Health and Safety Executive

This version of the SAPs has been superseded by the 2014 version.
Please see www.onr.org.uk/saps

Safety Assessment Principles for Nuclear Facilities

2006 Edition

Redgrave Court
Bootle
Merseyside
L20 7HS

Throughout the document individual paragraphs are numbered, but for clarity of presentation principles are presented in boxes and separately numbered. The numbering of principles is of the form XY.1 or XYZ.1 etc, where XY and XYZ represent the thematic headings above.

FOREWORD

Her Majesty's Nuclear Installations Inspectorate (NII) is that part of the Health and Safety Executive (HSE) with responsibility for regulating the safety of nuclear installations in Great Britain. Its inspectors use these Safety Assessment Principles (SAPs), together with the supporting Technical Assessment Guides (TAGs), to guide regulatory decision making in the nuclear permissioning process. Underpinning such decisions is the legal requirement on nuclear site licensees to reduce risks so far as is reasonably practicable, and the use of these SAPs should be seen in that context.

The principles were first published in 1979 for nuclear power reactors. Corresponding principles for nuclear chemical plants followed in 1983. The principles were amended in 1988, following a recommendation by Sir Frank Layfield arising from the Sizewell B inquiry. He also recommended that the Health and Safety Executive (HSE) should publish for discussion its thinking on risk assessment. The HSE paper *The tolerability of risk from nuclear power stations* (1988, revised in 1992) emerged in response. It provides background on levels of risks that may be tolerable by comparing them with other risks that society chooses to bear in return for certain benefits.

In 1992 the SAPs underwent a thorough revision with the objectives of:

a) consolidating the revisions made as a result of the recommendations of the Sizewell B inquiry;

b) implementing lessons learned since first publication;

c) ensuring greater consistency with international criteria (International Atomic Energy Agency (IAEA) Safety Standards, Codes and Guides);

d) implementing suggestions made in HSE's *The tolerability of risk from nuclear power stations* (TOR) paper (1988) and also in its 1992 revision; and

e) combining nuclear power reactor and nuclear chemical plant principles.

Since that review, experience in their use and developments in the field of nuclear safety, both internationally and in the UK, have led to the need to undertake a further thorough revision of the principles.

On the international front, the International Atomic Energy Agency (IAEA) has restructured and has revised, or is revising, all of its safety standards. This has been occurring in parallel with greater European recognition that IAEA standards are an appropriate high standard to benchmark against. IAEA requirements are explicit in requiring a Regulatory Body to keep its principles, regulations and guidance under review from time to time, taking account of internationally endorsed standards and recommendations. We agree with this need for periodic review, and this new edition of the SAPs is the result of such a review and has included benchmarking against the IAEA standards, as they existed in 2004. The UK's goal-setting legal framework for health and safety does not apply IAEA requirements in a prescriptive manner, but they are reflected within the principles.

NII is a member of the Western European Nuclear Regulators' Association (WENRA), which is dedicated to ensuring that all European Union countries and candidate countries with civil nuclear power stations as well as Switzerland have harmonised high levels of nuclear safety. To this end, WENRA is developing reference levels that represent good practices for civil nuclear power plants and for radioactive waste management and decommissioning. Harmonisation requires there to be no substantial differences from the safety point of view in generic, formally issued, national safety goals, and in their resulting implementation on nuclear power station licensed sites. In the UK, the reference levels will be secured using a combination of: national laws; health and safety regulations; conditions attached to nuclear site licences; and the SAPs, TAGs and other forms of guidance used when granting nuclear site licences and in regulating licensees' activities.

On the domestic front the scope of our work now includes a wider range of Ministry of Defence (MOD) related sites. The Defence Nuclear Safety Regulator (DNSR) and the Environment Agency (EA) have worked closely in the preparation of this revision of the SAPs. This will assist DNSR's proposed adoption of the principles for its assessment of defence nuclear activities. It will also assist the EA in their development of their own guidance.

In addition, a significant proportion of assessment work is directed towards the periodic safety review (PSR) of older facilities, decommissioning and radioactive waste management. The 1992 SAPs, with their focus on design, were not readily suited to these applications and complementary guidance had to be created. This new revision of the SAPs, while remaining applicable to new nuclear facilities, makes greater provision for decommissioning and radioactive waste management, and is also clearer in its application to safety cases related to existing facilities.

In 2001 HSE built upon its work on *The tolerability of risks from nuclear power stations* (TOR) with its publication *Reducing risk, protecting people: HSE's decision making process* (known as R2P2). This further

explains HSE's decision making process, and has been supported by guidance on the principle that risks should be As Low as Reasonably Practicable (ALARP). There were, however, aspects of societal concerns specific to the nuclear context that R2P2 did not tackle and HSE has further developed its thinking in this area.

Since the last edition of the SAPs in 1992, we have been developing assessment guidance for NII inspectors in our TAGs, which give further interpretation of the principles and guidance in their application. These have been written to help interpret the 1992 SAPs and in some cases have addressed gaps in them. This current edition of the SAPs covers these gaps, and the TAGs will be subject to review in the light of the revised principles. The SAPs and the TAGs will become a more integrated suite of guidance.

In summary, therefore, this edition of the SAPs has been:

a) benchmarked against the IAEA Safety Standards, as they existed in 2004, that represent good practice;

b) expanded to address emergency arrangements, remediation and decommissioning;

c) reviewed for application to defence nuclear activities covered by DNSR;

d) clarified for the assessment of safety cases, and now includes safety management systems;

e) updated to be consistent with HSE's thinking on societal risk.

In reviewing and revising these principles we have taken into account the technical interests and views of others through inviting comment on specific technical topic areas, and wider issues. However, the final decision on the content has been ours.

Dr M W Weightman
HM Chief Inspector

INTRODUCTION

The purpose of the Safety Assessment Principles (SAPs)

1 The SAPs apply to the assessment of safety cases for nuclear facilities that may be operated by potential licensees, existing licensees, or other dutyholders. The term 'safety case' is used throughout this document to encompass the totality of a licensee's (or dutyholder's) documentation to demonstrate high standards of nuclear safety and radioactive waste management, and any sub-set of this documentation that is submitted to Her Majesty's Nuclear Installations Inspectorate (NII).

2 The principles presented in this document relate only to nuclear safety and radioactive waste management. Other conventional hazards are excluded, except where they have a direct effect on nuclear safety or radioactive waste management. The use of the word 'safety' within the document should therefore be interpreted accordingly.

3 The SAPs provide inspectors with a framework for making consistent regulatory judgements on nuclear safety cases. The principles are supported by Technical Assessment Guides (TAGs), and other guidance, to further assist decision making by the nuclear safety regulatory process (see the HSE website). The SAPs also provide nuclear site dutyholders with information on the regulatory principles against which their safety provisions will be judged. However, they are not intended or sufficient to be used as design or operational standards, reflecting the non-prescriptive nature of the UK's nuclear regulatory system. In most cases the SAPs are guidance to inspectors, but where guidance refers to legal requirements they can be mandatory depending on the circumstances.

Regulatory background

4 Sections of the Nuclear Installations Act 1965 (as amended) (NIA) relating to the licensing and inspection of nuclear installations are relevant statutory provisions of the Health and Safety at Work etc Act 1974 (the HSW Act). In particular, section 1 of NIA, together with regulations made under the powers provided by section 1, prescribe the types of activity that may only be undertaken on a licensed site. Under this Act, apart from certain exceptions, no site may be used for the purpose of installing or operating any nuclear installation unless HSE has granted a licence. Additionally, section 4 of NIA enables HSE to attach conditions to a licence in the interests of safety or with respect to the handling, treatment and disposal of nuclear matter.

5 The Health and Safety Commission (HSC) is responsible for overseeing health and safety regulation in Great Britain. The Health and Safety Executive (HSE) is the enforcing authority who works in support of the Commission and NII is that part of HSE's Nuclear Safety Directorate (NSD) responsible for regulating the safety of nuclear installations in Great Britain. This includes granting nuclear site licences, attaching appropriate conditions to the licences, granting permissions, exercising other controls, and making judgements on the acceptability of responses made by licensees to the requirements of those conditions.

6 Installations currently in operation on nuclear licenced sites include; nuclear power stations; research reactors; nuclear fuel manufacturing; uranium enrichment and isotope production facilities; nuclear fuel stores; nuclear fuel reprocessing facilities; sites for building, maintaining and refuelling nuclear submarines*; sites for building, maintaining and dismantling nuclear devices; radioactive waste stores; and sites for both the storage and disposal of radioactive waste.

7 NIA is not the only legal requirement on the nuclear sites. In addition to the general provisions of the HSW Act, radiation protection is regulated against the Ionising Radiation Regulations 1999 (IRR). Emergency preparedness and associated radiation protection are regulated against the Radiation (Emergency Preparedness and Public Information) Regulations 2001 (REPPIR). Other relevant legislation is contained in the Management of Health and Safety at Work Regulations 1999 (the Management Regulations), that require, among other things, a suitable and sufficient risk assessment, and in the other regulations made under the HSW Act, eg Nuclear Reactors (Environmental Impact Assessment for Decommissioning) (Amendment) Regulations 2006 (EIADR); Provision and Use of Work Equipment Regulations; Lifting Operations and Lifting Equipment Regulations; Personal Protective Equipment at Work Regulations; Pressure Systems Safety Regulations; Control of Major Accident Hazards Regulations (as amended) and Dangerous Substances and Explosive Atmospheres Regulations. The latter requires a risk assessment for any substance identified in the Chemicals (Hazard Information and Packaging for Supply) Regulations. Nuclear operators must comply with these regulations in the same way as any other employer, and

* While NII regulates the activities on these sites under NIA its does not regulate the design of either the submarine reactor nor the design of the nuclear device.

the codes of practice associated with these regulations will often contain relevant good practice that can be used in safety cases when demonstrating what is reasonably practicable.

8 Not all relevant legislation is covered by the HSW Act. Other examples include the Anti-Terrorism, Crime and Security Act 2001 and its subordinate Nuclear Industry Security Regulations 2003, the Electricity Act 1989, the Environmental Protection Act 1990, the Radioactive Substances Act 1993, various planning acts and the Building Act 1984 and its subordinate Building Regulations.

SFAIRP, ALARP and ALARA

9 The SAPs are consistent with *Reducing risks protecting people: HSE's decision making process* (R2P2)[1], which provides an overall framework for decision making to aid consistency and coherence across the full range of risks falling within the scope of the HSW Act. This extended the framework in *The tolerability of risks from nuclear power stations* (TOR)[2]. R2P2[1] discusses the meaning of risk and hazard and explains the distinction HSE makes between the terms. Hazard is the potential for harm from an intrinsic property or disposition of something that can cause detriment, and risk is the chance that someone or something is adversely affected in a particular manner by the hazard. The SAPs use these definitions. HSE regards anything that presents the possibility of danger as a 'hazard'. The relative importance of likelihood and consequence in determining control measures may vary. In some circumstances, particularly where the consequences are very serious or knowledge of the likelihood is very uncertain, HSE may choose to concentrate solely on the consequences, that is, concerned only with the hazard.

10 R2P2[1] describes risks that are unacceptably high and the associated activities would be ruled out unless there are exceptional reasons, and risks that are so low that they may be considered broadly acceptable and no further regulatory pressure to reduce risks further need be applied. However, the legal duty to reduce risk so far as is reasonably practicable (SFAIRP) applies at all levels of risk and extends below the broadly acceptable level. Both R2P2[1] and TOR[2] set out indicative numerical risk levels, but the requirement to meet relevant good practice in engineering and operational safety management is of prime importance.

11 In applying the TOR[2] framework the term 'as low as reasonably practicable' (ALARP) has been introduced: for assessment purposes the terms ALARP and SFAIRP are interchangeable and require the same tests to be applied. ALARP is also equivalent to the phrase 'as low as reasonably achievable' (ALARA) used by other bodies nationally and internationally.

12 The SAPs assist inspectors in the judgement of whether, in their opinion, the dutyholder's safety case has satisfactorily demonstrated that the requirements of the law have been met. The guidance associated with each principle gives further interpretation on their application.

13 The basis for demonstrably adequate safety is that the normal requirements of good practice in engineering, operation and safety management are met. This is a fundamental requirement for safety cases. In addition, this is expected to be supported by a demonstration of how risk assessments have been used to identify any weaknesses in the proposed facility design and operation, showing where improvements were considered and to demonstrate that safety is not unduly reliant on a small set of particular safety features. A number of numerical targets are included in the SAPs and some of these embody specific statutory limits that must be met.

14 The principles are used in judging whether ALARP is achieved and that is why they are written using should or similar language. Priority should be given to achieving an overall balance of safety rather than satisfying each principle or making an ALARP judgement against each principle. The principles themselves should be applied in a reasonably practicable manner. The judgement using the principles in the SAPs is always subject to consideration of ALARP. This has not been stated in each case to avoid repetition. NII's inspectors need to apply judgement on the adequacy of a safety case in accordance with HSE guidance on ALARP (see www.hse.gov.uk/risk/theory/alarp.htm on the HSE website).

15 In many instances it will be possible to demonstrate that the magnitude of the radiological hazard will result in doses that will be low, in relation to the legal limits, so that considerations of off-site effects or detailed worker risks will be unnecessary.

16 The development of standards defining relevant good practice often includes ALARP considerations, so in many cases meeting these standards is sufficient to demonstrate that the legal requirement has been satisfied. In other cases, for example where standards and relevant good practice are less evident or not fully applicable or the demonstration of safety is complex, the onus is on the dutyholder to implement measures to the point where it can demonstrate to NII's inspectors that the

costs of any further measures would be grossly disproportionate to the risks their adoption would reduce.

17 The application of ALARP should be carried out comprehensively and balance the risks. This requires all applicable principles to be considered as a combined set. When judging whether risks have been reduced ALARP, it may be necessary to take account of conventional risks in addition to nuclear risks.

Permissioning

18 Regulatory regimes requiring safety submissions and/or a licence are referred to as 'permissioning regimes', and HSC's approach to such regimes is set out in its permissioning policy statement *Our approach to permissioning regimes*, published in 2003 (see the HSE website). Permissioning submissions arise under NIA licence conditions and other regulations such as IRR or REPPIR.

Interface with other regulatory bodies

19 Depending on the nature of the safety case being assessed, there may be other regulatory duties and processes that need to be taken into account when recommending a permissioning or enforcement action. These interactions are covered by relevant joint statements. The regulatory bodies whose processes NII most frequently interface with are:

a) The Environment Agency (EA) and the Scottish Environment Protection Agency (SEPA) (under Memoranda of Understanding);

b) The Office of Civil Nuclear Security (OCNS) on matters of civil nuclear security (under a Memorandum of Understanding); and

c) The Defence Nuclear Safety Regulator (DNSR) (under the MOD/HSE Agreement and relevant Letters of Understanding on defence nuclear matters).

20 Annex 1 gives further details on the regulatory interfaces between NII and other regulatory bodies.

International framework

21 The UK is a member state of the International Atomic Energy Agency (IAEA) and contributes to the development of safety standards that the IAEA publishes. The UK respects these Safety Standards and ensures that its own regulations and regulatory requirements are consistent with the expectations of the IAEA. NII leads on behalf of the UK Government in assisting the IAEA in developing their standards. In addition, NII assists the Government on other matters arising from the review meetings of the Convention on Nuclear Safety and the Joint Convention on the Safety of Spent Fuel Management and on the Safety of Radioactive Waste Management. Other areas where NII is active in the promotion of improvements to nuclear safety include participation in the Western Nuclear Regulators Association (WENRA), the International Nuclear Regulators Association and the Organisation for Economic Cooperation and Development's Nuclear Energy Agency.

Application of the SAPs

General

22 The SAPs contain principles and guidance. The principles form the underlying basis for regulatory judgements made by inspectors, and the guidance associated with the principles provides either further explanation of a principle, or their interpretation in actual applications and the measures against which judgements can be made.

23 Not all of the principles in this document apply to all assessments or every facility; clearly, principles specific to reactors do not apply to fuel-cycle facilities. Less obviously, not all of the reactor principles apply to all reactors: research reactors have significant differences from power reactors. Additionally, the assessment of a modification to a facility will only require the relevant principles to be applied. In short, the principles are a reference set from which the inspector needs to choose those to be used for the particular nuclear safety situation.

24 These SAPs will be used to assess safety cases associated with defence-related nuclear and radiological activities that fall within NII's responsibilities. In some cases nuclear and radiological safety legislation does not apply to defence-related nuclear activities, or exemptions may apply. An

annex to the MOD/HSE agreement recognises that these SAPs may not apply to the design of a naval reactor plant or a nuclear device*. The extent of application of these principles to safety cases associated with defence-related activities will be judged on a basis consistent with the ALARP principle, taking due cognisance of the unique operating purpose and that NII regulation only applies to discrete periods of their operating life-cycles.

Proportionality

25 The Management Regulations and its Approved Code of Practice[3] (ACoP) define three levels of risk assessment: low, intermediate and high. Nuclear installations are in the high category, which should use 'the most developed and sophisticated techniques'. However, there are a wide range of hazards associated with different facilities and activities on nuclear licensed sites. So, within the high category of assessment, the depth and rigour of the analysis required for nuclear facilities will vary considerably. This is consistent with HSC's Enforcement Policy Statement (see the HSE website) that the requirements of safety should be applied in a manner that is commensurate with the magnitude of the hazard. Therefore, the extent and detail of assessments undertaken by dutyholders as part of a safety case, including their independent assessment and verification, need to be commensurate with the magnitude of the hazards. Similarly, subject to other legal duties or public policy requirements, regulatory attention should also be commensurate with the magnitude of the hazard, although issues such as novelty and uncertainty will also be factors.

26 Safety cases, and the analyses and assessments contained within them, must be fit for purpose and in accordance with the nuclear site licence condition requirements and with regulation 3 of the Management Regulations. They must, among other things, be suitable and sufficient for the purpose of identifying all measures to control the risk.

27 Inspectors must be proportionate in what they require from dutyholders. The higher the hazard the more rigorous and comprehensive the analysis, which would be expected to lead to greater defence in depth to protect people. Therefore a low hazard facility may need a much more limited analysis to ensure adequacy. This might be expected to result in fewer or less extensive safety provisions.

28 In some cases, the magnitude of the potential radiological hazard may be uncertain. In these cases a precautionary approach should be applied (R2P2[1]) by erring on the side of safety. Where the absence of a radiological hazard cannot be shown, an assumption must be made of an appropriate radiological hazard and its magnitude.

Life-cycle

29 The SAPs are for regulatory assessment throughout the life-cycle of an activity on a nuclear licenced site. Specific sections of the SAPs are devoted to siting and decommissioning. However, not every principle in the other sections will apply to all the other life-cycle stages and as always the principles are a reference set from which the inspector chooses those to be used for the particular stage in the life-cycle. The sections of the SAPs on Leadership and management for safety *(paragraph 43 ff.)* and the Regulatory assessment of safety cases *(paragraph 70 ff.)* include life-cycle issues. The Engineering principles *(paragraph 131 ff.)* are relevant to design, construction, manufacture and installation, but will also apply to later operational stages. Commissioning is a key stage in providing the necessary assurance of safety and a number of the principles include aspects of commissioning. Decommissioning also needs to be considered at all life-cycle stages. IAEA Safety Standard NS-G-1.2[4] provides more detailed guidance for the assessment aspects to be considered at the main life-cycle stages.

New facilities

30 One of the aims of the SAPs is the safety assessment of new (proposed) nuclear facilities. They represent NII's view of good practice and NII would expect modern facilities to have no difficulty in satisfying their overall intent.

Facilities built to earlier standards

31 Inspectors will assess safety cases against the relevant SAPs when judging if a dutyholder has demonstrated whether risks have been controlled to be ALARP. The extent to which the principles

* In accordance with the AWE Act 1991 and Amendment Order 1997, the conditions attached to a licence under the NIA do not apply in as far as they affect the design of a nuclear device.

have been satisfied must also take into account the age of the facility or plant. For facilities that were designed and constructed to standards that are different from current standards the issue of whether sufficient measures are available to satisfy ALARP considerations will be judged case by case.

32 A common situation when the SAPs are applied to facilities built to earlier standards is in the assessment of a Periodic Safety Review (PSR) as required by Licence Condition 15 (see the HSE website). PSRs are a thorough and comprehensive review of the safety case at regular intervals throughout a nuclear facility's life. The reviews are more wide ranging than a restatement of the safety case (see IAEA Safety Standard NS-G-1.2[4] and NS-G-2.10[5]).

33 For certain activities, such as decommissioning, it is recognised that some principles may not be met transiently and this is allowable provided the result is to achieve a safer end-state. However, during this period, the requirement to reduce risks ALARP remains.

Ageing

34 As a facility ages, plant safety margins may be eroded and a dutyholder may argue that it is not worthwhile to make improvements. Remaining lifetime may be invoked in making the ALARP demonstration, but this factor should not be used to make a case for a facility to operate outside legal requirements. A minimum period of ten years, or the minimum future life of the facility if longer, should be used in ALARP demonstrations. Remaining lifetimes of less than ten years will be subject to regulatory action to ensure that the declared lifetime is not extended beyond that assumed without further justification.

Multi-facility sites

35 When considering the radiological hazards and risks posed by a nuclear site, all the facilities, services and activities on it need to be considered. In most cases, the SAPs are considered in relation to single facilities and so the control of risks is also generally considered on a facility basis. However, there is a need to consider the totality of control of risks from a site (see R2P2[1] paragraph 136). Two different situations arise: where all the facilities and services are under the control of a single licensee, covered by a single nuclear site licence, and where some of the facilities and services are on neighbouring sites, under the control of different dutyholders. Many of the issues are similar.

36 Sites that have multiple facilities often produce a set of individual safety cases for each facility. Shared services are also generally dealt with by separate cases. The division of the site in this way requires the definition of boundaries and interfaces between facilities, facilities and services, and services. It also requires an appropriate combination of the individual analyses to develop the site safety case. This is necessary to account for the interactions and interdependencies between facilities and services.

37 Determining whether risks have been controlled and reduced ALARP therefore requires an overall consideration of the site and, in determining if good practices have been met, all risks need to be assessed. On a complex site there will be many different radiological hazards and risks that, in determining the necessary safety measures for the site, may need to be balanced in demonstrating that the overall risks are ALARP.

Alternative approaches

38 The principles are written bearing in mind the content of safety cases likely to be submitted to the NII. However, dutyholders may wish to put forward a safety case that differs from this expectation and, as in the past, the inspector will consider such an approach. In these cases the dutyholder is advised to discuss the method of demonstration with NII beforehand. Such cases will need to demonstrate equivalence to the outcomes associated with the use of the principles here, and such a demonstration may need to be examined in greater depth to gain such an assurance. An example of such a situation is the greater use of passive safe concepts.

Structure of the principles

39 The principles are structured in separate sections, as follows.

- Fundamental principles. These principles are founded in UK health and safety law and international good practice, and underpin all those activities that contribute to sustained high standards of nuclear safety.
- Leadership and management for safety. This section sets out principles that form the foundation for the leadership and management for safety in the nuclear environment.
- The regulatory assessment of safety cases. This section sets out the principles applicable to the assessment of the production and nature of safety cases.
- The regulatory assessment of siting. This section provides principles applied in the assessment of a site, since the nature of a site can have a bearing on accident consequences.
- Engineering principles. This section comprises the major part of this document and covers many aspects of the design and operation of nuclear facilities.
- Radiation protection. This section provides a link with the IRR.
- Fault analysis.
- Numerical targets and legal limits. This section sets out the targets to assist in making ALARP judgements.
- Accident management and emergency preparedness. This section provides the links to assessing compliance with licence conditions and REPPIR.
- Radioactive waste management.
- Decommissioning.
- Control and remediation of radioactively contaminated land.

40 The glossary at the end of the document is provided to assist understanding of the particular usage of certain terms in the principles. It includes the sources of the definitions presented, where relevant.

FUNDAMENTAL PRINCIPLES

41 The following fundamental principles are considered to be the foundation for the subsequent safety and radioactive waste principles in this document and are based in UK law and international good practice.

