familiar with the arrangements. There will be a well-equipped off-site emergency centre to deal with non-plant related aspects, such as media communications and the interface with the civil authorities.

Offshore Oil Platforms

Basic objectives of Emergency Plan:

1. Muster and headcount to identify any missing persons.
2. Recovery and treatment of injured personnel.
3. Evacuation of non-essential platform staff.
4. Termination or mitigation of the incident.
5. Monitoring for oil releases.
6. Coordinate oil clean-up operations.
7. Advice to regional authorities (police, fire, health authorities, coastguard, etc).
8. Receipt of casualties.

9. Communications to the media.
10. Ensuring appropriate isolations to pipeline network.

There are three means of personnel evacuation:

1. If possible, and if time permits, the preferred evacuation method is by helicopter.
2. Lifeboats (TEMPSCs) are used if helicopters cannot be made available, either due to urgency or adverse weather.
3. Direct escape to sea, e.g. using rope ladders or jumping. (*This is a last resort*.)

There should be at least two possible escape routes to the muster stations from any point on the platform. There should be sufficient immersion suits and smoke hoods or BA sets at muster stations. There should be regular emergency drills to test all aspects of the Emergency Plan. All personnel should receive basic emergency training which should include time in a TEMPSC lifeboat.

There will be a well-equipped shore-based emergency centre to deal with media communications and the interface with the civil authorities.