42 The IAEA standards also have fundamental principles[6], but these cover a wider scope than regulatory assessment. IAEA fundamental principles relevant to regulatory assessment have informed the choice of fundamental principles set out below[*].

Fundamental principles	Responsibility for safety	FP.1
The prime responsibility for safety must rest with the person or organisation responsible for the facilities and activities that give rise to radiation risks.		

Fundamental principles	Leadership and management for safety	FP.2
Effective leadership and management for safety must be established and sustained in organisations concerned with, and facilities and activities that give rise to, radiation risks.		

Fundamental principles	Optimisation of protection	FP.3
Protection must be optimized to provide the highest level of safety that is reasonably practicable.		

Fundamental principles	Safety assessment	FP.4
The dutyholder must demonstrate effective understanding of the hazards and their control for a nuclear site or facility through a comprehensive and systematic process of safety assessment.		

Fundamental principles	Limitation of risks to individuals	FP.5
Measures for controlling radiation risks must ensure that no individual bears an unacceptable risk of harm.		

Fundamental principles	Prevention of accidents	FP.6
All reasonably practicable steps must be taken to prevent and mitigate nuclear or radiation accidents.		

Fundamental principles	Emergency preparedness and response	FP.7
Arrangements must be made for emergency preparedness and response in case of nuclear or radiation incidents.		

Fundamental principles	Protection of present and future generations	FP.8
People, present and future, must be protected against radiation risks.		

[*] The IAEA fundamental principles were adopted by the IAEA board in September 2006. Of the ten IAEA fundamental principles, the three which are not covered above relate to the role of Government, justification of facilities and activities, and radiation risks in situations outside the NIA which are addressed by the UK under its regulatory framework. The SAPs also have a fundamental principle on safety assessment, rather than considering this as a subset of preventing accidents.

LEADERSHIP AND MANAGEMENT FOR SAFETY

43 *The principles in this section set the foundation for the effective delivery of nuclear safety, including the development and maintenance of a positive safety culture. Inspectors should use the principles proportionately, reflecting the radiological hazards, the scale and complexity of the dutyholder's undertaking, part of which is to judge the dutyholder's approach to leadership and management for safety.*

44 *There are four high-level interrelated principles: leadership, capable organisation, decision making and learning. These set the outcomes to be achieved for effective leadership and management for safety rather than describing the systems, processes and procedures for achieving safety. Because of their inter-connected nature there is some overlap between them. The principles should be considered as a whole and an integrated approach will be necessary for their delivery.*

45 *The principles apply to the application of all law relevant to the nuclear industry. This includes those licence conditions that require 'adequate arrangements', where the need for policies, systems and procedures can be envisaged together with the need to set roles, responsibilities, competence levels and monitoring arrangements. They also apply to other submissions made as part of the nuclear permissioning regime, eg the assessment of a safety management prospectus, as required by a new licence applicant (see* The regulation of nuclear safety in the United Kingdom *on the HSE website).*

46 *The principles combine the key features of effective safety management arising from current national law and guidance; in particular the requirements of nuclear site licence conditions, the HSW Act, the Management Regulations and* Successful health and safety management HSG65 (Second edition)[7]. *They also draw on international guidance, good safety management practice, the lessons learned from serious incident investigations such as those contained in the Columbia Accident Investigation Report[8], and the work of researchers who have examined the operation of high reliability organisations.*

47 *In combining the key features of leadership and management for safety from a range of sources, the principles reflect:*

a) the emphasis HSE's strategy gives to leadership and management for safety, the role of directors and worker involvement;

b) the necessary emphasis on leadership and managing people and processes as well as on engineering; and

c) the need to consider the management of safety throughout the whole organisation in building and sustaining a positive safety culture.

Leadership and management for safety	**Leadership**	**MS.1**
Directors, managers and leaders at all levels should focus the organisation on achieving and sustaining high standards of safety and on delivering the characteristics of a high reliability organisation.		

48 Leadership is key to achieving appropriate, high levels of safety and establishing and sustaining a positive safety culture. In meeting Principle MS.1 the expectation is that the behaviour and activities of directors, managers and leaders at all levels should include:

a) establishing the safety strategies, policies, plans, goals and standards for safety and ensuring that they are delivered throughout the organisation;

b) providing direction and oversight to create a climate that establishes a strong safety culture that underpins safe operation;

c) visibly demonstrating commitment to safety through their activities;

d) recognising and resolving conflict between safety and other goals; and

e) ensuring that any reward systems promote the control of risk and accident prevention, recognise safe behaviour and challenge unsafe behaviour.

49 The value of safety as an integral part of good business and management practice should be reinforced through interactions between directors, managers, leaders and staff, including contractors, to establish a common purpose and collective social responsibility. Consultation and involvement of all staff secures effective engagement and co-operation in the development, maintenance and improvement of safety and promotes a shared concern for achieving safety goals. As a result, people at all levels in the organisation should be engaged in a common purpose that

recognises collective responsibility and accountability to each other and external stakeholders to ensure high standards of safety.

50 Oversight of safety performance, led by the management board, should provide assurance at all levels, and throughout all stages of the life of the undertaking, that safety is being maintained and improved. It should secure the adequate, proportionate monitoring and auditing of the implementation and effectiveness of the safety policies, strategies, plans, goals and standards, systems and procedures through the application of a 'quality management system' (QMS).

51 The QMS should be based on national and international standards or other defined documents and should be reviewed periodically. Consideration should be given to the adoption of a single company wide management system ensuring that the principle of continuous improvement is maintained.

Leadership and management for safety	**Capable organisation**	**MS.2**
The organisation should have the capability to secure and maintain the safety of its undertakings.		

52 An organisation needs adequate human resources, which means having the necessary competences and knowledge in such numbers so as to maintain the capability to manage safety reliably at all times, including during steady state conditions, periods of change and emergency situations.

53 The organisation structure and baseline staffing levels should be based on appropriate organisational design principles. Human resources baseline provisions should be established, controlled and regularly reviewed through robust, auditable processes. Changes to the organisation (eg structure, staffing, resources, competences), need systematic evaluation to ensure that they do not adversely affect nuclear safety management capabilities. This should include succession planning (especially where there is limited or singleton expertise). Succession planning should take into account expected changes (eg retirements) along with contingencies for the unexpected (eg resignations).

54 The organisational structure, roles and responsibilities should secure effective co-ordination and collaboration between all those involved, including contractors. Roles, responsibilities, accountabilities and performance standards for safety at all levels should be clear and avoid conflict with other business roles, responsibilities, accountabilities and objectives. All those with responsibilities for safety should have authority and access to resources to discharge those responsibilities effectively. This should ensure that proportionate control and supervision of safety at all levels is achieved. The design of jobs, processes, and procedures should take account of those factors that affect reliable performance of the organisation.

55 Processes and systems should secure and assure maintenance of the appropriate technical and behavioural competence of directors, managers and leaders and all other staff relevant to their safety roles and responsibilities.

56 An 'intelligent customer' capability should be maintained to ensure that the use of contractors in any part of the business does not adversely affect the ability to manage safety. A capable organisation requires the retention and use of knowledge to understand nuclear safety requirements and to control safety risks throughout all activities, including those undertaken by contractors.

57 Expertise and processes should be deployed to understand the intended and unintended behaviour of the technology and interpret information accurately and appropriately. The potential for multiple and complex interactions between the technical and human systems to create adverse consequences should be recognised. The processes should capture information from all relevant sources and recognise that early signs of failure may be unclear and ambiguous without adequate assessment of the safety potential. Collecting available knowledge about a situation is recognised as an essential basis for accurate diagnosis of fault conditions and the generation of options for effective decision making.

58 Knowledge of the intended design performance of plant, equipment, processes and systems should be maintained to provide an adequate corporate memory and baseline for monitoring. This includes the need for an effective process to transfer knowledge from experienced staff, leaving the organisation to the remaining or replacement staff.

59 Knowledge should be captured and communicated within the organisation in a systematic, appropriate and reliable manner to all those who need to make safety-related decisions. Multiple

and diverse information sources should be used to provide sufficient redundancy in communication networks so that key information is provided to inform decisions. Support documentation should provide more detailed information concerning management, organisation and responsibilities, along with the administrative and technical procedures and instructions.

60 There should be provision for identifying, updating and preserving documents and records relevant to safety. Documents and records should be stored securely and should be retrievable and readable throughout their anticipated useful life (including statutory retention periods). Particular attention should be paid to documents and records that:

a) will be of value throughout the whole life of a nuclear facility;
b) would assist management in the event of incidents;
c) are relevant to making modifications and decommissioning; and
d) would contribute to improvements in plant.

Leadership and management for safety	**Decision making**	**MS.3**
Decisions at all levels that affect safety should be rational, objective, transparent and prudent.		

61 Decision making processes should ensure that safety is given a high priority and this should be evident in all decision making. The processes should also ensure that available data and opinions are collected and considered, respecting and encouraging the contribution of those with divergent views. The processes should encompass means for setting safety priorities to aid decision making at all levels.

62 Factors that should be considered in decisions affecting safety should include:

a) consideration of the quality of the information;
b) the questioning of assumptions;
c) exploration of all relevant scenarios that may threaten safety;
d) consideration of health, safety, environmental, security, overall quality and economic requirements; and
e) relative priorities of the range of options to minimise overall risk both in the long and short term.

63 Decision making should be based on processes that ensure that conflict between safety and other business goals, including commercial and schedule pressures and external influences, are recognised and resolved.

64 Decisions at all levels affecting safety should also allow for error, uncertainty and the unexpected, and those taken in the face of uncertainty or the unexpected should be appropriately and demonstrably conservative.

65 Active challenge should be part of decision making throughout the organisation. This may have different forms and functions in different areas, but all aspects of challenge should be part of an integrated process for the whole organisation, including the most senior levels of management. This should ensure that active challenge:

a) occurs by design in all key decision making and for processes that may affect safety;
b) does not originate solely from independent nuclear safety assessment or peer review;
c) has a preoccupation with failure and actively looks for ways that things could go wrong;
d) applies to technical/plant-based and management decisions; and
e) applies to normal and crisis situations.

Leadership and management for safety	**Learning from experience**	**MS.4**
Lessons should be learned from internal and external sources to continually improve leadership, organisational capability, safety decision making and safety performance.		

66 An organisation should have effective processes for seeking out, analysing and acting upon lessons from a wide range of sources. A learning organisation should challenge established understanding and practice by reflecting on experiences to identify and understand the reasons for differences between actual and intended outcomes. An absence of major accidents and incidents alone does not indicate that safety risks are being adequately controlled and should not breed complacency. Near misses are opportunities to learn. Leading and lagging indicators should be used to monitor performance over time to track the effectiveness of the control of risks.

67 Learning should occur throughout the organisation and information should be collected from inside the organisation from a number of sources including:

a) workers (eg about strengths, weaknesses, deviations and errors in safety procedures and processes);
b) monitoring, review and audit of the implementation and effectiveness of safety strategies, policies, plans, goals, standards, processes and procedures;
c) monitoring of plant, systems and processes;
d) testing and validation of safety procedures under normal and emergency situations;
e) the inspection of sites, facilities, plant and equipment and other operational feedback systems;
f) the investigation of accidents and incidents specifically to ascertain immediate and underlying causes, including organisational, safety management and cultural factors;
g) self assessments; and
h) external assessments.

68 Learning opportunities from external sources and beyond the nuclear industry should be actively sought and used in learning processes. The information should be analysed to identify trends and issues, such as common cause failures (CCFs) or human factors, as a foundation for improvement. Sources outside the organisation should include:

a) reviews against international standards and practices;
b) lessons from the investigation of incidents in other organisations both within and outside the nuclear industry; and
c) benchmarking safety performance and safety management methods and processes with other organisations from both within and outside the nuclear industry.

69 The lessons derived from learning should be embedded through a structured system for implementing corrective actions that is rigorously applied and actively followed up to completion. Effectiveness reviews should be undertaken to confirm that the changes have delivered the desired improvements.

THE REGULATORY ASSESSMENT OF SAFETY CASES

70 *NII's assessment process consists of examining submissions from dutyholders to enable a judgement to be made that risks are ALARP and that appropriate attention has been paid to aspects important to safety and to radioactive waste management and decommissioning. NII's assessment covers both normal operation and fault conditions, including internal and external hazards and human errors, all of which have the potential for causing the exposure of workers or the public to significant unplanned doses of ionising radiation or releases of radioactivity. A submission assessed by NII might not cover a complete facility, for example, it may relate to a plant modification to part of a facility or to equipment within a facility.*

71 *Assessment involves the examination of documentation and arrangements that demonstrate the safety of a facility and its processes, operations and organisation. In addition, it also requires inspection of the facility to verify the accuracy of the safety case as a description of the facility, its assumptions, its safety provisions and requirements and compliance inspection with the procedures that ensure that the provisions and requirements have been implemented and continue to be adhered to. It is also important in establishing confidence in the reliability of the information and conclusions presented.*

72 *The primary purpose of a safety case (as required by Licence Condition 23, see the HSE website) is to provide the dutyholder with the information required to enable safe management of the facility or activity in question, and therefore it should be clearly owned by those with direct responsibility for safety.*

73 *NII uses a sampling approach in deploying its resources and not every safety case is assessed fully in every aspect. The extent of the sample depends on the hazards associated with the activities that are the subject of the safety case, a judgement of the dutyholder's competence in producing an adequate safety case, the confidence in the dutyholder's approach to leadership and management, and other relevant factors. Important factors in NII's permissioning decisions include:*

a) *the level of confidence NII has in the dutyholder's process for producing safety cases;*

b) *the level of confidence NII has in the dutyholder's approach to leadership and management for safety; and*

c) *the hazards associated with the activities covered by the safety case in question.*

74 *Important factors in NII's permissioning decisions include:*

a) *the extent to which the dutyholder has demonstrated that the safety objectives and regulatory requirements have been met;*

b) *the acceptability of the depth, completeness, accuracy and detail of the dutyholder's safety case, in relation to the nature of the facility and the magnitude of the risks it presents;*

c) *the extent to which the dutyholder has taken all reasonably practicable measures to remove, minimise or control the radiological hazards it has identified;*

d) *the dutyholder's state of knowledge concerning particular processes or effects (such as, but not exclusively, ageing); and*

e) *the confidence NII has in the conclusions reached by the dutyholder.*

75 *NII will use the findings from its assessment of the safety case to determine its inspection priorities.*

76 *The principles in this section cover how safety cases should be produced and managed, what they need to do and what they should contain. This section also expands on NII's philosophy of safety cases and explains what to look for in terms of good points and pitfalls if they are inappropriately applied or their limitations misunderstood. It sets out the links that inspectors should expect between safety cases, facility/plant, people and processes.*

77 *A safety case is a logical and hierarchical set of documents that describes the radiological hazards in terms of the facility, site and the modes of operation, including potential undesired modes, and those reasonably practicable measures that need to be implemented to prevent harm being incurred. It takes account of experience from the past, is written in the present, and sets expectations and guidance for the processes that should operate in the future if hazards are to be successfully controlled.*

78 *The documented safety case becomes the basis for risk management in the effect it has on the activities and behaviours of the people who interact with the facility. In this context there are two key 'users' of the safety case. Firstly, there are those who interact directly with the facility. These include the operators who control the conditions within the facility as well as those who maintain the*

condition of the facility. The second set is the company directors (and senior managers) who are accountable for the safety of their site and who rely on the safety case for accurate and objective information on control measures to make informed business decisions. Therefore the safety case and the identification of risk management options should be recognised as essential elements in the dutyholder's business processes. The safety case should not be used as a means of back-fitting an argument for design decisions or business decisions that have already been made.

79 *The production of a safety case does not in itself ensure the safety of a facility. The safety of a facility derives from a proper understanding of the safety case so that the technical requirements deriving from it can be properly implemented and the facility can be operated and maintained in a safe manner.*

Safety case processes

80 *The process of analysing safety requires creativity, where people can envisage the variety of routes by which potential radiological hazards can arise from the technology. A range of options can then be identified, from which the reasonably practicable ones can be selected and implemented. It requires an extensive understanding of the facility both in the present and in the foreseeable future, its behaviour in a variety of conditions, experience of failures in other facilities and the measures adopted to prevent their recurrence. It also requires an understanding of how people and organisations affect safety. It also requires an understanding of how people and organisations may affect safety. Imagination is required to identify potential failure modes arising in plant or people and opportunities for control and, if necessary, mitigation. Since all of this knowledge is unlikely to be found in a single individual, organisational effectiveness is required to enable the aggregation of the necessary expertise, both in developing the case and implementing its expectations. The inspector should look for evidence of these attributes.*

81 *Safety is achieved when the people and physical systems together reliably control the radiological hazards inherent in the technology. Therefore the organisational systems (ie interactions between people) are just as important as the physical systems, particularly bearing in mind that people, processes and organisations can have more failure modes than plant components. This starts with the system (process) for producing safety cases, which needs to be reliable and robust.*

The regulatory assessment of safety cases	Safety case process	SC.1
The process for producing safety cases should be designed and operated commensurate with the hazard, using concepts applied to high reliability engineered systems.		

82 Application of the concepts should result in:

a) a clear specification for the purpose, standards and expectations of each element in the safety case process;

b) defences or barriers being designed to militate against failure of the process;

c) monitoring and testing of the process being undertaken to ensure each element is functioning to the requisite specification and standards;

d) responsive feedback mechanisms to ensure that significant issues over the quality of individual safety cases are reviewed to check for underlying defects or weaknesses in the process; and

e) definition of training and qualification expectations for the formal roles within the process (to ensure that those who undertake the roles are suitably qualified and experienced).

83 The process used to produce safety cases needs to deliver consistently good quality, fit for purpose cases. In this context, 'to produce' encompasses all elements of the process including initial optioneering, writing the case, and any means of verification or review. For a safety case to claim that the facility under consideration is very reliable or highly unlikely to fail, the process used to derive such claims needs to have commensurate reliability.

84 The different elements of the whole safety case process should be defined clearly, including their purpose and key features, and their potential weaknesses or failure modes. The defences or barriers in response to the identified potential failures or weaknesses should be determined. To achieve the necessary high reliability in the process, consideration should be given to some form of diversity in the elements and their defences, not just redundancy. This should include safety case review by people who are independent of those involved in its production. The independent review

function (among others) should address defects in the safety case process, not just issues relating to the content of the safety case itself.

85 The design of the safety case production process and the means of monitoring and testing the adequacy of its defences or barriers to failure should utilise lessons from major failures and successes of safety management systems or safety case processes. In particular, specific measures should be in place to guard against known 'common cause failures' of the process (eg resource constraints, programme pressures, commercial drivers and incentive schemes) that can result in poor quality or incomplete safety cases and inadequate identification or management of the risks.

86 During times of high stress (eg tight deadlines, intense commercial or operational pressure), additional measures need to be considered to protect the quality of the safety case. The regular monitoring and testing of the safety case process should provide for such periods of increased stress and not be restricted to normal situations.

The regulatory assessment of safety cases	Safety case process	SC.2
The safety case process should produce safety cases that facilitate safe operation.		

87 The process for producing safety cases should take into account the needs of those who will use the safety case to ensure safe operations. It is essential that the safety case documentation is clear and logically structured so that the information is easily accessible to those who need to use it. This includes operations and maintenance staff, technical personnel and managers who are accountable for safety, and the regulator.

88 The safety case process should also take into account how the different levels and types of documentation fit together to cover the full scope and content of the safety case. The needs of users should be addressed by ensuring that all descriptions and terms are easy to understand by the prime audience, all arguments are cogent and coherently developed, all references are easily accessible, and that all conclusions are fully supported, and follow logically from the arguments. The trail from claims through argument to evidence should be clear.

Safety case characteristics

The regulatory assessment of safety cases	Safety case characteristics	SC.3
For each life-cycle stage, control of radiological hazards should be demonstrated by a valid safety case that takes into account the implications from previous stages and for future stages.		

89 Control of radiological hazards should be demonstrated in a safety case before any associated risks actually exist. The safety case for each stage should take account of other life-cycle stages, ie it should build on the safety case for previous stages and show that the safety intent for subsequent stages can be achieved. Any constraints that will apply in subsequent stages should be detailed in the safety case in which they are identified. The safety case for decommissioning should have been considered in all previous life-cycle stages to the extent necessary. In the case of early, unplanned permanent shutdown of a facility, the development of the outline safety case for decommissioning should be carried out as soon as is reasonably practicable, as required by Licence Condition 35 (see the HSE website).

90 The specific content and depth of information in a safety case will vary from stage to stage, and should be commensurate with the nature of a particular stage and interrelationships with other stages. For example, in the early stages (eg design concept) the safety case will be more a statement of future intent and principles, whereas a safety case for the operational stage will contain far more detail and analysis.

The regulatory assessment of safety cases	Safety case characteristics	SC.4
A safety case should be accurate, objective and demonstrably complete for its intended purpose.		

91 A safety case should:

a) link the information necessary to show that the facility is adequately safe, and what will be needed for it to remain so over the period for which the safety case is valid;

b) support arguments with appropriate evidence, and with experiment and/or analysis that validates performance assumptions;

c) accurately reflect the proposed activity and the reality of the facility and its systems;

d) explicitly set out the argument for how ALARP has been satisfied; and

e) identify surveillance, maintenance and inspection programmes to underpin operational assumptions in the case.

92 A safety case should contain:

a) identification of the hazards and the hazard potential by a thorough and systematic process;

b) identification of the failure modes of the plant or equipment by a thorough and systematic fault and fault sequence identification process;

c) a demonstration that the nuclear facility will or does conform to good nuclear engineering practice and sound safety principles. (A nuclear facility should be designed against a set of deterministic engineering rules, such as design codes and standards, using the concept of 'defence in depth' and with adequate safety margins);

d) sufficient information to demonstrate that the engineering rules have been applied in an appropriate manner. (In particular, it should be clearly demonstrated that all designated equipment important to safety has been designed, constructed, commissioned, operated, and maintained in such a way as to enable it to fulfil its safety function for its projected lifetime);

e) an analysis of normal operating conditions to show that resultant doses of ionising radiation, to both members of the workforce and the public are, and will continue to be, within regulatory limits and ALARP;

f) an analysis of possible faults using the complementary approaches of design basis and probabilistic analyses, and severe accident analysis as appropriate, demonstrating that control of hazards and residual risks are ALARP;

g) sufficient information to demonstrate that radioactive waste management and decommissioning have been addressed in an appropriate manner; and

h) the basis for the management for safety of people, plant and procedures by addressing management and staffing levels; training requirements; maintenance requirements; operating and maintenance instructions; rules and contingency and emergency instructions.

93 To demonstrate ALARP has been achieved for new facilities, modifications or periodic safety reviews, the safety case should:

a) identify and document all the options considered;

b) provide evidence of the criteria used in decision making or option selection; and

c) support comparison of costs and benefits where quantified claims of gross disproportion have been made.

The regulatory assessment of safety cases	Safety case characteristics	SC.5
Safety cases should identify areas of optimism and uncertainty, together with their significance, in addition to strengths and any claimed conservatism.		

94 The safety case should present a balanced view of the level of knowledge and understanding, and of the resultant risks. Otherwise, it can mislead those who need to use the safety case to take decisions on risks and on managing safety. An unbalanced case will also fail to identify areas where more work might be needed, either to support the current conclusions or to provide a valid basis for any subsequent work if the safety case needs to be revised (eg due to a proposed plant modification or a change to operating regime or procedures). This principle encompasses optimism and uncertainties in the design of a facility (eg material properties, defects, dynamic behaviour) and in the basis of the safety case (eg analytical methods and codes, underlying assumptions, data, margins and factors of safety). Areas of uncertainty need to be balanced with adequate conservatism.

95 To ensure that risks are understood and can be managed appropriately, potential weaknesses in the design or the safety case should be identified clearly (eg in the summary or main conclusions of the safety case). Mitigating measures that have been or can be applied to address the weaknesses should also be identified. It should also be made clear how any outstanding safety significant issues are being, or will be, addressed.

The regulatory assessment of safety cases	Safety case characteristics	SC.6
The safety case for a facility or site should identify the important aspects of operation and management required for maintaining safety.		

96 The important aspects of operation and management required to maintain safety should emerge from the safety case. All such aspects should be clearly set out and easy to understand and implement.

97 The safety case for each life-cycle stage should include:

a) the required maintenance, inspection and testing regimes that have been assumed for the case to remain valid;

b) the operating limits and conditions required to ensure that the facility is kept in a safe condition; and

c) inputs to emergency planning.

Safety case management

The regulatory assessment of safety cases	Safety case maintenance	SC.7
A safety case should be actively maintained throughout each of the life-cycle stages.		

98 A safety case should be:

a) described in a living suite of documents, easily accessible and understandable by those who need to use it;

b) managed through formal processes; and

c) reviewed regularly on a defined basis.

99 The safety case needs to be kept up to date. The knowledge used at the time of writing the safety case needs to be supplemented by monitoring of plant and data from commissioning and continued operation, periodic inspection and testing as well as longer-term research or experience from other facilities. Processes need to be in place to make legitimate changes that may be needed on an immediate or a longer-term basis. In practice this requires the incorporation of:

a) changes arising from modifications or operating methods;

b) changes arising from incidents, operating experience, examination or testing results, updated design, analysis methods, research findings or other new information;

c) the outcome from major periodic and interim safety reviews (Licence Condition 15, see the HSE website); and

d) changes arising from time-dependent degradation.

100 Safety case reviews of incidents, operating experience and other sources of information should not be restricted to the facility or site in question. They should include similar facilities or equipment and also a wider range of nuclear and non-nuclear experience, both national and international.

The regulatory assessment of safety cases	Safety case ownership	SC.8
Ownership of the safety case should reside within the dutyholder's organisation with those who have direct responsibility for safety.		

101 Ownership and responsibility require:

a) an understanding of the safety case, the standards applied in it, its assumptions and the limits and conditions derived from it;

b) the technical capability to understand and act upon the safety case work produced by others;

c) the ability to use the safety case to manage safety; and

d) that users of safety cases should be involved in their preparation to ensure that it reflects operational needs and reality.

102 The responsibility for ownership of a safety case may change within the dutyholder as the facility moves through its life-cycle or if the dutyholder changes. Management of transitions and changes of ownership from earlier to later stages of the life-cycle are important aspects that need to be controlled.

THE REGULATORY ASSESSMENT OF SITING

103 *Siting characteristics are relevant to various circumstances – new facilities or sites or modifications to them. The factors that should be considered in assessing sites cover three main aspects:*

a) the location and characteristics of the population around the site and the physical factors affecting the dispersion of released radioactivity that might have implications for the radiological risk to people;

b) external hazards that might preclude the use of the site for its intended purpose;

c) the suitability of the site for the engineering and infrastructure requirements of the facility.

104 *This section deals with the first aspect. The second aspect is covered in detail by SAPs on external hazards; and the third aspect is covered in SAPs on the engineering and operation of the facility.*

105 *The acceptability of a site is regulated by HSE with respect to the direct radiation shine from normal operation and for all doses from accidents. The environment agencies, in liaison with HSE, regulate discharges from normal operations. Protection against direct radiation shine is covered by the radiological protection principles, see paragraph 476 ff.*

106 *In assessing an application for the use of a site, NII takes account of the practicability of emergency responses to mitigate the health implications for humans of exposure to radiation through the inhalation of radioactivity, radiation shine from radioactivity in the atmosphere or deposited on the ground or structures, and inadvertent ingestion of contaminated dust or soil. Consideration of other routes of exposure such as contaminated foodstuffs or water, and effects on the non-human environment or economic activity, are undertaken using advice from these bodies. NII consults these other bodies before granting a licence for the use of the site, under NIA, as amended by the Environment Act 1995 Schedule 2 paragraph 7.*

107 *For an application to use a site for a new nuclear power station, and for subsequent land-use in the vicinity, UK Government policy at the time of writing includes the consideration of demographics to constrain the number of people who might be affected in the event of an emergency. Although siting is usually considered with respect to a new facility on a new site, any new facility, either on an existing site or in its vicinity, or any significant extension to such a facility, should be checked to ensure that its presence does not invalidate any of the arguments used in granting the licence. NII, as part of HSE, is a statutory consultee for any planning application in the vicinity of a nuclear licensed site.*

108 *Many of the principles and much of the guidance here are applicable before a site licence is granted.*

Siting	**Siting factors**	**ST.1**
Account should be taken of all relevant factors that might affect the protection of individuals and populations from radiological risk when assessing the siting of a new facility.		

109 The factors of interest here include: the demography around the site; the need for effective accident management and emergency preparedness; and certain external hazards associated with the site.

110 Any foreseeable variations in these factors during the expected life-cycle of the site should be identified and taken into account. The factors should be included in the periodic reviews of safety cases for the facility.

111 For new nuclear power stations, the criteria defined in Government policy should be used in assessment.

Siting	**Population characteristics**	**ST.2**
The safety case should demonstrate that the characteristics of the population off-site would allow for an effective off-site emergency response.		

112 Allowing for some natural growth in the size and distribution of the population around the site, it should be shown that:

a) it would be possible to invoke off-site countermeasures within an appropriate timescale consistent with the emergency plan (see the section on Accident management and emergency preparedness *(paragraph 639 ff.)*);

b) there are no institutions with a high concentration of relatively immobile people; or if there is any such institution, the emergency planning authority (ie the local authority) confirms that appropriate arrangements have been made in its emergency plan.

113 The characteristics of the off-site population should not prejudice the extendibility of emergency response beyond the Detailed Emergency Planning Zone (DEPZ), on an appropriate timescale, to deal with a larger radiation emergency than that used to define the DEPZ.

Siting	**Local physical data**	**ST.3**
The safety case should include information on local physical data relevant to the dispersion of released radioactivity and its potential effects on people.		

114 Consideration should be given to aspects that might affect the movement of people and goods, including nuclear materials, into and out of the site, regarding any implications for safety during normal operation (see the sub-section on Control of nuclear matter *(paragraph 392 ff.)*).

115 These considerations should include all transport routes, including road, rail, sea, air and underground routes.

116 The safety case should identify data on aspects of local topography, hydrology, geology and hydrogeology relevant to radioactivity dispersion.

117 The safety case should identify data on aspects of meteorology relevant to radioactivity dispersion off-site, including any local variations from the regional.

118 To demonstrate the practicability of emergency response, the data should be used in assessment of potential dispersion and deposition of radioactivity from possible radiation emergencies, using well-established and researched models.

119 The safety case should provide information on local topography and transport routes and identify any implications for the movement of people arising from the new facility.

120 Consideration should be given to implications for the emergency response of local topography and transport routes, taking account of factors including the evacuation of people off-site, movement and protection of emergency personnel and emergency vehicles and goods travelling to and from the site.

Siting	**External hazards**	**ST.4**
Natural and man-made external hazards should be considered if they have the potential to adversely affect the siting decision.		

121 If the external hazards over which the dutyholder has no control are judged to be too great to be accommodated through the design of plant, the use of a site may be precluded for its proposed purpose.

Siting	**Effect on other hazardous installations**	**ST.5**
The safety case should take account of any hazardous installations that might be affected by an incident at the nuclear facility.		

122 This principle covers possible situations where a non-nuclear hazardous installation off-site might be damaged by a nuclear or non-nuclear incident on the nuclear site. This may exacerbate the off-site effects of the nuclear site incident or increase the difficulty of remedial action on the nuclear site. It should cover transport facilities as well as fixed installations etc.

Siting	Multi-facility sites	ST.6
On multi-facility sites, the safety case should consider the site as a whole to establish that hazards from interactions between facilities have been taken into account.		

123 The assessment of interactions between facilities requires that:

a) all potential radiological hazards on the site should be identified;

b) all facilities on the site should be identified: for completeness, this must include facilities that do not contain radioactive or nuclear material;

c) all services on the site should be identified.

124 Interactions between facilities, between facilities and shared services and between shared services, where events in one may adversely affect others, should be explicitly considered in determining the potential for escalation of the risks for the site. This requires an analysis of events that can have physical effects outside the boundaries or limits for the particular facility or service. These may be:

a) faults, internal hazards or external hazards that affect more than one facility and shared service at the same time;

b) domino effects that can progress directly from one facility to another or via shared services;

c) interactions between shared services that affect several facilities.

125 In considering the risks from a site, and whether they are ALARP, consideration on a site-wide basis will be needed for certain internal or external hazards that have the potential to affect all the facilities and services on the site.

126 Where a site has been considered for analysis purposes as comprising several facilities, a specific consideration of overall site risks should be carried out, unless it can be shown that there are no common shared services or interactions between the facilities, between facilities and shared services and between shared services.

127 Where neighbouring sites, which may be under the control of different dutyholders, share common systems or have the potential for interactions, there should be co-operation between them in developing safety cases. Formal mechanisms should be established and demonstrated to be working to regulators. All relevant dutyholders should be able to demonstrate that they are undertaking liaison and acting upon agreed decisions with site owners and all external stakeholders.

Siting	Through life siting issues	ST.7
The safety case should be revised to take account of off-site changes that could affect safety on a nuclear site.		

128 The safety case needs to be reviewed to take account of the potential impact of local developments on the site.

129 Arrangements should be in place for the relevant planning authority(ies) to be consulted throughout the facility lifecycle on any proposed land-use developments off-site that might prejudice the effectiveness of the arrangements to protect individuals and populations. HSE makes similar arrangements to be consulted by planning authorities.

130 New information that could have an impact on activities on-site or off-site should be checked to establish the affect on safety. Suitable amendments should be made to the safety case and operation and emergency arrangements, as appropriate.

ENGINEERING PRINCIPLES

131 These principles comprise the major part of the SAPs. Engineering standards need to be high to achieve the necessary high level of nuclear safety. Achievement of this can then be checked against the fault analysis principles in the section on Fault analysis (paragraph 496 ff.), usually in an iterative manner.

132 The principles in this section are presented in three main groups as follows:

a) key principles;

b) general principles;

c) engineering principles for specific areas.

133 Collectively, this section brings together a range of engineering topics that should be considered in dealing with the assessment of a facility and/or site.

134 The ALARP principle has been discussed in the Introduction (paragraph 9 ff.) and applies in assessments made against the engineering principles. Similarly, the engineering principles apply across a wide range of facilities of differing magnitude of radiological hazard and the guidance on the proportionate approach set out earlier should be applied. Applying these principles therefore requires judgement in deciding whether in any particular instance enough has been done in relation to each of the relevant principles.

135 In applying these principles, the inspector should consider their application to all stages of a facility's life-cycle. For example, it should be designed and operated so that it may be decommissioned safely, as soon as is reasonably practicable, and in accordance with radioactive waste management principles.

Key engineering principles

Engineering principles: key principles	Inherent safety	EKP.1
The underpinning safety aim for any nuclear facility should be an inherently safe design, consistent with the operational purposes of the facility.		

136 An 'inherently safe' design is one that avoids radiological hazards rather than controlling them. It prevents a specific harm occurring by using an approach, design or arrangement that ensures that the harm cannot happen, for example a criticality safe vessel. Inherent safety is not the same as 'passive safety'. Where inherently safe design is not achievable, the design should be fault tolerant.

137 The achievement of inherently safe design can be assisted by:

a) reducing the inventory of potentially harmful substances to the minimum necessary to achieve the required function of the facility;

b) controlling the physical state of harmful substances to remove or minimise their potential effects;

c) minimising the energy potential within the process consistent with the required functionality of the facility, and of its various components.

138 Application of this principle should minimise the need for, and reliance on, safety systems and the challenges placed on them.

Engineering principles: key principles	Fault tolerance	EKP.2
The sensitivity of the facility to potential faults should be minimised.		

139 Any failure, process perturbation or mal-operation in a facility should produce a change in plant state towards a safer condition, or produce no significant response. If the change is to a less safe condition, then systems should have long time constants so that key parameters deviate only slowly from their desired values.

Engineering principles: key principles	Defence in depth	EKP.3
A nuclear facility should be so designed and operated that defence in depth against potentially significant faults or failures is achieved by the provision of several levels of protection.		

140 International consensus is that the appropriate strategy for achieving the overall safety objective is through the application of the concept of defence in depth. This should provide a series of levels of defence (inherent features, equipment and procedures) aimed at preventing accidents and ensuring appropriate protection in the event that prevention fails.

141 The levels of protection should prevent faults, or if prevention fails should ensure detection, limit the potential consequences and prevent escalation.

142 The concept of defence in depth should be applied so that:

a) deviations from normal operation and failures of structures, systems and components important to safety are prevented;

b) any deviations from normal operation are allowed for by safety margins that enable detection and action that prevents escalation;

c) inherent safety features of the facility, fail-safe design and safety measures are provided to prevent fault conditions that occur from progressing to accidents;

d) additional measures are provided to mitigate the consequences of severe accidents.

143 Defence in depth is generally applied in five levels. The methodology ensures that if one level fails, it will be compensated for, or corrected by, the subsequent level. The aims for each level of protection are described in detail in IAEA Safety Standard NS-R-1[9], on which Table 1 is based. It should be noted that Table 1 deals with the application of defence in depth in the design of a facility, and does not deal with other important contributions such as human performance or equipment reliability. These topics are addressed in other sections of the SAPs.

Table 1 Objective of each level of protection and essential means of achieving them

Level	Objective	Essential means
Level 1	Prevention of abnormal operation and failures by design	Conservative design, construction, maintenance and operation in accordance with appropriate safety margins, engineering practices and quality levels
Level 2	Prevention and control of abnormal operation and detection of failures	Control, indication, alarm systems or other systems and operating procedures to prevent or minimise damage from failures
Level 3	Control of faults within the design basis	Engineered safety features, multiple barriers and accident or fault control procedures
Level 4	Control of severe plant conditions in which the design basis may be exceeded, including the prevention of fault progression and mitigation of the consequences of severe accidents	Additional measures and procedures to prevent or mitigate fault progression and for accident management
Level 5	Mitigation of radiological consequences of significant releases of radioactive substances	Emergency control and on- and off-site emergency response

144 An important aspect of the implementation of defence in depth is the provision of multiple, and as far as possible independent, barriers to the release of radioactive substances to the environment, and to ensure the confinement of radioactive substances at specified locations. The number of barriers will depend on the magnitude of the radiological hazard and the consequences of failure.

Engineering principles: key principles	Safety function	EKP.4
The safety function(s) to be delivered within the facility should be identified by a structured analysis.		

145 The identification of safety functions should be based on an analysis of all significant fault sequences arising from possible initiating faults (see the Fault analysis section *(paragraph 496 ff.)*). The identification should include internal and external hazards, and consider the loss or failure of structures, systems and components needed for safety in normal operations, eg structural integrity and shielding, even where these can be threatened only by extremely remote or 'incredible' events but for which no design safety function capability is required.

Engineering principles: key principles	Safety measures	EKP.5
Safety measures should be identified to deliver the required safety function(s).		

146 Safety should be secured by characteristics as near as possible to the top of the list below:

a) Passive safety measures that do not rely on control systems, active safety systems or human intervention.

b) Automatically initiated active engineered safety measures.

c) Active engineered safety measures that need to be manually brought into service in response to the fault.

d) Administrative safety measures (see paragraph 376 f.).

e) Mitigation safety measures (eg filtration or scrubbing).

Note: The hierarchy above should not be interpreted to mean that the provision of an item towards the top of the list precludes provision of other items where they can contribute to defence in depth.

147 The availability and reliability of the safety measures should be commensurate with the significance of the radiological hazards to be controlled. There should also be measures in place to mitigate the consequences of any accident where radioactivity is released from its intended containment, but these should not be regarded as a substitute for fault prevention but as further defence in depth.

Safety classification and standards

148 The effective implementation of defence in depth needs support from a number of general principles and related measures that assure the reliability and capability of the means of achieving the objectives. It is important that structures, systems and components, including software for instrumentation and control, are classified on the basis of their safety significance and are designed, manufactured, installed and then subsequently commissioned, operated and maintained to a level of quality commensurate with their classification.

Engineering principles: safety classification and standards	Safety categorisation	ECS.1
The safety functions to be delivered within the facility, both during normal operation and in the event of a fault or accident, should be categorised based on their significance with regard to safety.		

149 A safety categorisation scheme could be determined on the following basis:

a) Category A – any function that plays a principal role in ensuring nuclear safety.

b) Category B – any function that makes a significant contribution to nuclear safety.

c) Category C – any other safety function.

150 The method for categorising safety functions should take into account:

a) the consequence of failing to deliver the safety function;
b) the extent to which the function is required, either directly or indirectly, to prevent, protect against or mitigate the consequences of initiating faults;
c) the potential for a functional failure to initiate a fault or exacerbate the consequences of an existing fault;
d) the likelihood that the function will be called upon.

151 The categorisation of safety functions should take no account of any redundancy, diversity or independence within the design – these aspects relate to the structures, systems and components required to deliver the safety function.

152 The categorisation assigned to each safety function should be used to classify structures, systems and components required to deliver that function.

Engineering principles: safety classification and standards	**Safety classification of structures, systems and components**	**ECS.2**
Structures, systems and components that have to deliver safety functions should be identified and classified on the basis of those functions and their significance with regard to safety.		

153 The method for classifying the safety significance of a structure, system or component should primarily be based on deterministic methods, complemented where appropriate by probabilistic methods and engineering judgement, with account taken of factors such as:

a) the category of safety function(s) to be performed by the item (see Principle ECS.1);
b) the consequences of failure to perform its function;
c) the probability that the item will be called upon to perform a safety function;
d) the time following any initiating fault at which, or the period throughout which, it will be called upon to operate.

154 A safety classification scheme could be determined on the following basis:

a) Class 1 – any structure, system or component that forms a principal means of fulfilling a Category A safety function.
b) Class 2 – any structure, system or component that makes a significant contribution to fulfilling a Category A safety function, or forms a principal means of ensuring a Category B safety function.
c) Class 3 – any other structure, system or component.

155 Appropriately designed interfaces should be provided between structures, systems and components of different classes to ensure that any failure in a lower class item will not propagate to an item of a higher class. Equipment providing the function to prevent the propagation of failures should be assigned to the higher class.

156 Auxiliary services that support components of a system important to safety should be considered part of that system and should be classified accordingly unless failure does not prejudice successful delivery of the safety function.

Engineering principles: safety classification and standards	**Standards**	**ECS.3**
Structures, systems and components that are important to safety should be designed, manufactured, constructed, installed, commissioned, quality assured, maintained, tested and inspected to the appropriate standards.		

157 The standards should reflect the functional reliability requirements of structures, systems and components and be commensurate with their safety classification.

158 Appropriate national or international codes and standards should be adopted for Classes 1 and 2 of structures, systems and components. For Class 3, appropriate non-nuclear-specific codes and standards may be applied.

159 Codes and standards should be preferably nuclear-specific codes or standards leading to a conservative design commensurate with the importance of the safety function(s) being performed. The codes and standards should be evaluated to determine their applicability, adequacy and sufficiency and should be supplemented or modified as necessary to a level commensurate with the importance of the safety function(s) being performed.

160 Where a structure, system or component is required to deliver multiple safety functions, and these can be demonstrated to be delivered independently of one another, codes and standards should be used appropriate to the category of the safety function. Where independence cannot be demonstrated, codes and standards should be appropriate to the class of the structure, system or component (ie in accordance with the highest category of safety function to be delivered). Whenever different codes and standards are used for different aspects of the same structure, system or component, the compatibility between these should be demonstrated.

161 The combining of different codes and standards for a single aspect of a structure, system or component should be avoided or justified when used. Compatibility between these codes and standards should be demonstrated.

Engineering principles: safety classification and standards	**Codes and standards**	**ECS.4**
For structures, systems and components that are important to safety, for which there are no appropriate established codes or standards, an approach derived from existing codes or standards for similar equipment, in applications with similar safety significance, may be applied.		

Engineering principles: safety classification and standards	**Use of experience, tests or analysis**	**ECS.5**
In the absence of applicable or relevant codes and standards, the results of experience, tests, analysis, or a combination thereof, should be applied to demonstrate that the item will perform its safety function(s) to a level commensurate with its classification.		

Equipment qualification

Engineering principles: equipment qualification	**Qualification procedures**	**EQU.1**
Qualification procedures should be in place to confirm that structures, systems and components that are important to safety will perform their required safety function(s) throughout their operational lives.		

162 The qualification procedures should demonstrate a level of confidence commensurate with their safety classification.

163 Procedures for the qualification of equipment should address operational, environmental and fault conditions (including severe accidents where appropriate) specified in the design.

164 The procedures should include a physical demonstration that individual items can perform their safety function(s) under the required conditions, and within the time substantiated in the facility's safety case.

165 The procedures should ensure that adequate arrangements exist (Licence Condition 6, see the HSE website) for the recording and retrieval of lifetime data covering the item's construction, manufacture, testing, inspection and maintenance to demonstrate that any assumptions made in the safety case remain valid throughout operational life.

Design for reliability

166 *Engineered structures, systems and components should be designed to deliver their required safety functions with adequate reliability, according to the magnitude and frequency of the radiological hazard, to provide confidence in the robustness of the overall design.*

167 *Ideally, the structures, systems and components important to safety should be fail-safe, ie they should have no unsafe failure modes.*

168 *The design should incorporate redundancy to avoid the effects of random failure, and diversity and segregation to avoid the effects of common cause failure. Examples of diversity are different operating conditions, different working principles or different design teams, different sizes of equipment, different manufacturers, different components, and types of equipment that use different physical methods. The design should also be tolerant of random failure occurring anywhere within the safety systems provided to secure each safety function.*

169 *The application of the principles in this section may vary according to whether the structures, systems and components form part of a safety system (which acts in response to a plant fault, to prevent or mitigate a radiological consequence) or a safety-related system (a plant system other than a safety system, on which safety may depend).*

Engineering principles: design for reliability	**Failure to safety**	**EDR.1**
Due account should be taken of the need for structures, systems and components important to safety to be designed to be inherently safe or to fail in a safe manner and potential failure modes should be identified, using a formal analysis where appropriate.		

Engineering principles: design for reliability	**Redundancy, diversity and segregation**	**EDR.2**
Redundancy, diversity and segregation should be incorporated as appropriate within the designs of structures, systems and components important to safety.		

170 It should be demonstrated that the required level of reliability for their intended safety function has been achieved.

Engineering principles: design for reliability	**Common cause failure**	**EDR.3**
Common cause failure (CCF) should be explicitly addressed where a structure, system or component important to safety employs redundant or diverse components, measurements or actions to provide high reliability.		

171 CCF claims should be substantiated.

172 In general, claims for CCF should not be better than one failure per 100 000 demands. The figure of one failure per 100 000 demands represents a judgement by NII of the best limit that could reasonably be supported for a simple system by currently available data and methods of analysis. A worse figure may need to be used (say 1 per 10 000 or 1 per 1000) according to the complexity and novelty of the system, the nature of threat and the capability of the equipment.

173 Nevertheless, it is conceivable that the continuing accumulation of good data and advances in its analysis could lead, in exceptional circumstances, to a situation where a strong case could be made by the dutyholder for better figures. Such a case would not then be ruled out of consideration.

174 Where required reliabilities cannot be achieved due to CCF considerations, the required safety function should be achieved taking account of the concepts of diversity and segregation, and by providing at least two independent safety measures.

Engineering principles: design for reliability	Single failure criterion	EDR.4
During any normally permissible state of plant availability no single random failure, assumed to occur anywhere within the systems provided to secure a safety function, should prevent the performance of that safety function.		

175 Consequential failures resulting from the assumed single failure should be considered as an integral part of the single failure. Further discussion of the single failure criterion is given in IAEA Safety Standard NS-G-1.2.[4]

Reliability claims

Engineering principles: reliability claims	Form of claims	ERL.1
The reliability claimed for any structure, system or component important to safety should take into account its novelty, the experience relevant to its proposed environment, and the uncertainties in operating and fault conditions, physical data and design methods.		

176 Adequate reliability and availability should be demonstrated by suitable analysis and data.

177 Where reliability data is unavailable, the demonstration should be based on a case-by-case analysis and include:

a) a comprehensive examination of all the relevant scientific and technical issues;

b) a review of precedents set under comparable circumstances in the past;

c) an independent third-party assessment in addition to the normal checks and conventional design;

d) periodic review of further developments in technical information, precedent and best practice.

178 Where data is shown to be inadequate, appropriate measures should be taken to ensure that the onset of failure can be detected, and that the consequences of failure are minimised. This may include replacing the component after a fixed lifetime, or dependent on inspection results.

Engineering principles: reliability claims	Measures to achieve reliability	ERL.2
The measures whereby the claimed reliability of systems and components will be achieved in practice should be stated.		

179 Evidence, including quality assurance, should be provided to demonstrate the adequacy of any such measures. This should include a reliability analysis of both random and systematic failures. Assumptions made in the course of the reliability analysis should be justified.

Engineering principles: reliability claims	Engineered safety features	ERL.3
Where reliable and rapid protective action is required, automatically initiated engineered safety features should be provided.		

180 For requirements that are less demanding or on a longer timescale, operator actions or administrative control may be acceptable to complement the engineered systems. The objective should be to minimise the dependence on human action to maintain a safe state.

Engineering principles: reliability claims	Margins of conservatism	ERL.4
Where multiple safety-related systems and/or other means are claimed to reduce the frequency of a fault sequence, the reduction in frequency should have a margin of conservatism with allowance for uncertainties.		

181 Usually, safety-related systems tend to be more complex than safety systems and are typically designed to less rigorous standards. Hence special attention should be devoted to potential common cause failures, due pessimism in assigned reliability values, availability, and measures to ensure that its safety significance will continue to be recognised throughout its life. This is particularly important where claims are made on combinations of more than one safety-related system.

Commissioning

Engineering principles: commissioning	Commission testing	ECM.1
Before operating any facility or process that may affect safety it should be subject to commissioning tests to demonstrate that, as built, the design intent claimed in the safety case has been achieved.		

182 The commissioning tests should endeavour to identify any errors made during the design, manufacture, or construction/installation stages.

183 Commissioning should be more than a demonstration that the plant will work. It should also include safety tests as a key step in assuring safety. This is the intent of Licence Condition 21 (see the HSE website). The tests should be designed to demonstrate that the plant and associated safety systems provide the intended degree of protection against faults, including human errors.

184 The safety case should identify those commissioning tests and inspections required to:

a) confirm the facility's design safety assumptions and predicted performance, in particular that of the safety provisions; and

b) characterise the facility as a basis for evaluating its behaviour during its operational life. The safety analysis should be reviewed in the light of the results of the commissioning programme and of any modifications made to the design or intended operating procedures since the commencement of construction.

185 The tests should be divided into stages to complete as much inactive testing before the introduction of radioactive substance. Inactive testing should demonstrate that the facility has been constructed, manufactured, and installed correctly. Where any deviations from the documentation are found, the licensee should demonstrate that this does not compromise the safety analysis in the safety case.

186 Inactive testing should also be used to confirm the operational features of the facility and be used to develop the operating instructions, which should then be confirmed during active commissioning. Before active commissioning can begin, the necessary arrangements to satisfy Principles MS.2 *(paragraph 51 f.)* and SC.6 *(paragraph 95 f.)*, especially in relation to operating limits and conditions, together with accident management and emergency preparedness, should be in place.

Maintenance, inspection and testing

Engineering principles: maintenance, inspection and testing	Identification of requirements	EMT.1
Safety requirements for in-service testing, inspection and other maintenance procedures and frequencies should be identified in the safety case.		

187 Appropriate and sufficient locations should be provided within the plant where process materials, plant items, construction materials and other items arising from plant breakdown, maintenance or refurbishment can be temporarily stored so that their level of contamination, chemical and physical properties, ease of decontamination and repair can be assessed.

Engineering principles: maintenance, inspection and testing	**Frequency**	**EMT.2**
Structures, systems and components important to safety should receive regular and systematic examination, inspection, maintenance and testing.		

Engineering principles: maintenance, inspection and testing	**Type-testing**	**EMT.3**
Structures, systems and components important to safety should be type tested before they are installed to conditions equal to, at least, the most severe expected in all modes of normal operational service.		

188 For components of particular concern and where it is not possible to confirm the ability to operate under the most onerous design conditions, reference data from commissioning or rig testing should be established for comparison against in-service test results.

Engineering principles: maintenance, inspection and testing	**Validity of equipment qualification**	**EMT.4**
The validity of equipment qualification for structures, systems and components important to safety should not be unacceptably degraded by any modification or by the carrying out of any maintenance, inspection or testing activity.		

Engineering principles: maintenance, inspection and testing	**Procedures**	**EMT.5**
Commissioning and in-service inspection and test procedures should be adopted that ensure initial and continuing quality and reliability.		

189 Such inspection should be of sufficient extent and frequency to give adequate confidence that degradation will be detected before loss of the safety function.

Engineering principles: maintenance, inspection and testing	**Reliability claims**	**EMT.6**
Provision should be made for testing, maintaining, monitoring and inspecting structures, systems and components important to safety in service or at intervals throughout plant life commensurate with the reliability required of each item.		

190 In especially difficult circumstances where this cannot be done, either additional design measures should be incorporated to compensate for the deficiency, or it should be demonstrated that the adequate long-term performance would be achieved without such measures.

191 Where test equipment, or other engineered means, is claimed as part of in-service or periodic testing, maintenance, monitoring and inspection provisions, the extent to which they reveal failures affecting safety functions should be justified. The test equipment, or other engineered means, should be tested at intervals sufficient to uphold the reliability claims of the equipment within which it is claimed to reveal faults.

Engineering principles: maintenance, inspection and testing	Functional testing	EMT.7
In-service functional testing of systems, structures and components important to safety should prove the complete system and the safety-related function of each component.		

192 Maintenance, inspection and testing are a part of normal operation and it should be possible to carry out these tests without any loss of any safety function.

193 Where complete functional testing is claimed not to be reasonably practicable, an equivalent means of functional proving should be demonstrated.

Engineering principles: maintenance, inspection and testing	Effect of internal/external events	EMT.8
Structures, systems and components important to safety should be inspected and/or re-validated after any internal or external event that might have challenged their design basis.		

Ageing and degradation

Engineering principles: ageing and degradation	Safe working life	EAD.1
The safe working life of structures, systems and components that are important to safety should be evaluated and defined at the design stage.		

194 Particular attention should be given to the evaluation of those components that are judged to be difficult or impracticable to replace.

195 There should be an adequate margin between the intended operational life and the predicted safe working life of such structures, systems and components.

Engineering principles: ageing and degradation	Lifetime margins	EAD.2
Adequate margins should exist throughout the life of a facility to allow for the effects of materials ageing and degradation processes on structures, systems and components that are important to safety.		

196 The design process and periodic reviews should allow for any uncertainties in determining the initial state of components and the rate of ageing and degradation.

197 Programmes for monitoring, inspection, sampling, surveillance and testing, to detect and monitor ageing and degradation processes, should be used to verify assumptions and assess whether the margins will be adequate for the remaining life of the structure, system or component.

198 Appropriate testing of material aged under representative conditions should be undertaken and the results reviewed against the safety case expectations for such changes.

199 The effects of and interactions between the mechanical, thermal, chemical, physical, biological and radiation environment on materials properties, materials ageing and degradation processes should be considered.

200 Timely mitigation of ageing and its effects should be undertaken to ensure that the required safety margins are maintained.

Engineering principles: ageing and degradation	Periodic measurement of material properties	EAD.3
Where material properties could change with time and affect safety, provision should be made for periodic measurement of the properties.		

201 The properties should be obtained from fully representative samples of material especially when the component or structure forms a principal means of ensuring nuclear safety.

Engineering principles: ageing and degradation	Periodic measurement of parameters	EAD.4
Where parameters relevant to the design of plant could change with time and affect safety, provision should be made for their periodic measurement.		

Engineering principles: ageing and degradation	Obsolescence	EAD.5
A process for reviewing the obsolescence of structures, systems and components important to safety should be in place.		

202 This principle is more likely to be applicable to systems and components rather than the main structural elements of a facility. The process should identify threats from obsolescence and ensure that an adequate supply of spare parts is available until a solution to any obsolescence issues can be found. The solution will depend on the particular circumstances, but may involve providing alternative components or items of equipment that can carry out the same safety duty, or it may involve redesigning the plant to remove the need for the obsolescent system or components.

Layout

203 The following principles address the layout of the facilities on a site, the plant within a facility(ies) and structures, systems and components within a plant. Specific principles, where appropriate, are contained in subsequent sub-sections.

204 The layout of a site or of plant in any particular facility is important to safety in that it can affect ease of access for normal operational needs. Facility layout may have an influence upon the ability to meet the duty to reduce radiation doses to ALARP and can be a factor in providing means of preventing unauthorised access. Layout can also affect consequences of incidents, particularly internal and external hazards, and the access conditions following an incident.

Engineering principles: layout	Access	ELO.1
The design and layout should facilitate access for necessary activities and minimise adverse interactions during such activities.		

205 The layout should:

a) ensure that sufficient access, lighting etc is available to be able to carry out all necessary operational, maintenance, inspection and testing activities;
b) ensure that radiation doses to workers carrying out operational, maintenance, inspection and testing activities are ALARP;
c) minimise adverse interactions during operational, maintenance, inspection and testing activities with other structures systems or components;
d) provide an alternative means of access to facilities and control functions essential to safety that may require local manual intervention;

e) ensure a safe means of escape, with normal and emergency lighting, from buildings or plant areas that may be affected by an incident; and

f) have alternative access to rescue equipment in all normally manned areas.

Engineering principles: layout	Unauthorised access	ELO.2
Unauthorised access to or interference with safety systems and their reference data and with safety-related structures and components should be prevented.		

Engineering principles: layout	Movement of nuclear matter	ELO.3
Site and facility layouts should minimise the movement of nuclear matter.		

Engineering principles: layout	Minimisation of the effects of incidents	ELO.4
The design and layout of the site and its facilities, the plant within a facility and support facilities and services should be such that the effects of incidents are minimised.		

206 For example, the design and layout should:

a) minimise the direct effects of incidents, particularly internal and external hazards, on structures, systems or components;

b) minimise any interactions between a failed structure, system or component and other safety-related structures, systems or components;

c) ensure site personnel are physically protected from direct or indirect effects of incidents;

d) facilitate access for necessary recovery actions following an event.

207 Support facilities and services important to the safe operation of the nuclear facility should be designed and routed so that, in the event of incidents, sufficient capability to perform their emergency functions will remain. Support facilities and services include access roads, water supplies, fire mains and site communications.

External and internal hazards

208 External hazards are those natural or man-made hazards to a site and facilities that originate externally to both the site and its processes, ie the dutyholder may have very little or no control over the initiating event. External hazards include earthquake, aircraft impact, extreme weather, electromagnetic interference (off-site cause) and flooding as a result of extreme weather/climate change (this list is not exhaustive). Terrorist or other malicious acts are assessed as external hazards. The dutyholder should demonstrate that an effective process has been applied to identify all types of external hazard relevant to a particular site.

209 Internal hazards are those hazards to plant and structures that originate within the site boundary but are, for example, external to the process in the case of nuclear chemical plant, or external to the primary circuit in the case of power reactors. That is, the dutyholder has control over the initiating event in some form. Internal hazards include internal flooding, fire, toxic gas release, dropped loads and explosion/missiles.

210 This sub-section starts with general principles, followed by principles for specific internal and external hazards.

Engineering principles: external and internal hazards	Identification	EHA.1
External and internal hazards that could affect the safety of the facility should be identified and treated as events that can give rise to possible initiating faults.		

211 This identification should include consequential events and, as appropriate, combinations of consequential events from a common initiating event.

212 Any generic type of hazard with a total frequency that is demonstrably below once in ten million years may be excluded. Any generic type of hazard, the impact of which has no effect on the safety of the facility, can also be excluded. This screening should retain all hazards for which the frequency of realisation and the potential impact might make a significant contribution to the overall risks from the facility.

213 The potential of a hazard to affect the safety of a facility may take account of factors such as the source of the hazard in relation to the facility and the design characteristics of the facility.

Engineering principles: external and internal hazards	Data sources	EHA.2
For each type of external hazard either site specific or, if this is not appropriate, best available relevant data should be used to determine the relationship between event magnitudes and their frequencies.		

Engineering principles: external and internal hazards	Design basis events	EHA.3
For each internal or external hazard, which cannot be excluded on the basis of either low frequency or insignificant consequence, a design basis event should be derived.		

214 Some hazards may not be amenable to the derivation of a design basis event. Such hazards may include fire and lightning, but are addressed through appropriate application of codes and standards.

Engineering principles: external and internal hazards	Frequency of exceedance	EHA.4
The design basis event for an internal and external hazard should conservatively have a predicted frequency of exceedance of no more than once in 10 000 years.		

215 Consideration may also be given to arguments presented to derive the design basis event from a higher frequency of exceedance if the facility cannot give rise to high, unmitigated doses.

216 Where the radiological consequences arising from an external hazard are low, it may be appropriate for a facility to be designed to hazard loads using normal industrial standards.

Engineering principles: external and internal hazards	Operating conditions	EHA.5
Hazard design basis faults should be assumed to occur simultaneously with the most adverse normal facility operating condition.		

Engineering principles: external and internal hazards	Analysis	EHA.6
Analyses should take into account simultaneous effects, common cause failure, defence in depth and consequential effects.		

217 To achieve the above two principles the analysis should take into account that:

a) certain internal or external hazards may not be independent of each other and may occur simultaneously or in a combination that it is reasonable to expect;

b) an internal or external hazard may occur simultaneously with a facility fault, or when plant is out for maintenance;

c) there is a significant potential for internal or external hazards to act as initiators of common cause failure, including loss of off-site power and other services;

d) many internal and external hazards have the potential to threaten more than one level of defence in depth at once;

e) internal hazards (eg fire) can arise as a consequence of faults internal or external to the site and should be included, therefore, in the relevant fault sequences; and

f) the severity of the effects of the internal or external hazard experienced by the facility may be affected by facility layout, interaction, and building size and shape.

Engineering principles: external and internal hazards	'Cliff-edge' effects	EHA.7
A small change in DBA parameters should not lead to a disproportionate increase in radiological consequences.		

Engineering principles: external and internal hazards	Aircraft impact	EHA.8
The total predicted frequency of aircraft crash, including helicopters and other airborne vehicles, on or near any facility housing structures, systems and components important to safety should be determined.		

218 The calculation of crash frequency should include the most recent crash statistics, flight paths and flight movements for all types of aircraft and take into account foreseeable changes in these factors if they affect the risk. (Malicious acts are dealt with separately).

219 Should the total predicted frequency of aircraft crash be shown to be lower than that typically defined as a design basis event, and greater than that which can be automatically excluded, efforts should be made to understand and minimise the potential impact consequences on structures, systems and components important to safety. The external hazard associated with the impacts should include the possibility of fires and/or explosions from aircraft fuel.

Engineering principles: external and internal hazards	Earthquakes	EHA.9
The seismology and geology of the area around the site and the geology of the site should be evaluated to derive a design basis earthquake (DBE).		

220 The studies should:

a) establish information on historical and instrumentally recorded earthquakes that have occurred in the region;

b) be proportionate to the radiological hazard posed by the site, while covering those aspects that could affect the estimation of the seismic hazard at the site; and

c) enable buildings, structures and plant in the nuclear facility to be designed to withstand safely the ground motions involved, if needed.

221 An operating basis earthquake (OBE) should also be determined. No structure, system or component important to safety should be impaired by the repeated occurrence of ground motions at the OBE level. Where the appropriate response to an OBE is a facility shutdown, the facility should not be restarted until inspection has shown that it is safe to do so.

222 In determining the effect of a seismic event on any facility, the simultaneous effect of that event on any other facility or installation in the vicinity, and on the safety of any system or service that may have a bearing on safety, should also be taken into account.

Engineering principles: external and internal hazards	Electromagnetic interference	EHA.10
The design of facility should include protective measures against the effects of electromagnetic interference.		

223 An assessment should be made to determine whether any source of electromagnetic interference either on-site or off-site could cause malfunction in or damage to safety-related equipment or instrumentation.

Engineering principles: external and internal hazards	Extreme weather	EHA.11
Nuclear facilities should withstand extreme weather conditions that meet the design basis event criteria.		

224 Types of extreme weather should include abnormal wind loadings, wind blown debris, precipitation, accumulated ice and snow deposits, lightning, extremes of high and low temperature, humidity and drought.

225 The design basis event should take account of reasonable combinations of extreme weather conditions that may be expected to occur, and of the effect of failure of any non-nuclear hazardous installations off-site and other nuclear facilities, on- or off-site, during such conditions.

226 The reasonably foreseeable effects of climate change over the lifetime of the facility should be taken into account.

Engineering principles: external and internal hazards	Flooding	EHA.12
Nuclear facilities should withstand flooding conditions that meet the design basis event criteria.		

227 The area around the site should be evaluated to determine the potential for flooding due to external hazards eg precipitation, high tides, storm surges, barometric effects, overflowing of rivers and upstream structures, coastal erosion, seiches and tsunamis.

228 The design basis flood should take account, as appropriate, of the combined effects of high tide, wind effects, wave actions, duration of the flood and flow conditions.

Engineering principles: external and internal hazards	Fire, explosion, missiles, toxic gases etc – use and storage of hazardous materials	EHA.13
The on-site use, storage or generation of hazardous materials should be minimised, and controlled and located so that any accident to, or release of, the materials will not jeopardise the establishing of safe conditions on the facility.		

229 The potential for generation of hazardous materials (including toxic, corrosive and flammable) through normal or abnormal processes should be considered.

Engineering principles: external and internal hazards	Fire, explosion, missiles, toxic gases etc – sources of harm	EHA.14
Sources that could give rise to fire, explosion, missiles, toxic gas release, collapsing or falling loads, pipe failure effects, or internal and external flooding should be identified, specified quantitatively and their potential as a source of harm to the nuclear facility assessed.		

230 This identification should take into account:

a) projects and planned future developments on and off the site;

b) the adequacy of protection of the nuclear facility from the effects of any incident in an installation, means of transport, pipeline, power supplies, water supplies etc either inside or outside the nuclear site.

c) sources could be either on or off the site;

Engineering principles: external and internal hazards	Fire, explosion, missiles, toxic gases etc – effect of water	EHA.15
The design of the facility should prevent water from adversely affecting structures, systems and components important to safety.		

231 The design of the facility should include adequate provision for the collection and discharge of water reaching the site from any design basis external event or internal flooding hazard or, if this is not achievable, the structures, systems and components important to safety should be adequately protected against the effects of water.

Engineering principles: external and internal hazards	Fire, explosion, missiles, toxic gases etc – fire detection and fighting	EHA.16
Fire detection and fire-fighting systems of a capacity and capability commensurate with the credible worst-case scenarios should be provided.		

232 The systems should be designed and located so that any damage they may sustain or their spurious operation does not affect the safety of the facility.

233 A fire hazard analysis should be made of the facility to:

a) analyse the potential for fire initiation and growth and the possible consequences on safety systems and other structures, systems and components important to safety;

b) determine the need for segregation of plant and the location and required fire resistance of boundaries to limit the spread of fire; and

c) determine the capacity and capability of the detection and fire-fighting systems to be provided.

Engineering principles: external and internal hazards	Fire, explosion, missiles, toxic gases etc – use of materials	EHA.17
Non-combustible or fire-retardant and heat-resistant materials should be used throughout the facility.		

Pressure systems

Engineering principles: pressure systems	Removable closures	EPS.1
The failure of a removable closure to a pressurised component or system that could lead to a major release of radioactivity should be prevented.		

234 In such situations:

a) adequate redundancy and where appropriate, diversity of closure method should be provided; and

b) provision should be made to ensure closures cannot be removed when it is unsafe to do so.

Engineering principles: pressure systems	Flow limitation	EPS.2
Flow limiting devices should be provided to piping systems that are connected to or form branches from a main pressure circuit, to minimise the consequences of postulated breaches.		

235 The flow limiting devices should be as close to the main circuit as practicable. There should be redundancy and diversity of such devices. Closure times of valves and the flow conditions under which they can close should be consistent with the protection they are claimed to provide. Dynamic loadings due to valve closure should be considered.

Engineering principles: pressure systems	Pressure relief	EPS.3
Adequate pressure relief systems should be provided for pressurised systems and provision should be made for periodic testing.		

Engineering principles: pressure systems	Overpressure protection	EPS.4
Overpressure protection should be consistent with any pressure-temperature limits of operation.		

236 Basic characteristics of pressure relief are the pressure at which the relief actuates and the flow capacity of the relief route. The differences between the pressures for first actuation, full relief flow and termination of relief need to be considered. If the pressure relief system is a combination of relief valves and an active protection system to terminate generation of energy or mass input (eg reactor trip), the case for the system as a whole needs to be made.

237 In some circumstances the safe operating pressure of a system may vary with temperature (eg a ferritic reactor vessel moving from cold shutdown to normal operation). The overpressure protection system should provide protection for all operating temperatures. This may require the provision of programmable safety relief valves that can be reset as the pressure vessel temperature changes.

Engineering principles: pressure systems	Discharge routes	EPS.5
Pressure discharge routes should be provided with suitable means to ensure that any release of radioactivity from the facility to the environment is minimised.		

Integrity of metal components and structures

238 This sub-section is concerned with the engineering assessment of the integrity of metallic components and structures such as pressure vessels, boilers, pressure parts, coolant circuits, pipework, core support, pumps, valves, storage tanks and the freestanding metal shell of pressure retaining containment structures. It includes metal pressure boundary penetrations, metal linings of concrete containments and pressure vessels but not the concrete structures as a whole[*].*

239 Any structural integrity safety case should be based on sound engineering practice and take account of safety functional requirements. Taken together, the various elements of sound engineering practice provide defence in depth against a structural integrity failure occurring. Novel approaches and features may be acceptable provided they are supported by appropriate research and development and are tested to show they meet the requirements before coming into service, and monitored during service.

240 Throughout this sub-section, unless specified otherwise, the term 'defect' means any significant deviation from nominal. So, in general, the term 'defect' covers for example, crack-like defects, wall thinning, creep damage and dimensional deviations (eg those affecting buckling).

241 The general lack of adequate reliability data for the disruptive failure of metal components and structures leads to assessment being based primarily on established engineering practice. As a result, although the radiological consequences of failure of a component or structure may be significant (into the range where societal risk is relevant), it is not possible to calculate a plausible failure frequency for inclusion in a fault analysis. At best it might be possible to adopt a representative failure rate that would allow the effect of the component or structure failure to be

[*] Note that should non-metallic components and structures be used, the principles in this sub-section should be interpreted appropriately.

included in a fault analysis in a nominal way or as a sensitivity study. If the safety case is sensitive to the failure frequency, then the estimate will need substantial support from engineering analyses and engineering judgement. At the least, an engineering judgement would be needed to confirm the component or structure in question has characteristics similar to those in the database used to determine reliability values. If lines of protection exist to cope with the effects of the initiating component or structure failure, the overall case may not demand high confidence in the structural integrity claim.

242 Reliability statements for components or structures of interest here might be used to:

a) judge whether an initiating event needs to be included within the design basis. In particular, whether for faults internal to a facility, the expected frequency is greater than 1 x 10^{-5} per annum (pa) (see Principle FA.5 (paragraph 513 f.));

b) provide initiating frequency input to fault analyses. This may require consideration of initiating events with claimed frequencies rather less than 1 x 10^{-5} pa. As claimed failure frequencies for components and structures decrease (and certainly for claims notably less frequent than 1 x 10^{-5} pa) it becomes more difficult to have confidence in the values claimed. Direct actuarial data are absent and models inevitably lack validation against actual occurrences. In such cases a considered judgement is required;

c) give an indication of the level of reliability that is expected from the deterministic integrity arguments of the safety case and so provide a context for judging the adequacy of the deterministic arguments.

Highest reliability components and structures

243 Discounting gross failure of a component or structure is an onerous route to constructing a safety case. Such a case should provide in-depth explanation of the measures over and above normal practice that support and justify the claim. If discounting gross failure cannot be justified, it may be possible to consider a case based on consequences (see paragraph 246).

244 A rule of thumb, generally accepted in the UK for many years, is that it is difficult to substantiate a claim of much less than about 1 x 10^{-7} per vessel year for gross failure of a reasonable sized pressure vessel. Therefore a claim that gross failure of a pressure vessel can be discounted cannot plausibly be associated with a failure rate much better than 1x 10^{-7} to 1 x 10^{-8} per vessel year. There is no generally accepted lowest plausible failure frequency for individual welds, for instance individual pipe welds. As a general guide, claims for pipework weld failure rates for gross failure (eg guillotine failure) much better than 1 x 10^{-8} to 1 x 10^{-9} per weld year should not be considered plausible. This implies that a facility safety case should not rely on claims that gross failure can be discounted for large numbers of pipework and similar welds.

245 A general aim is that no single class of accident should dominate overall facility risk. This general aim should be borne in mind when considering a structural integrity safety case for a particular type of component or system.

246 Where:

a) the case cannot meet the level needed for a claim that the likelihood of a failure event can be discounted, and

b) all practical avenues to improve the structural integrity case have been exhausted;

the basis of the safety case needs to be revisited and the consequences of gross failure of components or structures explicitly considered. This would potentially involve a site-specific evaluation of short and long-term off-site consequences and would still require some estimate of the reliability of the components or structures in question. This broadening of the basis of the safety case would clearly require involvement of disciplines in addition to structural integrity.

247 Principles EMC.1 to EMC.3 should be invoked where:

a) a metal component or structure forms a principal means of ensuring nuclear safety; and

b) the estimated likelihood of gross failure needs to be very low or the safety case claims gross failure can be discounted.

Note: *These principles are supplemented by the other principles for metal components that also need to be met in these situations (see Principles ECS.3 (paragraph 156 f.) and EMC.4 to EMC.34).*

248 An example of the need to apply Principles EMC.1 to EMC.3 would be considering the safety case for a steel reactor pressure vessel (RPV) containing a large core. The RPV is required to have a very low frequency of gross failure. However such low frequencies cannot be demonstrated using actuarial statistics because of a lack of data, and cannot be plausibly or confidently estimated using theoretical modelling. Instead the approach is one of sound engineering practice that gives a high level of confidence in the ability of the vessel to deliver its required safety function throughout its life.

Engineering principles: integrity of metal components and structures: highest reliability components and structures	**Safety case and assessment**	**EMC.1**
The safety case should be especially robust and the corresponding assessment suitably demanding, in order that an engineering judgement can be made for two key requirements: a) the metal component or structure should be as defect-free as possible; b) the metal component or structure should be tolerant of defects.		

249 In the first instance the safety case development process should identify situations that fall under Principle EMC.1. For non-redundant items (eg pressure boundary), the emphasis will be on avoiding defects; for redundant items (eg some support structures) the emphasis might lie more in the redundancy argument than avoidance of defects.

Engineering principles: integrity of metal components and structures: highest reliability components and structures	**Use of scientific and technical issues**	**EMC.2**
The safety case and its assessment should include a comprehensive examination of relevant scientific and technical issues, taking account of precedent when available.		

250 Wherever possible, safety cases should not rely on claims of extremely high structural integrity.

251 A minor failure in a component or structure that forms a principal means of ensuring nuclear safety should not lead to significant radiological hazard.

Engineering principles: integrity of metal components and structures: highest reliability components and structures	**Evidence**	**EMC.3**
Evidence should be provided to demonstrate that the necessary level of integrity has been achieved for the most demanding situations.		

252 To meet Principles EMC.1 and EMC.2, the structural integrity safety case should include appropriate evidence of the following:

a) the use of sound design concepts and proven design features;
b) a detailed design loading specification covering normal operation, plant transients, faults and internal and external hazards;
c) consideration of potential in-service degradation mechanisms;
d) analysis of the potential failure modes for all conditions arising from design specification loadings;
e) use of proven materials;
f) application of high standards of manufacture, including manufacturing inspection and examination;
g) high standards of quality assurance throughout all stages of design, procurement, manufacture, installation and operation;
h) pre-service and in-service examination to detect and characterise defects at a stage before they could develop to cause gross failure;

i) defined limits of operation to ensure the facility is operated within the limits of the safety case. Where appropriate, limits of operation should be supported by protection systems, for instance overpressure protection;

j) in-service monitoring of facility operational parameters;

k) in-service materials monitoring schemes;

l) a process for review of facility operation to ensure the facility is operated and materials performance is within the assumptions of the safety case;

m) a process for review of and response to deviations;

n) a process for review of experience from other facilities, developments in design and analysis methodologies and the understanding of degradation mechanisms for applicability to the component or structure in question;

o) a process for control of in-service repairs or modifications to similar codes, specifications and standards as for original manufacture, taking account of developments since manufacture.

253 The strength and extent of the evidence that is provided to support the safety case should be balanced against the importance of any particular leg that the evidence is supporting.

Other components and structures

254 For components and structures that are not of such major safety significance as to fall under Principle EMC.1 above, the guidance under Principle EMC.3 is still relevant, as are Principles ECS.3 (paragraph 156 f.) and EMC.4 to EMC.34 below that expand on the requirements of Principle EMC.3.

255 The stringency of their application and corresponding depth of assessment should reflect the nuclear safety importance of the item. The structural integrity safety case should clearly set out its position within the wider context of the overall safety case.

256 Where there is a robust consequences argument that shows there are features to mitigate the effects of a component or structure failure, the demands on the structural integrity safety case may be reduced.

257 If there are parallel and independent features to mitigate the effects of component or structure failure and each parallel route contains redundancy, then the reliance on the structural integrity reliability in the overall case may be reduced.

General

258 Components and structures important to safety should be designed, manufactured, installed, examined and inspected using codes, specifications and standards commensurate with their safety classification in accordance with Principle ECS.3 (paragraph 156 f.).

Engineering principles: integrity of metal components and structures: general	**Procedural control**	**EMC.4**
Design, manufacture and installation activities should be subject to procedural control.		

259 Changes in design, manufacture and installation should be carefully controlled through a formal procedure for change. Communication and control of the effects of change across organisation or technical interfaces warrant particular attention.

Engineering principles: integrity of metal components and structures: general	**Defects**	**EMC.5**
It should be demonstrated that safety-related components and structures are both free from significant defects and are tolerant of defects.		

260 The requirements to provide defect-free structures under Principle EMC.5 are expected to be less than for the structures covered by the demanding situations under Principle EMC.1. The precise requirements will depend on the safety significance of the component or structure.

Engineering principles: integrity of metal components and structures: general	Defects	EMC.6
During manufacture and throughout the operational life the existence of defects of concern should be able to be established by appropriate means.		

261 For redundant components and structures, the argument may rely more on the redundancy claim, combined with suitable arguments for avoidance of defects.

Design

Engineering principles: integrity of metal components and structures: design	Loadings	EMC.7
For safety-related components and structures, the schedule of design loadings (including combinations of loadings), together with conservative estimates of their frequency of occurrence should be used as the basis for design against normal operating, plant transient, testing, fault and internal or external hazard conditions.		

Engineering principles: integrity of metal components and structures: design	Requirements for examination	EMC.8
Geometry and access arrangements should have regard to the requirements for examination.		

Engineering principles: integrity of metal components and structures: design	Product form	EMC.9
The choice of product form of metal components or their constituent parts should have regard to enabling examination and to minimising the number and length of welds in the component.		

Engineering principles: integrity of metal components and structures: design	Weld positions	EMC.10
The positioning of welds should have regard to high-stress locations and adverse environments.		

262 For example, other factors being equal:

a) forged austenitic stainless steel is preferred over cast stainless steel because of the better ultrasound transmission in the forged form (aid to volumetric examination);

b) welds and other features that require examination should not be placed within civil structures or so close to other features that inspection is prevented;

c) designs should consider avoiding welds in high neutron radiation locations.

Engineering principles: integrity of metal components and structures: design	Failure modes	EMC.11
Failure modes should be gradual and predictable.		

263 In particular, a metal pressure-retaining boundary should, where appropriate, have characteristics that prevent fast propagation of any defect.

Engineering principles: integrity of metal components and structures: design	Brittle behaviour	EMC.12
Designs in which components of a metal pressure boundary could exhibit brittle behaviour should be avoided.		

Manufacture and installation

264 Manufacture and installation should achieve the design intent and provide a sound basis for pre- and in-service inspections, operation and maintenance. Manufacture and installation should also be consistent with the claims and assumptions that are contained in the safety case.

Engineering principles: integrity of metal components and structures: manufacture and installation	Materials	EMC.13
Materials employed in manufacture and installation should be shown to be suitable for the purpose of enabling an adequate design to be manufactured, operated, examined and maintained throughout the life of the facility.		

265 Welding processes and procedures must be suitable for the base materials being joined and due account should be taken of the operating environment eg high temperatures that can cause creep, or water chemistry that can lead to stress corrosion cracking.

Engineering principles: integrity of metal components and structures: manufacture and installation	Techniques and procedures	EMC.14
Manufacture and installation should use proven techniques and approved procedures to minimise the occurrence of defects that might affect the required integrity of components or structures.		

Engineering principles: integrity of metal components and structures: manufacture and installation	Control of materials	EMC.15
Materials identification, storage and issue should be closely controlled.		

Engineering principles: integrity of metal components and structures: manufacture and installation	Contamination	EMC.16
The potential for contamination of materials during manufacture and installation should be controlled to ensure the integrity of components and structures is not compromised.		

Engineering principles: integrity of metal components and structures: manufacture and installation	Examination during manufacture	EMC.17
Provision should be made for examination during manufacture and installation to demonstrate the required standard of workmanship has been achieved.		

Engineering principles: integrity of metal components and structures: manufacture and installation	Third-party inspection	EMC.18
Manufacture and installation operations should be subject to appropriate third-party independent inspection to check that processes and procedures are being carried out as required.		

Engineering principles: integrity of metal components and structures: manufacture and installation	Non-conformities	EMC.19
Where non-conformities with the procedures are judged to have a detrimental effect on integrity or significant defects are found and remedial work is necessary, the remedial work should be carried out to an approved procedure and should be subject to the same requirements as the original.		

Engineering principles: integrity of metal components and structures: manufacture and installation	Records	EMC.20
Detailed records of manufacturing, installation and testing activities should be made and be retained in such a way as to allow review at any time during subsequent operation.		

266 Pressure vessels, pipework and systems require a pressure test at completion of manufacture and after installation. This is an important test of the strength properties of the materials and section thicknesses. It should not be relied upon as a significant argument for the absence of crack-like defects.

Operation

Engineering principles: integrity of metal components and structures: operation	Safe operating envelope	EMC.21
Throughout their operating life, safety-related components and structures should be operated and controlled within defined limits consistent with the safe operating envelope defined in the safety case.		

267 The parameters of the defined limits should be consistent with the type of component or structure, potential modes of failure and operational considerations.

Engineering principles: integrity of metal components and structures: operation	Material compatibility	EMC.22
Materials compatibility for components should be considered for any operational or maintenance activities.		

Engineering principles: integrity of metal components and structures: operation	Ductile behaviour	EMC.23
For metal pressure vessels and circuits, particularly ferritic steel items, the operating regime should ensure that they display ductile behaviour when significantly stressed.		

268 In particular, for ferritic steel nuclear reactor pressure vessels:

a) clear safety benefits derive from operating on the upper shelf of the toughness transition curve to ensure ductile behaviour;

b) RPVs must, for normal steady-state operation, operate on the upper shelf.

Note: For other conditions, the RPVs should be on the upper shelf. However, where upper shelf conditions cannot be achieved – eg during shutdown, start-up or limited duration transients – it is important that all uncertainties and conditions are considered and that adequate margins on toughness are shown.

Monitoring

269 Monitoring aspects of ageing and degradation are dealt with in Principles EAD.2 (paragraph 195 f.), EAD.3 (paragraph 200 f.) and EAD.4 (paragraph 201 f.).

Engineering principles: integrity of metal components and structures: monitoring	**Operation**	**EMC.24**
Facility operations should be monitored and recorded to demonstrate compliance with the operating limits and to allow review against the safe operating envelope defined in the safety case.		

Engineering principles: integrity of metal components and structures: monitoring	**Leakage**	**EMC.25**
Means should be available to detect, locate, monitor and manage leakage that could indicate the potential for an unsafe condition to develop or give rise to a significant radiological effect.		

Engineering principles: integrity of metal components and structures: monitoring	**Forewarning of failure**	**EMC.26**
Detailed assessment should be carried out where monitoring is claimed to provide forewarning of significant failure.		

270 Assessment should show that the:

a) means of monitoring;
b) frequency of monitoring; and
c) actions to be taken in response to monitoring results;

are consistent with the degradation mechanism in question, the anticipated rate of degradation and the estimated time from detection of degradation to an unsafe state arising. Potential unsafe states to be considered include the consequential effects on structures, systems and components of any leakage, not just the degradation causing the leakage.

Pre- and in-service examination and testing

Engineering principles: integrity of metal components and structures: pre- and in-service examination and testing	**Examination**	**EMC.27**
Provision should be made for examination that is reliably capable of demonstrating that the component or structure is manufactured to the required standard and is fit for purpose at all times during service.		

271 This principle applies to both pre-service and in-service inspection and so does not preclude ongoing confirmation by in-service inspection.

Engineering principles: integrity of metal components and structures: pre- and in-service examination and testing	**Margins**	**EMC.28**
An adequate margin should exist between the nature of defects of concern and the capability of the examination to detect and characterise a defect.		

Engineering principles: integrity of metal components and structures: pre- and in-service examination and testing	Redundancy and diversity	EMC.29
Examination of components and structures should be sufficiently redundant and diverse.		

Engineering principles: integrity of metal components and structures: pre- and in-service examination and testing	Control	EMC.30
Personnel, equipment and procedures should be qualified to an extent consistent with the overall safety case and the contribution of examination to the structural integrity aspect of the safety case.		

272 The nuclear safety classification should be taken into account when determining the appropriate extent of the redundancy, diversity and qualification requirements.

In-service repairs and modifications

Engineering principles: integrity of metal components and structures: in-service repairs and modifications	Repairs and modifications	EMC.31
In-service repairs and modifications should be carefully controlled through a formal procedure for change.		

273 For physical changes to plant, the principles of design, manufacture and installation should be used. Changes to defined limits of operation, monitoring, examination, testing and maintenance should be dealt with as modifications. Incidental consequences of a change should be considered for their significance, not just the direct purpose of the change.

Analysis

Engineering principles: integrity of metal components and structures: analysis	Stress analysis	EMC.32
Stress analysis (including when displacements are the limiting parameter) should be carried out as necessary to support substantiation of the design and should demonstrate the component has an adequate life, taking into account time-dependent degradation processes.		

274 The stress analysis itself should use methods that have been validated and their application should be verified. Where the stress analysis depends on, for instance, thermal or thermal-hydraulic analysis results, those supporting analyses should use methods that are validated with verified application.

Engineering principles: integrity of metal components and structures: analysis	Use of data	EMC.33
The data used in analyses and acceptance criteria should be clearly conservative, taking account of uncertainties in the data and the contribution to the safety case.		

275 In particular, the uncertainties associated with material properties affected by degradation should be taken into account.

276 Where appropriate, studies should be carried out to determine the sensitivity of analytical results to the assumptions made, the data used, and the methods of calculation.

Engineering principles: integrity of metal components and structures: analysis	Defect sizes	EMC.34
Where high reliability is required for components and structures and where otherwise appropriate, the sizes of crack-like defects of structural concern should be calculated using verified and validated fracture mechanics methods with verified application.		

277 The calculated crack sizes of concern should be compared with the results of the manufacturing, pre-service and in-service examinations.

278 Initiation fracture toughness should be the basis for analysis of frequent loading conditions. For fracture analyses of infrequent fault or hazard loading conditions, results using initiation fracture toughness may be supplemented with results using fracture toughness based on limited amounts of stable tearing. In this case, there must be valid materials fracture toughness data up to at least the limited extent of tearing used. In all cases toughness values used in analyses should be appropriate lower bounds. Thermal and residual stresses should be considered in fracture analyses and the nature of the residual stresses (primary or secondary) appropriately included.

279 Where analysis is conducted for dynamic loading events (where the component or structure mass and stiffness are both required to characterise the response to a loading, often a fault or hazard condition), the time-domain, frequency-domain or other methods used and modelling assumptions should be appropriate. Where necessary, materials data used should take account of rate effects and any simplifications should be conservative and justified. Where dynamic load effects are evaluated by correlation with test results (eg impact tests), the adequacy of the tests, the limit criteria and any statistical treatment should be validated and verified as appropriate.

Civil engineering

280 This part of the SAPs is concerned with the engineering assessment of the integrity of structural components such as steel-framed buildings, crane supports, concrete structures, masonry, foundations, embankments, slopes, river and coastal defences. Any specific differences are stated in the appropriate principles. Where a structural component also forms containment, the principles in the Containment and ventilation sub-section (paragraph 418 ff.) are also relevant. When assessing very high integrity metal civil structures, inspectors may need to consider appropriate principles in the sub-section on Integrity of metal components and structures (paragraph 238 ff.).

281 The general lack of sufficient reliability data for structural components leads to design being based primarily on good practice, typically as set out in design standards, material specifications and construction practice. Some design standards are specifically for the design of nuclear safety-related structures, dealing with the structural forms most commonly encountered in the nuclear industry and with issues peculiar to the nuclear industry. Other design standards may be for the design of structures in general.

Engineering principles: civil engineering	Functional performance	ECE.1
The required safety functional performance of the civil engineering structures under normal operating and fault conditions should be specified.		

Engineering principles: civil engineering	Independent arguments	ECE.2
For structures requiring the highest levels of reliability, several related but independent arguments should be used.		

282 The arguments should be based on the following:

a) the use of sound design concepts and proven design features;
b) the use of specific nuclear design standards appropriate to the circumstances, where such a standard exists;
c) a detailed schedule of structural actions for both serviceability and ultimate limit states, covering normal operation, plant transients, faults and internal and external hazards;
d) consideration of potential in-service degradation mechanisms;
e) the analysis of potential failure modes for conditions arising from design basis faults;
f) the use of proven materials;
g) the application of high standards, verified by inspection, of the construction and of the materials used;
h) high standards of quality assurance throughout all stages of design, procurement, construction and operation;
i) pre-service and in-service inspection to detect defects that have the potential for causing or developing into a failure mode; and
j) for structures for which the consequence of failure would be high, predictable, gradual and detectable failure modes for severe loadings.

283 Sufficiently high margins may be provided to ensure that, for structure types that are inherently less ductile, failure would be extremely unlikely to occur for credible initiating events.

284 For structures that are not of major safety significance, the list of requirements in paragraph 282 above remains relevant, though the stringency of their application should reflect the safety classification of the item.

285 Structures, systems and components important to safety should be designed, constructed, inspected and maintained to the standards commensurate with their safety classification.

Engineering principles: civil engineering	**Defects**	**ECE.3**
It should be demonstrated that safety-related structures are sufficiently free of defects so that their safety functions are not compromised, that identified defects are tolerable, and that the existence of defects that could compromise their safety function can be established through their life-cycle.		

Investigations

Engineering principles: civil engineering: investigations	**Natural site materials**	**ECE.4**
Investigations should be carried out to determine the suitability of the natural site materials to support the foundation loadings specified for normal operation and fault conditions.		

286 Investigations should follow codes and standards applicable to the structures proposed.

Engineering principles: civil engineering: investigations	**Geotechnical investigation**	**ECE.5**
The design of foundations should utilise information derived from geotechnical site investigation.		

287 The information should include ground-water conditions, contamination conditions, soil dynamic properties and any potential for liquefaction or cyclic mobility. Similar investigation may be required for slopes and for material retained by walls etc.

Design

Engineering principles: civil engineering: design	Loadings	ECE.6
For safety-related structures, load development and a schedule of load combinations within the design basis together with their frequency should be used as the basis for the design against operating, testing and fault conditions.		

288 For more severe loadings of structures that provide a principle means of ensuring nuclear safety, predicted failure modes should be gradual, ductile and, for slowly developing loads, detectable.

289 The data from the devices and measurements referred to in paragraph 298 should be used during the periodic reviews of the safety case or in post-event analysis for civil structures.

Engineering principles: civil engineering: design	Foundations	ECE.7
The foundations should be designed to support the structural loadings specified for normal operation and fault conditions.		

Engineering principles: civil engineering: design	Inspectability	ECE.8
Designs should allow key load bearing elements to be inspected and, if necessary, maintained.		

290 The design should take account of hindrances to inspection such as radiation, burial and access difficulties.

291 If elements cannot be inspected, the design should demonstrate high confidence that the performance of these elements will remain adequate for the design life.

Engineering principles: civil engineering: design	Earthworks	ECE.9
The design of embankments, natural and excavated slopes, river levees and sea defences close to a nuclear facility should be such so as to protect and not to jeopardise the safety of the facility.		

Engineering principles: civil engineering: design	Ground-water	ECE.10
The design should be such that the facility remains stable against possible changes in the ground-water conditions.		

Engineering principles: civil engineering: design	Naturally occurring gases	ECE.11
The design should take account of the possible presence of naturally occurring explosive gases or vapours in underground structures such as tunnels, trenches and basements.		

Structural analysis and model testing

Engineering principles: civil engineering: structural analysis and model testing	Structural analysis and model testing	ECE.12
Structural analysis or model testing should be carried out to support the design and should demonstrate that the structure can fulfil its safety functional requirements over the lifetime of the facility.		

292 The analysis or model testing should use methods and data that have been validated and verified.

Engineering principles: civil engineering: structural analysis and model testing	Use of data	ECE.13
The data used in any analysis should be such that the analysis is demonstrably conservative.		

293 Uncertainties associated with structural analysis, structural capacity, and the properties of material affected by degradation properties should be taken into account.

Engineering principles: civil engineering: structural analysis and model testing	Sensitivity studies	ECE.14
Studies should be carried out to determine the sensitivity of analytical results to the assumptions made, the data used, and the methods of calculation.		

Engineering principles: civil engineering: structural analysis and model testing	Validation of methods	ECE.15
Where analyses have been carried out on civil structures to derive static and dynamic structural loadings for the design, the methods used should be adequately validated.		

294 The method should be assessed to ascertain whether the controlling physical equations have been correctly implemented into computer code, or, in the case of hand calculations, correctly incorporated into the calculational procedures. Calculations should be validated in proportion to where the calculation fits into the overall safety case.

295 Validation may need to consider the limits of application of the calculational method, the structural representation in the model, comparison with other calculational methods, the level of quality assurance and user proficiency.

296 Calculations of beyond design basis conditions involve the prediction of extreme physical behaviour and the calculational methods used are often not amenable to rigorous validation. In such cases the results should be reviewed to ensure that they sensibly reflect the expected physical performance in broad terms.

Construction

Engineering principles: civil engineering: construction	Materials	ECE.16
Civil construction materials should be compliant with the design methodologies used, and shown to be suitable for the purpose of enabling the design to be constructed, operated, inspected and maintained throughout the life of the facility.		

Engineering principles: civil engineering: construction	Prevention of defects	ECE.17
The construction should use appropriate materials, proven techniques and approved procedures to minimise the occurrence of defects that might affect the required integrity of structures.		

Engineering principles: civil engineering: construction	Inspection during construction	ECE.18
Provision should be made for inspection during construction to demonstrate that the required standard of workmanship has been achieved.		

Engineering principles: civil engineering: construction	Non-conformities	ECE.19
Where construction non-conformities are judged to have a detrimental effect on integrity or significant defects are detected, remedial measures should achieve the original design intent.		

297 The acceptability of the work or the need for remedial work should be managed through a construction concession in accordance with quality assurance procedures, or through a design change such that the original design intent is achieved.

Monitoring

298 Principle ESR.1 (paragraph 364 f.) will apply to devices and measurements that do not provide direct protection against a hazardous event but that detect and record such events or that may provide safety significant information. For example, seismic detectors and the recording of meteorological conditions are of particular relevance.

In-service inspection and testing

Engineering principles: civil engineering: in-service inspection and testing	In-service inspection and testing	ECE.20
Provision should be made for inspection during service that is capable of demonstrating that the structure can meet its safety functional requirements.		

Engineering principles: civil engineering: in-service inspection and testing	Proof pressure tests	ECE.21
Pre-stressed concrete pressure vessels and containment structures should be subjected to a proof pressure test, which may be repeated during the life of the facility.		

299 Other structural components, such as piles and rock anchors, should be proof tested as required by the safety consequences of their failure or by the uncertainties in their design and/or construction.

Engineering principles: civil engineering: in-service inspection and testing	Leak tightness	ECE.22
Civil engineering structures that retain or prevent leakage should be tested against the leak tightness requirements prior to operation to demonstrate that the design intent has been met.		

300 Where appropriate, drainage systems should be provided to confirm the continuing containment integrity of the structures or to detect, locate, collect, quantify and where possible allow repair of leakages.

Engineering principles: civil engineering: in-service inspection and testing	**Inspection of sea and river flood defences**	**ECE.23**
Provision should be made for the routine inspection of sea and river flood defences to determine their continued fitness for purpose.		

301 This provision should cover such aspects as erosion and degradation of materials and structures that protect the site. Provision should be made for non-routine inspection following extreme weather or other indications of degradation.

Engineering principles: civil engineering: in-service inspection and testing	**Settlement**	**ECE.24**
There should be arrangements to monitor foundation settlement of major facilities during and after construction, and the information should be fed back into design reviews.		

302 The safety case should define other parameters, such as tendon loads and ground-water levels, that need to be monitored and compared with action levels.

Graphite components and structures

303 Due to differences in design and safety functions, graphite core structures in some instances may be defect tolerant, although in others safety functions may exhibit low defect tolerance. Therefore the principles need to cater for a spectrum of safety performance.

304 Safety cases for graphite components and structures are expected to present a multi-legged approach, based upon independent and diverse arguments. The rigour of application and robustness of the supporting data and information should be based upon the safety classification of the graphite components and structures. The multi-legged arguments, when taken together with the various elements of established engineering practice, should provide defence in depth.

305 Novel approaches may be acceptable provided they are supported by appropriate research and development, and the novel features are tested to show they meet design requirements before coming into service, and are monitored during service.

306 Safety cases for graphite components or structures are expected to fall into one or more of the following four categories:

a) *those that form a principal means of ensuring nuclear safety;*
b) *those where there is inadequate reliability data;*
c) *those where the design basis analysis discounts failure of the graphite component or structure to perform its safety function because the assumed initiating fault frequency is lower than about 1 x 10^{-5} pa (see Principle FA.5 (paragraph 513 f.));*
d) *those that do not form a principal means of ensuring nuclear safety.*

Engineering principles: graphite components and structures	Safety cases	EGR.1

The safety case should demonstrate that either:

a) the graphite component or structure is free of defects that could impair its safety functions;

OR

b) the safety functions of the graphite components or structure are tolerant of those defects that might be present.

307 The safety case should:

a) include a comprehensive examination of all relevant scientific, technological and engineering issues;

b) incorporate a rigorous analysis of the effect of uncertainty and data scatter on any predictions; and

c) take due account of relevant precedent; and include, where appropriate, independent expert peer review.

308 To demonstrate achievement of Principle EGR.1 the safety case should develop multi-legged arguments based upon the following:

a) design;

b) manufacture, construction and commissioning;

c) component and structure condition assessment (CSCA);

d) defect tolerance assessment;

e) analysis of radiological consequences of defectiveness;

f) monitoring; and

g) examination, inspection, surveillance, sampling and testing.

309 Principles expanding on paragraph 308 are presented below; these should be applied having due regard for the importance of the safety case for graphite components and structures within the overall safety case.

310 For graphite components and structures that do not form a principal means of ensuring nuclear safety, the list of requirements presented below is still relevant, however the stringency of its application and corresponding depth of assessment should reflect the nuclear safety importance of the item. The safety case for such graphite components or structures should clearly set out its position within the wider context of the overall safety case. Where there is a robust consequences argument that shows there are facility design features to mitigate the effects of a component or structure failure, the demands on the graphite safety case may be reduced. If there are parallel and independent design features to mitigate the effects of component or structure failure and each parallel route contains redundancy, then the reliance on the graphite safety case may be reduced.

311 A defect in a graphite component is a deviation from design specification in a component or structure. Not all defects pose a threat to safety. A defect that could call into question the safety function of a component or structure is termed a 'significant deviation from design specification'.

General

312 The metal component principles referred to in the paragraphs below are relevant to graphite components but the word 'installation' should be read as 'construction'.

313 Principles EMC.3 (paragraph 251 f.), EMC.4 (paragraph 258 f.), EMC.21 (paragraph 266 f.), EMC.32 to EMC.34 (paragraph 273 ff.) and Principles EDR.1 (paragraph 169 f.), EAD.1 and EAD.4 (paragraph 193 ff.), EKP.1 (paragraph 135 f.), and ECS.2 to ECS.5 (paragraph 152 ff.) are relevant to graphite components and structures and should be considered.

314 A general requirement throughout is that analytical models should use methods that have been verified and validated. This applies equally well to both component condition assessment and defect tolerance assessment.

Design

315 Principles EMC.7 and EMC.8 (paragraph 261 ff.) are relevant to graphite components and structures and should be considered.

Engineering principles: graphite components and structures: design	**Demonstration of tolerance**	**EGR.2**
The design should demonstrate tolerance of graphite component and structure safety functions to: a) ageing processes; b) the schedule of design loadings; and c) potential mechanisms of formation of defects arising from design specification loadings.		

Engineering principles: graphite components and structures: design	**Monitoring**	**EGR.3**
There should be appropriate monitoring systems to enable the graphite structure to be maintained within its safe-operating envelope for the duration of the life of the installation.		

Engineering principles: graphite components and structures: design	**Inspection and surveillance**	**EGR.4**
Features should be provided to: a) facilitate inspection during manufacture and service; and b) permit the inclusion of surveillance samples for monitoring of materials behaviour.		

Manufacture, construction and commissioning

316 Principles EMC.13 to EMC.20 (paragraph 264 ff.) are relevant to graphite component and structures and should be considered.

Engineering principles: graphite components and structures: manufacture, construction and commissioning	**Manufacturing records**	**EGR.5**
A record should be made of the manufacturing case histories.		

Engineering principles: graphite components and structures: manufacture, construction and commissioning	**Location records**	**EGR.6**
A record should be made of the position of individual components in the structure during construction.		

317 Records should be maintained to enable traceability of individual components to manufacturing batch, test certificate and component inspection results.

Component and structure condition assessment (CSCA)

318 Some graphite components may fail during the lifetime of gas-cooled reactors. The mode of failure and the spatial and temporal distribution need to be estimated to demonstrate that the cores will continue to perform their safety functions. The CSCA leg of a safety case should present the results of analyses to predict the condition of components and structures.

Engineering principles: graphite components and structures: component and structure condition assessment	Materials properties	EGR.7
Analytical models should be developed to enable the prediction of graphite component (and structure as applicable) material properties, displacements, stresses, loads and condition.		

319 Such models should consider interactions between graphite components and with other components and structures such as fuel assemblies, control rods, and core support structures. Models should initially give best estimate predictions. An understanding of the effect of uncertainty, and data scatter, should be investigated by either sensitivity studies or probabilistic approaches, particularly in relation to identification of any potential cliff-edge effects.

320 For components or structures important for safety, and where it is not possible to directly qualify them under the most onerous conditions, reference data from commissioning, model, rig or experimental tests should be established to justify extrapolations from in-service test results.

Engineering principles: graphite components and structures: component and structure condition assessment	Predictive models	EGR.8
Predictive models should be shown to be valid for the particular application and circumstances by reference to established physical data, experiment or other means.		

Engineering principles: graphite components and structures: component and structure condition assessment	Materials properties data	EGR.9
Extrapolation and interpolation from available materials properties data should be undertaken with care, and data and model validity beyond the limits of current knowledge should be robustly justified.		

321 Materials data should be available that bounds graphite component operational exposure conditions by an adequate margin.

Defect tolerance assessment

Engineering principles: graphite components and structures: defect tolerance assessment	Effect of defects	EGR.10
An assessment of the effect of defects in graphite components and structures should be undertaken to establish the tolerance of their safety function during normal operation, plant transients, faults and hazards.		

322 Possible degradation and failure mechanisms should be taken into account and local and global effects of component and structural defectiveness should be considered.

323 It may be necessary to consider a consequences case (taking into account the effect of graphite component and structure defectiveness on the fault analysis) if the defect tolerance assessment is unable to clearly demonstrate that safety functionality will be achieved under reasonably foreseeable conditions.

Engineering principles: graphite components and structures: defect tolerance assessment	Safe working life	EGR.11
The safe working life of graphite components and structures should be evaluated.		

324 There should be an adequate margin between the intended operational life and the predicted safe working life of graphite components and structures. Safety margins should take due account of uncertainty in life predictions.

Engineering principles: graphite components and structures: defect tolerance assessment	Margins	EGR.12
There should be an adequate margin between the operating and fault envelope and any assumed condition over the full, intended lifetime with allowance for uncertainty.		

325 If component or structure defectiveness is shown, or predicted to occur, effects on safety functions should be shown to be progressive with the possibility of disruptive failures, without adequate forewarning, being remote.

Engineering principles: graphite components and structures: defect tolerance assessment	Use of data	EGR.13
Data used in the analysis should be soundly based and demonstrably conservative. Studies should be undertaken to establish the sensitivity to analysis parameters.		

Monitoring

326 Principles EMC.24 and EMC.26 (paragraph 269 ff.) are relevant to monitoring of the safety functions of graphite components and structures and should be considered.

Engineering principles: graphite components and structures: monitoring	Monitoring systems	EGR.14
The design, manufacture, operation, maintenance, inspection and testing of monitoring systems should be commensurate with the required duty and reliability claimed in the safety case.		

327 Monitoring should be performed continuously or at appropriate intervals, to ensure the timely identification of degradation.

328 Results of monitoring should be evaluated and reviews undertaken periodically.

329 Monitoring systems should enable trending and evaluation of behaviour with time and the development of suitable and sufficient warning and investigation criteria.

330 Arrangements should enable timely response to mitigate untoward trends in monitoring parameters before safety functions are impaired.

Examination, inspection, surveillance, sampling and testing

331 Principles EMC.25 to EMC.30 (paragraph 269 ff.) and EMT.1 to EMT.8 (paragraph 186 ff.) are also relevant and should be considered.

Engineering principles: graphite components and structures: examination, inspection, surveillance, sampling and testing	Extent and frequency	EGR.15
In-service examination, inspection, surveillance, and sampling should be of sufficient extent and frequency to give sufficient confidence that degradation of graphite components and structures will be detected well in advance of any defects affecting safety function.		

332 Testing undertaken, either during a periodic shutdown or of samples removed from the reactor, should be in accordance with appropriate national or international standards. Where no such standards exist, adequate arrangements should be developed to ensure the consistency of testing procedures and the validity of the tests.

Safety systems and safety-related instrumentation

333 Nuclear facilities use a variety of systems concerned with safety. At the highest level of importance there are the safety systems. These are provided to detect potentially dangerous plant failures or conditions and to implement appropriate safety actions. The 'safety systems' principles below apply to the engineered systems upon which any safety function depends. They encompass, therefore:

a) protection systems that sense unsafe conditions in the facility and automatically initiate the operation of appropriate systems for maintaining a safe condition;

b) safety actuation systems, such as heat removal systems and reactor shutdown systems that are brought in to assure the preservation of a safe state condition within the facility; and

c) essential services (or safety system support features) that provide electrical or pneumatic power, cooling and lubrication required by protection systems and the safety actuation systems.

334 The principles in this section apply to both active and passive safety systems. However, in the case of passive safety systems, not all of the principles may apply or their application may be more restricted because of the inherent features of such systems.

335 Additional principles that should also be applied are to be found in the sub-sections following the key principles (paragraph 148 ff.). Protection and safety actuation systems may also be served by essential services (or safety system support features) and additional principles relating to these are to be found in the sub-section on Essential services (paragraph 370 ff.).

Safety systems

Engineering principles: safety systems	Requirement for safety systems	ESS.1
All nuclear facilities should be provided with safety systems that reduce the frequency or limit the consequences of fault sequences, and that achieve and maintain a defined safe state.		

336 A reactor should be provided with safety systems that can shut it down safely in normal operating and fault conditions and maintain it in the shutdown condition. There should be a margin of reactivity that allows for systematic changes and uncertainties in nuclear characteristics, variations in plant state and other processes or mechanisms that might affect the reactivity of the core, even for the most reactive conditions of the core.

Engineering principles: safety systems	Determination of safety system requirements	ESS.2
The extent of safety system provisions, their functions, levels of protection necessary to achieve defence in depth and required reliabilities should be determined.		

337 The design basis (Principles FA.4 *(paragraph 512 f.)* and FA.9 *(paragraph 525 f.)*) and probabilistic safety (Principle FA.14 *(paragraph 540 f.)*) analyses (or other suitable analyses) should determine the safety system provisions, functions and required reliabilities.

Engineering principles: safety systems	Monitoring of plant safety	ESS.3
Adequate provisions should be made to enable the monitoring of the plant state in relation to safety and to enable the taking of any necessary safety actions.		

338 Monitoring provisions should be classified as safety or safety-related systems as appropriate and should be made:

a) in a central control location; and

b) at emergency locations (preferably a single point) that will remain habitable during foreseeable facility emergencies.

Engineering principles: safety systems	Adequacy of initiating variables	ESS.4
Variables used to initiate a safety system action should be identified and shown to be sufficient for the purpose of protecting the facility.		

339 The limiting conditions for these variables for which the safety system has been qualified should be specified. The safety system should be designed to respond so that these limiting conditions are not transgressed.

Engineering principles: safety systems	Plant interfaces	ESS.5
The interfaces required between a safety system and the plant to detect a fault sequence and bring about a safe facility state should be engineered by means that have a direct, known, timely and unambiguous relationship with plant behaviour.		

340 For example, if the action is to initiate a coolant flow then the flow should be measured directly and not inferred from measurement of power to actuation devices such as pumps, valves etc.

Engineering principles: safety systems	Adequacy of variables	ESS.6
Where it is not possible to use a directly related variable to detect a fault sequence, the variable chosen should have a known relationship with the fault sequence.		

341 The physical and temporal coupling should be as close as possible. Any mechanism for the transmission of misleading information should be analysed and appropriate corrective measures adopted.

Engineering principles: safety systems	Diversity in the detection of fault sequences	ESS.7
The protection system should employ diversity in the detection of fault sequences, preferably by the use of different variables, and in the initiation of the safety system action to terminate the sequences.		

342 This principle applies in particular to UK civil nuclear power reactor safety systems and in particular to high integrity safety systems.

Engineering principles: safety systems	Automatic initiation	ESS.8
A safety system should be automatically initiated and normally no human intervention should be necessary following the start of a requirement for protective action.		

343 The design should be such that facility personnel cannot negate correct safety system action at any time, but they can initiate safety system functions and perform necessary actions to deal with circumstances that might prejudice safety.

Engineering principles: safety systems	Time for human intervention	ESS.9
Where human intervention is necessary following the start of a requirement for protective action, then the time before such intervention is required should be demonstrated to be sufficient.		

344 The practice on UK civil nuclear power reactor facilities is that no human intervention should be necessary for approximately 30 minutes following the start of a requirement for protective action. It would be expected that this practice continues to be met.

Engineering principles: safety systems	Definition of capability	ESS.10
The capability of a safety system, and of each of its constituent sub-systems and components, should be defined.		

345 The capability should exceed by a clear margin the maximum service requirement(s) including the environmental envelope. The selected margin should make due allowance not only for uncertainties in plant characteristics, but also for the effects of foreseeable degradation mechanisms.

Engineering principles: safety systems	Demonstration of adequacy	ESS.11
The adequacy of the system design as the means of achieving the specified function and reliability should be demonstrated for each system.		

346 A ‘safety schedule’ (also known as a fault and protection schedule) should be provided that lists all postulated faults and hazards with unacceptable consequences. The schedule should include all initiating faults with their frequencies and consequences, the safety systems and beneficial safety-related systems involved for each initiating fault and the overall protection claim.

Engineering principles: safety systems	Prevention of service infringement	ESS.12
Adequate provisions should be made to prevent the infringement of any service requirement of a safety system, its sub-systems and components.		

347 Infringement of any service would include removal or degradation of support services such as power supplies, instrument air, environment etc.

348 Where prevention, or acceptably low likelihood, of infringement cannot be demonstrated, features should be incorporated to ensure a fail-safe outcome.

Engineering principles: safety systems	Confirmation to operating personnel	ESS.13
There should be a direct means of confirming to operating personnel: a) that a demand for safety system action has arisen; b) that the safety actuation systems have operated fully; and c) whether any limiting condition for which the safety system has been qualified has been exceeded.		

349 Such means should be clear and preferably sourced from the system carrying out the action.

Engineering principles: safety systems	Prohibition of self-resetting of actions and alarms	ESS.14
Safety system actions and associated alarms should not be self-resetting, irrespective of the subsequent state of the initiating fault.		

Engineering principles: safety systems	Alteration of configuration, operational logic or associated data	ESS.15
No means should be provided, or be readily available, by which the configuration of a safety system, its operational logic or the associated data (trip levels etc) may be altered, other than by specifically engineered and adequately secured maintenance/testing provisions used under strict administrative control.		

Engineering principles: safety systems	No dependency on external sources of energy	ESS.16
Where practicable, following a safety system action, maintaining a safe facility state should not depend on an external source of energy.		

350 For this principle an external source of energy means external to a safety system.

Engineering principles: safety systems	Fault identification and assurance of safe state	ESS.17
Foreseeable faults within a safety system that could cause any single plant variable, or combination of variables, to change to significantly less safe values should be identified and, as necessary, avoidance measures or appropriate protective features provided.		

351 This principle is aimed at ensuring that the plant remains safe following the occurrence of foreseeable safety system faults. This includes, but is not limited to, the placement of the safety system in a fail-safe state, where practicable and achievable, following the detection of safety system faults.

Engineering principles: safety systems	Failure independence	ESS.18
No fault, internal or external hazard should disable a safety system.		

352 Safety systems should be physically separate, independent, isolated from other systems, including safety-related systems, and share no equipment or services. There should be adequate segregation between independent parts of the safety system (including pipework and cabling) and also between a safety system and other facility equipment that, in the event of a fault, might jeopardise the safe working of the safety system.

Engineering principles: safety systems	Dedication to a single task	ESS.19
A safety system should be dedicated to the single task of performing its safety function.		

353 Where it is necessary for other functions to be encompassed, the whole system should be classified as a safety system and the safety function should not be jeopardised by the other functions.

Engineering principles: safety systems	Avoidance of connections to other systems	ESS.20
Connections between any part of a safety system (other than the safety system support features) and a system external to the plant should be avoided.		

354 If connections external to the plant cannot be avoided, for electrical, electronic or computer-based safety systems they should be restricted in function to that of monitoring only, and should incorporate adequate isolation features so that no fault associated with that equipment or its connections would jeopardise the function of the safety system.

Engineering principles: safety systems	Reliability	ESS.21
The design of a safety system should avoid complexity, apply a fail-safe approach and incorporate the means of revealing internal faults from the time of their occurrence.		

355 Where this principle cannot be achieved because of the use of complex hardware, the elements of a safety demonstration should be determined. The demonstration should include:

a) a comprehensive examination of all the relevant scientific and technical issues;

b) a review of precedents set under comparable circumstances in the past;

c) an independent third-party assessment in addition to the normal checks and conventional design;

d) periodic review of further developments in technical information, precedent and best practice.

356 The nature of some systems may be such that it is not possible to reveal all faults until the time of a test, eg in the case of fluid or mechanical systems. In such cases, in-service or periodic testing will be the sole means available to support reliability claims for the equipment, see Principle EMT.6 *(paragraph 189 f.)*.

Engineering principles: safety systems	Avoidance of spurious operation	ESS.22
A safety system should avoid spurious operation at a frequency that might directly or indirectly degrade safety.		

Engineering principles: safety systems	Allowance for unavailability of equipment	ESS.23
In determining the safety system provisions, allowance should be made for the unavailability of equipment.		

357 Sources of equipment unavailability will include:

a) testing and maintenance;

b) non-repairable equipment failures; and

c) unrevealed failures.

Engineering principles: safety systems	Minimum operational equipment requirements	ESS.24
The minimum amount of operational safety system equipment for which any specified facility operation will be permitted should be defined and shown to meet the single failure criterion.		

Engineering principles: safety systems	Safety system vetoes	ESS.25
The vetoing or the taking out of service of any safety system function should be avoided.		

358 Where such action is proposed, each need should be justified and the adequacy of its implementation demonstrated. In a safety system comprising several redundant or diverse sub-systems no single action should affect more than one sub-system.

Engineering principles: safety systems	Maintenance and testing	ESS.26
Maintenance and testing of a safety system should not initiate a fault sequence.		

359 For a computer-based safety system the technology is not amenable to traditional methods of reliability assessment. The following principle presents the elements of a procedure to demonstrate the adequacy of a safety system using computer-based technology. The safety demonstration for the hardware elements of such systems should include the items listed in paragraph 355.

Engineering principles: safety systems	Computer-based safety systems	ESS.27
Where the system reliability is significantly dependent upon the performance of computer software, the establishment of and compliance with appropriate standards and practices throughout the software development life-cycle should be made, commensurate with the level of reliability required, by a demonstration of 'production excellence' and 'confidence-building' measures.		

360 'Production excellence' requires a demonstration of excellence in all aspects of production, covering initial specification through to the finally commissioned system, comprising the following elements:

a) Thorough application of technical design practice consistent with current accepted standards for the development of software for computer-based safety systems.

b) Implementation of an adequate quality assurance programme and plan in accordance with appropriate quality assurance standards.

c) Application of a comprehensive testing programme formulated to check every system function, including:

- prior to installation on site, the verification of all phases of the system production process and the validation of the integrated system against its requirements specification by persons not involved in the specification and design activities;
- following installation on site, a demonstration that the safety system, in conjunction with the plant, performs to requirements, this demonstration being devised by persons other than the system specifiers, designers or manufacturers; and
- a programme of dynamic testing, applied to the complete system, that is capable of demonstrating that the system meets its reliability requirements.

361 Independent 'confidence-building' should provide an independent and thorough assessment of a safety system's fitness for purpose. This comprises the following elements:

a) Complete and preferably diverse checking of the finally validated production software by a team that is independent of the systems suppliers, including:

- independent product checking providing a searching analysis of the product;
- independent checking of the design and production process, including activities needed to confirm the realisation of the design intention; and

b) Independent assessment of the test programme, covering the full scope of test activities.

362 Should weaknesses be identified in the production process, compensating measures should be applied to address these. The type of compensating measures will depend on, and should be targeted at, the specific weaknesses found.

Control and instrumentation of safety-related systems

363 *Besides the safety systems identified above there are other systems, known as safety-related systems that, while having a significant influence on safety, do not have a direct fault sequence termination function. The control and instrumentation of safety-related systems (which includes the facility control system, indicating and recording instrumentation, alarm systems and communications systems) have a close relationship with safety systems and are covered in this sub-section.*

364 *There is also a group of systems used for the detection of criticality incidents, ie incidents involving the inadvertent accumulation into a critical mass of material that can undergo nuclear fission. A criticality incident detection system is strictly an alarm system that provides an additional layer of safety by causing prompt evacuation of personnel and therefore limitation of doses. Such systems are regarded as sufficiently important to warrant the provision of high reliability systems and are therefore classed as safety-related systems.*

Engineering principles: control and instrumentation of safety-related systems	**Provision in control rooms and other locations**	**ESR.1**
Suitable and sufficient safety-related system control and instrumentation should be available to the facility operator in a central control room, and as necessary at appropriate locations on the facility.		

365 Principle EHF.7 *(paragraph 382 f.)* on user interfaces is also relevant to this principle.

366 The provisions should encompass normal operation, abnormal operation and postulated fault conditions including, where reasonably practicable, severe accidents. The equipment should include indicating and recording instrumentation and controls as appropriate.

Engineering principles: control and instrumentation of safety-related systems	**Performance requirements**	**ESR.2**
The reliability, accuracy, stability, response time, range and, where appropriate, the readability of instrumentation, should be adequate for its required service.		

Engineering principles: control and instrumentation of safety-related systems	**Provision of controls**	**ESR.3**
Adequate and reliable controls should be provided to maintain variables within specified ranges.		

Engineering principles: control and instrumentation of safety-related systems	**Minimum operational equipment**	**ESR.4**
The minimum control and instrumentation for which facility operation may be permitted should be specified and its adequacy substantiated.		

Engineering principles: control and instrumentation of safety-related systems	**Standards for computer based equipment**	**ESR.5**
Where computers or programmable devices are used in safety-related systems, evidence should be provided that the hardware and software are designed, manufactured and installed to appropriate standards.		

Engineering principles: control and instrumentation of safety-related systems	Power supplies	ESR.6
Safety-related system control and instrumentation should be operated from power supplies whose reliabilities and availabilities are consistent with the functions being performed.		

367 In the cases of monitoring, warning and communication functions, the supplies should be uninterruptible.

Engineering principles: control and instrumentation of safety-related systems	Communications systems	ESR.7
Adequate communications systems should be provided to enable information and instructions to be transmitted between locations and to provide external communications with auxiliary services and such other organisations as may be required.		

368 These communication systems should not have any adverse effect on safety systems, or safety-related systems.

Engineering principles: control and instrumentation of safety-related systems	Monitoring of radioactive substances	ESR.8
Instrumentation should be provided to enable monitoring of the locations and quantities of radioactive substances that may escape from their engineered environment.		

Engineering principles: control and instrumentation of safety-related systems	Response of control systems to normal plant disturbances	ESR.9
Control systems should respond in a timely and stable manner to normal plant disturbances without causing demands on safety systems.		

Engineering principles: control and instrumentation of safety-related systems	Demands on safety systems in the event of control system faults	ESR.10
Faults in control systems and other safety-related instrumentation should not cause an excessive frequency of demands on a safety system.		

369 An analysis should be provided that identifies the foreseeable ways in which control systems under fault conditions, including multiple control faults, could generate demands on safety systems.

Essential services

370 Essential services are those resources necessary to maintain the safety systems in an operational state at all times, and they may also provide supplies to safety-related systems. The services may include electricity, gas, water, compressed air, fuel and lubricants, and may need to satisfy two requirements. The first requirement is to provide a guaranteed, or non-interruptible short-term supply to ensure continuity until the long-term essential supply is established, and the second is to ensure that there is adequate capacity to supply the service until normal supplies can be restored. The following principles are additional to the safety system and safety-related instrumentation principles.

Engineering principles: essential services	Provision	EES.1
Essential services should be provided to ensure the maintenance of a safe plant state in normal operation and fault conditions.		

Engineering principles: essential services	Sources external to the site	EES.2
Where a service is obtained from a source external to the nuclear site, that service should also be obtainable from a back-up source on the site.		

Engineering principles: essential services	Capacity, duration, availability and reliability	EES.3
Each back-up source should have the capacity, duration, availability and reliability to meet the maximum requirements of its dependent systems.		

371 It should provide that service for a sufficient period of time to allow the facility to be brought to a safe state and maintained in that state until such time as the normal supply is restored.

Engineering principles: essential services	Sharing with other plants	EES.4
Where essential services are shared with other plants on a multi-facility site, the effect of the sharing should be taken into account in assessing the adequacy of the supply.		

372 It should be shown that the safety requirements for all facilities are met for all operational states (including maintenance) and fault conditions.

Engineering principles: essential services	Cross-connections to other services	EES.5
The capacity of the essential services to meet the demands of the supported safety functional requirement(s) should not be undermined by making cross-connections to services provided for non-safety functions.		

373 Where such cross-connections are necessary, provisions should be made to isolate the essential services from these other services so that the essential services can meet their safety functional requirements.

Engineering principles: essential services	Alternative sources	EES.6
Alternative sources of essential services should be designed so that their reliability would not be prejudiced by adverse conditions in the services to which they provide a back-up.		

Engineering principles: essential services	Protection devices	EES.7
Protection devices provided for essential service components or systems should be limited to those that are necessary and that are consistent with facility requirements.		

374 Possible actions of protection devices should be taken into account in reliability assessments.

Engineering principles: essential services	Sources external to the site	EES.8
Where a source external to the nuclear site is employed as the only source of the essential services needed to provide adequate protection, the specification and in particular the availability and reliability should be the same as for an on-site source.		

Engineering principles: essential services	Loss of service	EES.9
Essential services should be designed so that the simultaneous loss of both normal and back-up services will not lead to unacceptable consequences.		

Human factors

375 *A nuclear facility is a complex socio-technological system that comprises both engineered and human components. The human contribution to nuclear safety can be positive or negative, and may be made during facility design, construction, commissioning, operation, maintenance and decommissioning. A systematic approach to understanding the factors that affect human performance, and minimising the potential for human error to contribute to faults, should therefore be applied throughout the entire facility life-cycle. Assessments of the way in which individual, team and organisational performance can impact upon nuclear safety should influence the design of the plant, equipment and administrative control systems. The allocation of safety actions to human or engineered components should take account of their differing capabilities and limitations. The assessments should demonstrate that interactions between human and engineered components are fully understood, and that human actions that might impact on nuclear safety are clearly identified and adequately supported.*

Engineering principles: human factors	Integration with design, assessment and management	EHF.1
A systematic approach to integrating human factors within the design, assessment and management of systems should be applied throughout the entire facility life-cycle.		

Engineering principles: human factors	Allocation of safety actions	EHF.2
When designing systems, the allocation of safety actions between humans and technology should be substantiated and dependence on human action to maintain a safe state should be minimised.		

376 Where safety actions are identified in the administrative safety measures (EKP.5 *paragraph 145 f.*) they should meet the guidance in paragraphs 146 and 147. Principles ESS.8 and ESS.9 *(paragraph 342 ff.)* on safety system initiation are also relevant to this principle.

Engineering principles: human factors	Identification of actions impacting safety	EHF.3
A systematic approach should be taken to identifying human actions that can impact on safety.		

377 This principle includes defining the safety actions of personnel responsible for monitoring and controlling plant and responding to faults, and of personnel carrying out maintenance, testing and calibration activities. It also includes considering the impact on safety of engineers, analysts, managers and other staff who may not directly interact with plant and equipment.

Engineering principles: human factors	Identification of administrative controls	EHF.4
Administrative controls used to remain within the safe operating envelope should be systematically identified.		

378 The design of these controls should be such that the requirements for personnel action are clearly identified and unambiguous to those responsible for their implementation.

Engineering principles: human factors	Task analysis	EHF.5
Analysis should be carried out of tasks important to safety to determine demands on personnel in terms of perception, decision making and action.		

379 The analysis should address the actions identified using Principles EHF.3 and EHF.4, and should include consideration of physical, psychological and cognitive factors that could impact on human performance.

380 The analysis should demonstrate the feasibility of these actions within the available timescales and should inform the way they are designed and supported to achieve reliable task performance. It should be sufficiently detailed, and demonstrably employed, to provide a basis for developing user interfaces, procedures and job aids, as well as defining operator roles and responsibilities, staffing levels, personnel competence and training needs, communication networks and workspace design.

381 The workload of personnel required to fulfil safety-related actions should be analysed and demonstrated to be reasonably achievable. Wherever possible, this demonstration should form part of the inactive commissioning of the facility.

382 Shift systems should be designed to minimise the likelihood of human error.

Engineering principles: human factors	Workspaces	EHF.6
Workspaces in which plant operations and maintenance are conducted should be designed to support reliable task performance, by taking account of human perceptual and physical characteristics and the impact of environmental factors.		

Engineering principles: human factors	User interfaces	EHF.7
User interfaces, comprising controls, indications, recording instrumentation and alarms should be provided at appropriate locations and should be suitable and sufficient to support effective monitoring and control of the plant during all plant states.		

383 This principle applies to central control rooms, local control stations on the plant and emergency locations that should remain habitable during foreseeable facility emergencies. It also applies to provisions for maintenance and testing.

384 The user interface provisions should encompass normal operation, abnormal operation and postulated fault conditions including, where reasonably practicable, severe accidents.

385 The user interface should:

a) enable the operator to determine plant states and the availability, and status, of plant equipment;
b) provide a conspicuous early warning of any safety-related changes in plant state;
c) provide the means of confirming safety system challenges and identifying, initiating and confirming necessary safety actions;
d) support effective diagnosis of plant deviations; and
e) enable the operator to determine and execute appropriate system actions, including actions to overcome failures of automated safety systems or to reset a safety system after its operation.

386 The user interface should be designed to ensure compatibility with human psychological and physical characteristics and to facilitate reliable human performance. Interfaces and equipment should be clearly labelled.

Engineering principles: human factors	Personnel competence	EHF.8
A systematic approach to the identification and delivery of personnel competence should be applied.		

387 The process for identifying and delivering competence should encompass the phases of: job analysis; identification of competence requirements; training needs analysis; training programme design and implementation; formal assessment of competence; and evaluation. The process should be applied to all those whose actions could impact on safety, including employees and other groups of staff such as contractors. Directors, managers and leaders should be included in this process. Appropriate supervision and monitoring should be maintained until individuals are demonstrably competent to perform their tasks.

Engineering principles: human factors	Procedures	EHF.9
Procedures should be produced to support reliable human performance during activities that could impact on safety.		

388 Procedures should be accurate and designed and presented in a format that is compatible with the needs of the end user and suitable for the task that they are designed to support.

Engineering principles: human factors	Human reliability	EHF.10
Risk assessments should identify and analyse human actions or omissions that might impact on safety.		

389 Assessments should include precursor errors, such as the introduction of unrevealed errors during maintenance, actions that contribute to initiating events, post-fault responses and long-term recovery actions.

390 The selection and application of probability data for human errors should be:

a) derived from operational experience data and/or through the application of recognised human reliability assessment techniques. Use of either approach should be justified and its relevance for the task and context demonstrated;

b) underpinned by task analysis and reflect the influence of human performance shaping factors, making due allowance for uncertainty.

391 Risk assessments should directly model dependent human errors committed by a single operator or different operators. The results of the risk assessments should be used in the fault analysis.

Control of nuclear matter

392 The principles in this sub-section apply to all types of nuclear matter unless the wording makes it clear that limited application was intended, or unless it can be shown that the total amount of nuclear matter concerned is sufficiently small or is in such a chemical or physical form as to make it unnecessary to apply to any one or more of the principles. However, when nuclear matter has been designated as radioactive waste, the principles in the section on Radioactive waste management (paragraph 646 ff.) also apply. Many of the more specific principles in other sub-sections are also relevant, eg Containment and ventilation (paragraph 418 ff.).

Engineering principles: control of nuclear matter	Strategies for nuclear matter	ENM.1
A strategy (or strategies) should be made and implemented for the management of nuclear matter.		

393 The strategy(ies) should be consistent with Government policy and integrated with other relevant strategies.

Engineering principles: control of nuclear matter	Provisions for nuclear matter brought onto, or generated on, the site	ENM.2
Nuclear matter should not be generated on the site, or brought onto the site, unless sufficient and suitable arrangements are available for its safe management.		

Note: Licence Condition 4 (see the HSE website), which addresses restrictions on nuclear matter on the site, is relevant here.

394 Such arrangements should include where appropriate:

a) handling provisions;
b) flasks, containers, and other packages;
c) treatment and processing facilities;
d) designated storage areas, of appropriate capacity, including spare and buffer capacity where necessary;
e) disposal facilities;
f) rail and road transport provisions.

Engineering principles: control of nuclear matter	Transfers and accumulation of nuclear matter	ENM.3
Unnecessary or unintended generation, transfer or accumulation of nuclear matter should be avoided.		

395 Plant components such as vessels, pipework, ducting and secondary containment structures should be designed to avoid unintended accumulation of nuclear matter, and to facilitate decontamination.

396 Temporary isolations should be effective and controlled by suitable management arrangements. Particular attention should be paid to situations in which ineffective or partially effective temporary isolations could lead to unintended transfers of nuclear matter, eg through leaking valves.

397 Temporary re-routing of nuclear matter is best avoided, but where necessary should be routed appropriately and returned to its normal locations.

Engineering principles: control of nuclear matter	Control and accountancy of nuclear matter	ENM.4
Nuclear matter should be appropriately controlled and accounted for at all times.		

398 Nuclear matter should be identified and an inventory established that should be reviewed and kept up to date. This should include (Licence Conditions 25 and 32, see the HSE website):

a) origin and ownership;
b) receipts of nuclear matter onto the site;
c) shipments of nuclear matter from the site,
d) internal movements of nuclear matter on the site and within facilities;
e) nuclear matter stored or accumulated on the site.
f) appropriate characterisation information (such as that considered in Principle ENM.5 below);
g) details of containers and packaging.

399 The design and operation of facilities on the site, including any modifications to facilities or processes, should facilitate the control and accountancy of nuclear matter.

400 Monitoring, recording and alarm systems should be used to report significant deviations from normal operating conditions as an aid to maintaining plant control and detecting leakage.

401 Containers or packages used for the transport or movement of nuclear matter on site, or within a facility, should be appropriately marked or labelled.

402 The unauthorised access to, or removal of, nuclear matter should be prevented.

403 Records are required to facilitate the management of nuclear matter, and to comply with the requirements of the nuclear site licence. In the case of nuclear matter that is classified as radioactive waste, Principle RW.7 *(paragraph 681 f.)* also applies.

404 Records should be maintained in a secure and accessible form, and for the appropriate period of time (Licence Conditions 6, 25 and 32, see the HSE website).

Engineering principles: control of nuclear matter	**Characterisation and segregation**	**ENM.5**
Nuclear matter should be characterised and segregated to facilitate its safe management.		

405 Nuclear matter should be characterised at appropriate stages in terms of its physical, chemical, radiological and biological properties, radioactivity levels, fissile content, temperature, enrichment, burn up, cooling time, and the presence of contaminants.

406 Sufficient representative information should be obtained from characterisation of nuclear matter to support future management activities.

407 Provision should be made for identifying, assessing and dealing with nuclear matter that does not meet existing process specifications.

408 Nuclear matter should be segregated from incompatible materials where mixing or contact could adversely affect subsequent steps in its management.

409 Where it is proposed to mix different types of nuclear matter, such mixing should be justified.

Engineering principles: control of nuclear matter	**Storage in a condition of passive safety**	**ENM.6**
When nuclear matter is to be stored on site for a significant period of time it should be stored in a condition of passive safety and in accordance with good engineering practice.		

410 Principle RW.5 *(paragraph 666 f.)* (concerned with the passive safe storage of radioactive waste) also applies to nuclear matter, with due allowance made for the planned future use of the material.

Engineering principles: control of nuclear matter	**Retrieval and inspection of stored nuclear matter**	**ENM.7**
Storage of nuclear matter should be in a form and manner that allows it to be retrieved and, where appropriate, inspected.		

411 The design of facilities and the associated operational arrangements should:

a) enable nuclear matter to be retrieved within an appropriate timescale;

b) enable nuclear matter to be inspected, where appropriate, within an appropriate timescale. This may involve in situ inspection, or retrieval of the nuclear matter, or a sample thereof for inspection. Any proposal to rely on sampling should be justified (see also paragraph 397);

c) take account of the anticipated storage duration and any changes in the characteristics of the nuclear matter and its containment that might occur during the storage period.

Engineering principles: control of nuclear matter	Nuclear material accountancy	ENM.8
Nuclear material accountancy data should be analysed and reviewed periodically.		

412 Engineering and operational controls should provide the main lines of protection against leaks and escapes of radioactive, corrosive or toxic substances and accumulation of nuclear matter. Nuclear material accountancy is often aimed primarily at satisfying international safeguards, but the data collected may also help to maintain nuclear safety. Analysis of accountancy data may lead to early detection of accumulation or diversion of nuclear matter – eg due to leaks or blockages.

413 Procedures should be established to implement, verify, approve, monitor, audit and review the effectiveness of accountancy systems.

414 The extent and frequency of analysis will depend on the safety case and may be influenced by the availability of data collected for international safeguards purposes.

415 Any unexplained or unexpected changes, with the potential to affect nuclear safety, should result in the operations being terminated safely, the cause investigated and appropriate action taken.

416 Display systems should be configured to provide an overview of the condition of the process including, where appropriate, mass and volumetric balance summaries.

417 Operators should perform volumetric, mass balance and radioactive concentration checks whenever unusual level or flow imbalances are experienced within a unit.

Containment and ventilation

418 Containment and ventilation systems should confine the nuclear matter within the facility and prevent its leakage and escape to the environment in normal operation and fault conditions, except in accordance with authorised discharge conditions, or as part of a planned transfer to another facility.

419 The term 'containment' encompasses a wide range of structures and plant items, from the massive buildings surrounding power reactors, to glove boxes and individual packages and containers. Containments often have associated systems, such as cooling systems and sprays, which are considered to be part of the containment system.

420 The use of pressure gradients and flows within ventilation systems between contamination zones ensures that any movement of radioactive material is generally from the zones with the lowest contamination level to those with the highest levels, and eventually to places where such material may be disposed of safely.

421 Containment and associated nuclear ventilation systems will form part of a safety system, hence the general principles applicable to engineering and safety systems should be applied. Ventilation systems may be required on parts of a facility that would not be considered as containment, in the sense that there are areas to which access is freely available, and would not be classed as safety systems.

422 The potential for a fire can have a major impact on the design of the ventilation and containment system, influencing for example the position, number and type of fire dampers. Where fire dampers are provided, their position and operation should not compromise the containment function, and their effect on the ventilation system should be considered. In addition to the principles in this sub-section, other impacts of fire may need to be considered, and reference should be made to the principles on protection against fire (paragraph 228 ff.).

Engineering principles: containment and ventilation: containment design	Prevention of leakage	ECV.1
Radioactive substances should be contained and the generation of radioactive waste through the spread of contamination by leakage should be prevented.		

Engineering principles: containment and ventilation: containment design	Minimisation of releases	ECV.2
Nuclear containment and associated systems should be designed to minimise radioactive releases to the environment in normal operation, fault and accident conditions.		

423 The safety functionality should be clearly identified for operational states and fault and accident conditions. Where appropriate, containment should be designed to protect the facility from external hazards and to withstand internal hazards.

Engineering principles: containment and ventilation: containment design	Means of confinement	ECV.3
The primary means of confining radioactive substance should be by the provision of passive sealed containment systems and intrinsic safety features, in preference to the use of active dynamic systems and components.		

424 Where appropriate, containment design should:

a) define the containment boundaries with means of isolating the boundary;
b) establish a set of design safety limits for the containment systems and for individual structures and components within each system;
c) define the requirements for the performance of the containment in the event of a severe accident as a result of internal or external hazards, including its structural integrity and stability;
d) include provision for making the facility safe following any incident involving the release of radioactive substances within or from a containment, including equipment to allow decontamination and post-incident re-entry to be safely carried out;
e) minimise the size and number of service penetrations in the containment boundary, which should be adequately sealed to reduce the possibility of nuclear matter escaping from containment via routes installed for other purposes;
f) avoid the use of ducts that need to be sealed by isolating valves under accident conditions. Where isolating valves and devices are provided for the isolation of containment penetrations, their performance should be consistent with the required containment duties and should not prejudice adequate containment performance;
g) provide discharge routes, including pressure relief systems, with treatment system(s) to minimise radioactive releases to acceptable levels. There should be appropriate treatment or containment of the fluid or the radioactive material contained within it, before or after its released from the system;
h) allow the removal and reinstatement of shielding;
i) define the performance requirements of containment systems to support maintenance activities;
j) demonstrate that the loss of electrical supplies, air supplies and other services does not lead to a loss of containment nor the delivery of its safety function;
k) demonstrate the control methods and timescales for re-establishing the containment conditions where access to the containment is temporarily open (eg during maintenance work);
l) incorporate measures to minimise the likelihood of unplanned criticality wherever significant amount of fissile materials may be present.

425 Should the pressure relief system operate, the performance of the containment should not be degraded.

Engineering principles: containment and ventilation: containment design	Provision of containment barriers	ECV.4
Where the radiological challenge dictates, waste storage vessels, process vessels, piping, ducting and drains (including those that may serve as routes for escape or leakage from containment) and other plant items that act as containment for nuclear matter, should be provided with further containment barrier(s) that have sufficient capacity to deal safely with the leakage resulting from any design basis fault.		

426 When considering secondary containment, the design should include appropriate means of isolation. It should also incorporate, where appropriate, redundant storage provisions with sufficient capacity and associated services to ensure prolonged safe storage of the maximum anticipated volume of material requiring relocation, allowing for any volume increase due to the method of transfer (eg from the use of ejectors).

Engineering principles: containment and ventilation: containment design	Minimisation of personnel access	ECV.5
The need for access by personnel to the containment should be minimised.		

427 Where access is necessary it should be designed to ensure that at all times the containment will perform its safety function.

428 There should be no requirement for access to the containment to ensure the safety of the facility in either the short or long term following an accident.

429 Where gloveboxes and associated ventilation systems are provided, their design should:

a) prevent containment boundary failure due to pressure excursions caused by ventilation faults;
b) accommodate glove failure and still maintain containment;
c) ensure that major failure of a glove box envelope does not compromise containment performance of associated gloveboxes.

Engineering principles: containment and ventilation: containment monitoring	Monitoring devices	ECV.6
Suitable monitoring devices with alarms and provisions for sampling should be provided to detect and assess changes in the stored radioactive substances or changes in the radioactivity of the materials within the containment.		

430 The devices and alarms should monitor safety-related conditions and ensure detection and aid assessment of unplanned or uncontrolled changes in the volume, radioactivity, or fissile content of nuclear substances within the containment.

Engineering principles: containment and ventilation: containment monitoring	Leakage monitoring	ECV.7
Appropriate sampling and monitoring systems and other provisions should be provided outside the containment to detect, locate, quantify and monitor leakages of nuclear matter from the containment boundaries under normal and accident conditions.		

431 This should include provision for environmental surveys in the vicinity of the facility.

432 Provision should be made for testing the containment systems at suitable periods to confirm overall system performance eg depressions, airflows and if relevant inerting gas concentrations, filter performance and valve response times (see also Principle EMT.6 *(paragraph 189 f.)*).

Engineering principles: containment and ventilation: import and export of nuclear material	Minimisation of provisions	ECV.8
Where provisions are required for the import or export of nuclear matter into or from the facility containments, the number of such provisions should be minimised.		

Engineering principles: containment and ventilation: import and export of nuclear material	Standards	ECV.9
The design should ensure that controls on fissile content, radiation levels, the overall containment and ventilation standards are suitable and sufficient at all times.		

433 Where appropriate, the following should be provided:

a) Remote handling devices and means to facilitate their operation, decontamination and repair.

b) Additional containment, local ventilation, and shielding.

Engineering principles: containment and ventilation: ventilation design	Safety functions	ECV.10
The safety functions of the ventilation system should be clearly identified and the safety philosophy of the system in normal and fault conditions should be defined in terms of the relative priorities given to the functions associated with the system.		

434 Functions associated with a system would include: direct protection of people; control and minimisation of discharges from the plant; fire protection and process protection.

435 Where a ventilation system is deemed necessary, it should include appropriate treatment systems to remove and collect airborne radioactive material prior to discharge of the cleaned gas stream to the environment in accordance with the authorisation granted by the relevant environment agency. Such systems may include particulate filtration and incorporate other methods of treatment such as scrubbers and cyclones where appropriate.

436 Where appropriate, ventilation should include the following:

a) Provision of a suitable working environment for personnel and safety-related equipment, particularly in the control rooms.

b) Maintaining the segregation of process and breathing zone air streams.

c) Ensuring that the flow of ventilation air within buildings is always from zones of lower to higher levels of potential contamination at a sufficient velocity to provide protection to occupants against airborne contamination, for both engineered and accidental openings.

d) Controlling the dispersal of contamination and reducing the concentration of airborne activity within the process plant and in aerial discharges to the lowest reasonably practicable levels.

e) Controlling the temperature, pressure and composition of the atmosphere inside the containment as necessary, including where appropriate the moisture content.

f) Safeguarding the facility and personnel against ingress of gases or vapours from external sources where the ingress of such substances, gases or materials could prejudice the safety of operators or operations due to their chemical or radioactive properties etc.

g) Siting intakes to avoid contamination of intake air during normal and fault conditions in the facility and on the site.

h) Provision of inlet filters and dampers to prevent the ingress and egress of radioactive substances as appropriate.

i) Minimising the risk arising from the chemical and toxic properties of process radioactive substances and from explosive mixtures, including gases and vapours, that may be generated.

j) Segregation and isolation to protect against internal and external hazards and to prevent the mixing of ventilation streams of different hazard potentials, eg explosive, toxic and radioactive. Such hazards should be managed to avoid compounding the harm potential.

k) Facilitating, where appropriate, permanent or temporary access to facility zones without impairing the performance of the ventilation system(s).

l) Restricting the outward flow of building air to appropriately controlled authorised discharge points.

m) Accounting for effects of wind velocity and potential air pressure fluctuations caused by nearby structures, discharges from other facilities and extreme weather conditions.

n) Removal and reinstatement of ventilation equipment for maintenance and replacement purposes.

o) Qualification of ventilation systems in terms of their safety function and appropriate selection of materials and equipment for the required design life.

p) Minimising the total airflow through the system from inlet to discharge to reduce the requirement for disposal of filters, while retaining a safe atmosphere, airflow velocities, pressure differences and other features of the design.

q) The need for inerting atmospheres, for example in gloveboxes, either as part of normal operations, or temporarily as part of a fire suppression system.

437 The location of ventilation filters should minimise the dose rates to facility personnel, where necessary shielding should be provided. There should be provision for the safe replacement of filter elements and the safe storage of contaminated filters. Provision should be made to enable filters to be changed, in accordance with a defined replacement regime, while maintaining the effectiveness of the ventilation system.

438 The design should provide for monitoring and testing of ventilation systems and associated filters and gas treatment systems to ensure that they continue to meet the design requirements. This should include provision of appropriate alarm/control systems on key plant parameters.

Reactor core

439 The principles described in this sub-section apply to the reactor core as an assembly and to its main elements (eg the fuel, moderator, coolant, neutron absorbers, core restraints/supports and also breeder assemblies in fast reactors) individually when in the core. Specific principles for graphite cores are in the sub-section on Graphite components and structures (paragraph 303 ff.). The principles relate to the requirements to control reactivity, heat generation/removal and other aspects of the design so that components within the reactor can be kept within specified limits set to ensure an appropriate level of safety during operation and in design basis fault conditions.

Engineering principles: reactor core	**Design and operation of reactors**	**ERC.1**
The design and operation of the reactor should ensure the fundamental safety functions are delivered with an appropriate degree of confidence for permitted operating modes of the reactor.		

440 The above principle covers normal operation, refuelling, testing and shutdown and design basis fault conditions. The fundamental safety functions are:

a) control of reactivity (including re-criticality following an event);

b) removal of heat from the core;

c) confinement or containment of radioactive substances.

441 There should be suitable and sufficient margins between the normal operational values of safety-related parameters and the values at which the physical barriers to release of fission products are challenged.

442 The requirements for loading and unloading of fuel and core components, refuelling programmes, core monitoring and the criteria and strategy for dealing with fuel failures should be specified.

443 No single moveable fissile assembly, moderator or absorber when added to or removed from the core should increase the reactivity by an amount greater than the shutdown margin, with an appropriate allowance for uncertainty. The uncontrolled movement of reactivity control devices should be prevented.

Engineering principles: reactor core	Shutdown systems	ERC.2
At least two diverse systems should be provided for shutting down a civil reactor.		

444 Where a shutdown system is also used for the control of reactivity, a suitable and sufficient shutdown margin should be maintained at all times.

445 Reactor shutdown and subsequent hold-down should not be inhibited by mechanical failure, distortion, erosion, corrosion etc of plant components, or by the physical behaviour of the reactor coolant, under normal operation or design basis fault conditions.

Engineering principles: reactor core	Stability in normal operation	ERC.3
The core should be stable in normal operation and should not undergo sudden changes of condition when operating parameters go outside their specified range.		

446 An increase in reactivity or reduction in coolant flow, caused by the unplanned:

a) movement within the core;
b) loss from the core; or
c) addition to the core;

of any component, object or substance should be prevented.

447 The geometry of the core should be maintained within limits that enable the passage of sufficient coolant to remove heat from all parts of the core. Where appropriate, means should be provided to prevent any obstruction of the coolant flow that could lead to damage to the core as a result of overheating. In particular the overheating of fuel should be prevented where this would give rise to:

a) fuel geometry changes that have an adverse effect on heat transport;
b) failure of the primary coolant circuit.

Note: Where these mechanisms cannot be prevented by design, protective measures should be available to maintain the plant in a safe condition.

448 The structural integrity limits for the core structure and its components (including the fuel) should ensure that their geometry will be suitably maintained.

449 Changes in temperature, coolant voiding, core geometry or the nuclear characteristics of components that could occur in normal operation or fault conditions should not cause uncontrollably large or rapid increases in reactivity.

450 Effects of changes in coolant condition or composition on the reactivity of the reactor core should be identified. The consequences of any adverse changes should be limited by the provision of protective systems or by reactor core design parameters.

451 There should be suitable and sufficient design margins to ensure that any reactivity changes do not lead to unacceptable consequences. Limits should be set for the maximum degree of positive reactivity.

452 The design of the core and its components should take account of any identified safety-related factors, including:

a) irradiation;
b) chemical and physical processes;
c) static and dynamic mechanical loads;
d) thermal distortion;
e) thermally-induced stress; and
f) variations in manufacture.

453 The core should be securely supported and positively located with respect to other components in the reactor to prevent gross unplanned movements of the structure of the core or adverse internal movements.

454 Core components should be mutually compatible and compatible with the remainder of the plant.

455 The incorrect location of any core components should be physically inhibited.

Engineering principles: reactor core	Monitoring of safety-related parameters	ERC.4
The core should be designed so that safety-related parameters and conditions can be monitored in all operational and design basis fault conditions and appropriate recovery actions taken in the event of adverse conditions being detected.		

456 Fuel assemblies should be designed to permit suitable and sufficient inspection of their structure and parts before loading into the core. Provision should be made for in-service monitoring and post-irradiation inspection to confirm fuel behaviour and performance.

457 The design should allow fuel to be removed from the reactor, despite any environmentally induced damage such as bowing, swelling or from other damage occurring in normal operation and in design basis fault conditions.

Heat transport systems

458 These principles relate to the systems required to transport heat within the facility, both in normal operation and fault conditions, and cover the full range of heat transfer applications in reactors, chemical facilities, fuel storage ponds, etc. Where the heat transport system serves as a safety system or safety-related system, the general principles applicable to engineering and safety systems should also apply.

Engineering principles: heat transport systems	Design	EHT.1
Heat transport systems should be designed so that heat can be removed or added as required.		

459 Sufficient capacity should be available to do this at an adequate rate.

Engineering principles: heat transport systems	Coolant inventory and flow	EHT.2
Sufficient coolant inventory and flow should be provided to maintain cooling within the safety limits for operational states and design basis fault conditions.		

460 The various sources of heat to be added to or removed from any system and its component parts under normal and fault conditions should be quantified, and the uncertainties estimated in each case.

461 Inherent cooling processes such as natural circulation can be taken into account in assessing the effectiveness of the heat transport system, providing they are shown to be effective in the conditions for which they are claimed.

462 In the case of liquid heat transport systems, there should be a margin against failure of the operating heat transfer regime under anticipated normal and fault conditions and procedures. The minimum value of this margin should be stated and justified with reference to the uncertainties in the data and in the calculational methods employed.

Engineering principles: heat transport systems	Heat sinks	EHT.3
A suitable and sufficient heat sink should be provided.		

463 Provision should be made for removal of heat to an adequate heat sink at any time throughout the life of the facility, irrespective of the availability or otherwise of external resources. Consideration should be given to the site-related environmental parameters such as variations in air and water temperatures, available levels and flow rates of water etc, to ensure adequate heat removal capacity at all times.

Engineering principles: heat transport systems	Failure of heat transport system	EHT.4
Provisions should be made in the design to prevent failure of the heat transport system that could adversely affect the heat transfer process, or safeguards should be available to maintain the facility in a safe condition and prevent any release in excess of safe limits.		

464 Provision should be made to:

a) minimise the effects of faults within the facility that may propagate through the heat removal and ventilation systems. Personnel and structures, systems and components important to safety should be protected where necessary from the radiation, thermal and/or dynamic effects of any fault involving the heat transport fluids;

b) prevent an uncontrolled loss of inventory coolant from the coolant pressure boundary. Provision should be made for the detection of significant loss of heat transport fluid or any diverse change in heat transport that might lead to an unsafe state. Provisions should be made in the design to minimise leakage of the coolant and keep it within specified limits. Isolation devices should be provided to limit any loss of radioactive fluid;

c) where appropriate, provide a sufficient and reliable supply of reserve heat transfer fluid, separate from the normal supply, to be available in sufficient time in the event of any significant loss of heat transfer fluid.

465 The properties of any heat transport fluid, its composition and impurity levels should be so specified as to minimise adverse interactions with facility components and any degradation of the fluid caused by radiation. Appropriate chemical and physical parameters should be monitored and filtration, processing or other plant provided to ensure that the specified limits are maintained.

466 Where mutually incompatible heat transport fluids are used within the facility, provision should be made to prevent their mixing and, where appropriate, to prevent harm to personnel and safety-related structures in the event of such mixing.

Engineering principles: heat transport systems	Minimisation of radiological doses	EHT.5
The heat transport system should be designed to minimise radiological doses.		

467 Components subject to neutron irradiation should be fabricated from materials that minimise the effects of neutron activation.

468 Provision for removing and storing the radioactive coolant to allow inspection and repair work should be made where appropriate.

469 The design, construction and operation of the facility and the choice of heat transfer fluid should minimise the amount of radioactive substances in that fluid. Provision should be made to monitor and remove any significant build-up of radioactive substances from the heat transport fluid and associated containment.

Criticality safety

470 Criticality safety principles apply to the processing, handling or storage of fissile materials in significant quantities with respect to the minimum critical mass, and in locations where criticality is not intended. The principles in this sub-section, which should be read in conjunction with the Fault analysis section, are specific to criticality safety.

Engineering principle: criticality safety	Safety measures	ECR.1
Wherever significant amount of fissile materials may be present, there should be a system of safety measures to minimise the likelihood of unplanned criticality.		

471 The hierarchy of controls set out in the Key engineering principles sub-section (*paragraph 135 ff.)* is appropriate for criticality safety, and gives preference to minimising the amount of fissile material present, consistent with the process requirements. For non-reactor facilities, the principal means of passive engineering control of criticality should be geometrical constraint. Where sub-criticality cannot be maintained through geometrical constraint alone, additional engineered safety measures should be specified, such as fixed neutron absorbers. Reliance on neutron absorbers requires assurance of their continued presence and effectiveness.

472 Further safety measures may need to be specified such as:

a) controlling the mass and isotopic composition of the fissile material present in a nuclear process;
b) controlling the concentration of fissile material in solutions; and
c) controlling the amount of neutron moderating and reflecting material associated with the fissile material.

473 The design and operation of plant and equipment dealing with fissile material should be such as to facilitate the termination of a criticality incident.

Engineering principle: criticality safety	Double contingency approach	ECR.2
A criticality safety case should incorporate the double contingency approach.		

474 The double contingency approach requires that unintended criticality cannot occur unless at least two unlikely, independent concurrent changes in the conditions originally specified as essential to criticality safety have occurred.

475 For long-term storage of radioactive waste containing fissile materials, traditional deterministic criticality assessments can lead to very conservative limits on fissile materials. Consideration should be given to a risk-informed approach that balances the risks from an unplanned criticality against other factors, such as the dose accrued as a result of the preparation of waste packages.

RADIATION PROTECTION

476 *The provision of adequate protection against exposure to ionising radiation and radioactive contamination is required both in normal operations and accident conditions to protect both the workers and members of the public. All facilities should be operated, inspected, maintained and decommissioned in compliance with regulations relating to the safe use of ionising radiations. These currently include IRR, supported by an Approved Code of Practice (ACoP)[10]. Adequate protection is that level of protection that ensures compliance with the ALARP requirements of all relevant legislation, where appropriate to the SAPs, and takes into account the latest modern standards.*

477 *The principles and guidance in this section relate to the permissioning of activities on licensed sites. They highlight aspects that inspectors are expected to look for in safety cases. They cover some matters that are already featured in IRR and its ACoP[10], but with additional details relevant to safety cases, along with relevant good practice for licensed sites.*

478 *The system of radiation protection is based on the principles of justification of practices and interventions, optimisation of protection and individual dose limitation. Justification is not regulated by HSE and is not considered in the SAPs. The underpinning concept in radiation protection is the hierarchy of control measures. The dutyholder should establish a hierarchy of control measures in accordance with IRR regulation 8(2), see the guidance in the box below.*

Guidance L121 p74[10]: 'Regulation 8(2) establishes a hierarchy of control measures for restricting exposure. First and foremost, in any work with ionising radiation, radiation employers should take action to control doses received by their employees and other people by engineered means. Only after these have been applied should consideration be given to the use of supporting systems of work. Lastly radiation employers should provide personal protective equipment to further restrict exposure where this is reasonably practicable.'

479 *There should be a strategy to restrict radiation exposure. This should include, but is not restricted to, the minimisation of sources of radiation, system and component design including shielding optimisation and layout, and management arrangements including the use of time and distance during operations. Optimisation of protection and limitation of doses to individuals should be adequately dealt with in the safety cases. An important element of optimisation of protection is that the collective effective dose to people on site, as a result of the operation of the nuclear facility, should be kept ALARP.*

Radiation protection	**Normal operation**	**RP.1**
Adequate protection against exposure to radiation and radioactive substances in normal operation should be provided in those parts of the facility to which access needs to be gained.		

Radiation protection	**Accident conditions**	**RP.2**
Adequate protection against exposure to radiation and radioactive contamination in accident conditions, should they occur, should be provided in those parts of the facility to which access needs to be gained. This should include prevention or mitigation of accident consequences.		

480 In line with guidance in the ACoP[10], preference should be given to the use of appropriate engineering controls and design features. The restriction of exposure to radiation and radioactive contamination should not preclude admission to, or occupancy of, any facility area where access is required to achieve and maintain a safe facility state.

481 There should be appropriate provisions for the measurement of radiation doses to individuals. Personnel exposures should be estimated in advance and monitored during work activity, using suitably located devices where appropriate.

482 Effective systems should be provided, where appropriate, under normal operation and fault conditions for monitoring ionising radiations in the facility to ensure that breakdowns in systems and controls, and long-term changes to radiological conditions, are detected.

483 Instrumentation should be provided, where appropriate, to give prompt, reliable and accurate indication of airborne and direct radiation, including activity levels in operating areas, and should be fitted with alarms to indicate significant changes in levels that require prompt action. Such equipment should be capable of providing reliable indications and alarms, taking into account prevailing environmental conditions. Consideration should be given to the provision for remote indication of radiological conditions following accident situations.

484 Adequate warning systems (not necessarily a Criticality Incident Detection (CID) system) should be provided wherever fissile material is present, unless an assessment shows that no criticality excursion could give any individual a whole body dose exceeding the annual whole body dose limit, or that the predicted frequency is acceptably low. An estimate of the criticality consequences should inform the need for the installation of the warning system. Where appropriate, a criticality warning system may have an additional function and be linked to safety systems design to achieve the safe termination of the criticality incident (eg it may initiate boron injection), or trigger an alarm.

Radiation protection	Designated areas	RP.3
Where appropriate, designated areas should be further divided, with associated controls, to restrict exposure and prevent the spread of radioactive substances.		

485 The further division of designated areas should be based upon the levels of radiation, contamination and airborne activity, measured and/or expected as the result of particular planned work activities.

486 Each area should have appropriate controls on access and egress (including evacuation), occupancy and adequate arrangements for the use of personal protective equipment.

487 Where doses of a significant fraction of any statutory dose limit are likely to be incurred in a matter of minutes in any area, access should be controlled by physical means such as interlocks, alarms, or locked doors to prevent unauthorised entry. Prompt escape by any person from such places should not be obstructed. Where such control measures are not reasonably practicable, an equivalent standard of protection should be ensured by other arrangements.

Radiation protection	Contaminated areas	RP.4
Appropriate provisions for protecting persons entering and working in contaminated areas should be provided.		

488 There should be provision for monitoring and controlling the spread of airborne activity and contamination within and beyond each area.

489 The level of contamination within such areas should be kept ALARP for the nature of the activities undertaken.

490 The facility should include the ventilation of contaminated areas to control potential airborne contamination, and appropriate features for limiting the spread of contamination. Where change barriers are used, they should be located taking into account the balance between protecting people and reducing the spread of radioactive contamination.

Radiation protection	Decontamination	RP.5
Suitable and sufficient decontamination provisions for the people, the facility, its plant and equipment should be provided.		

491 This should include the provision for monitoring and decontamination of anything removed from contaminated locations. Provision should be made for local decontamination unless it can be demonstrated that in the particular circumstances a centralised decontamination facility is more appropriate.

492 Manipulation of items exhibiting high surface radiation dose rates should be carried out using appropriate arrangements to restrict exposures. These may include remote handling devices and enclosures to provide protection against the spread of radioactive contamination.

Radiation protection	Shielding	RP.6
Where shielding has been identified as a means of restricting dose, it should be effective under all conditions.		

493 In particular, precautions should be taken so that the use of shielding and associated equipment takes account of and, where appropriate, reduces:

a) the possible faults that may arise and changes of radiation types and levels during the lifetime of the facility, including any post-operational period prior to final decommissioning;

b) the incidence of localised levels of radiation due to streaming;

c) unplanned or uncontrolled movement or loss of shielding;

d) installation behind shielding of components requiring regular handling or to which regular access is required, except where such components are sources of radiation requiring shielding;

e) exposure of extremities of workers during handling and manipulation of radioactive sources; and

f) unplanned or uncontrolled removal from behind shielding of any source.

494 The use of shielding should be shown to be ALARP in that the dose saved by its use must exceed the dose received during its installation.

495 Where liquid is used as a shielding material, there should be design provisions for preventing unintentional loss of such liquid, suitable means should be provided for detecting such losses and initiating an alarm, and a recovery plan should be prepared and rehearsed.

FAULT ANALYSIS

496 The assessment of risks arising from nuclear facilities needs to consider those arising both from normal operation and from fault conditions. This section addresses the latter.

497 Conservative design, good operational practice, and adequate maintenance and testing should minimise the likelihood of faults. Nevertheless, faults may still occur and so a facility must be capable of tolerating them. Nuclear facilities are therefore designed to cope with, or are shown to withstand, a wide range of faults without unacceptable consequences by virtue of the facility's inherent characteristics or safety measures. This is known as the design basis.

498 Design basis analysis (DBA) is a robust demonstration of the fault tolerance of the facility, and of the effectiveness of its safety measures. Its principal aims are to guide the engineering requirements of the design, including modifications, and to determine limits to safe operation, so that safety functions can be delivered reliably during all modes of operation and under reasonably foreseeable faults. In DBA, any uncertainties in the fault progression and consequence analyses are addressed by the use of appropriate conservatism. In this approach, risk is not quantified, but the adequacy of the design and the suitability and sufficiency of the safety measures are assessed against deterministic targets. However, DBA alone may not be sufficient to demonstrate adequate safety of the facility.

499 Firstly, additional analysis may be needed to address the overall risk presented by the facility to allow comparisons to be made against the targets set out in this document, see the section on Numerical targets and legal limits (paragraph 568 ff.). It may also be essential for understanding the strengths and weaknesses of a design with complex systems and interdependencies; as part of evaluating modifications to plant; or changes in operating conditions; and for many other applications to safety decision making. These matters are normally addressed in the nuclear industry through probabilistic safety analysis (PSA).

500 Secondly, DBA may not include the full range of identified faults because it may not be reasonably practicable to make design provision against the more unlikely faults. It therefore does not address severe but very unlikely faults in which the design safety measures may be ineffective. This is addressed by severe accident analysis. Robust application of DBA should ensure that severe accidents are highly unlikely. Nevertheless, the principle of defence in depth requires that fault sequences leading to severe accidents are analysed and provision made to address their consequences. The analysis of severe accidents differs from the DBA in that it should be performed preferably on a best-estimate basis, since it is required primarily to give realistic guidance on the actions to be taken in the unlikely event of such an accident occurring. Severe accident analysis may also identify that providing further plant and equipment for accident management is reasonably practicable.

501 Criticality safety is important because of the very high levels of neutron and gamma radiation fields associated with criticality accidents. Unplanned criticalities can result in individuals in the immediate vicinity receiving high radiation doses, which could be fatal. For this reason, an unplanned criticality is a major radiological hazard, and suitable and sufficient measures should be taken to reduce the risks of such events. The fault analysis principles therefore apply to criticality safety.

502 Fault analysis of nuclear facilities is likely to involve consideration of many fault sequences and accident conditions for which there is limited or no experience. There are therefore often significant uncertainties and gaps in the physical and statistical data that are needed for the analysis. Handling quantifiable uncertainties, stemming from imprecision in knowledge and data, should be regarded as an intrinsic part of the risk assessment under HSE's precautionary approach to decision making. These uncertainties may be handled by introducing conservatisms, sensitivity analysis, or by a variety of explicit uncertainty analysis techniques. In every case, a key element of HSE's assessment will be professional judgement on whether the assumptions or estimates are supported by appropriate evidence.

503 The fault analysis principles are set out below. First there is a set of general principles that apply to the assessment of the fault analysis as a whole. Then there are more specific principles for assessing DBA, PSA and severe accident analysis respectively. Finally, there is a set of principles that, like the first, apply generally but relate to assuring and maintaining the validity of the fault analysis.

General

Fault analysis: general	Design basis analysis, PSA and severe accident analysis	FA.1
Fault analysis should be carried out comprising design basis analysis, suitable and sufficient PSA, and suitable and sufficient severe accident analysis.		

Fault analysis: general	Identification of initiation faults	FA.2
Fault analysis should identify all initiating faults having the potential to lead to any person receiving a significant dose of radiation, or to a significant quantity of radioactive material escaping from its designated place of residence or confinement.		

504 The process for identifying faults should be systematic, auditable and comprehensive, and should include:

a) significant inventories of radioactive material and also radioactive sources that may be lost or damaged;

b) planned operating modes and configurations, including shutdown states, decommissioning operations, and any other activities which could present a radiological risk; and

c) chemical and other internal hazards, man-made and natural external hazards, internal faults from plant failures and human error, and faults resulting from interactions with other activities on the site.

Faults lacking the potential to lead to doses of 0.1 mSv to workers, or 0.01 mSv to a hypothetical person outside the site, are regarded as part of normal operation and may be excluded from the fault analysis. These are the levels of individual dose above which should be regarded as significant in Principle FA.2. A significant quantity of radioactive material is one which if released could give rise to a significant dose.

Fault analysis: general	Fault sequences	FA.3
Fault sequences should be developed from the initiating faults and their potential consequences analysed.		

505 The scope, content, level of detail and rigour of the analysis should be proportionate to the complexity of the facility and the hazard potential.

506 There should be a clear relation between the fault sequences used in DBA and severe accident analysis, and the fault sequence development of the PSA.

507 Transient analysis or other analyses should be carried out as appropriate to provide adequate understanding of the behaviour of the facility under fault conditions.

508 For fault sequences that lead to a release of radioactive material or to exposure to direct radiation, radiological consequence analysis should be performed to determine the maximum doses to a worker on the site, to a person outside the site, eg directly downwind of an airborne release, and to the reference group for any other off-site release pathways. (The detail of this analysis differs according to its application, see paragraphs 601, 607 and 621.)

509 The calculated doses should include those arising from the potential release of radioactive material, direct radiation, and criticality incidents.

510 Radiological analysis of societal effects from possible releases from the site should be carried out to determine whether the consequences specified in the societal risk target (Target 9 *(paragraph 623 f.)*) could be reached.

511 Following the end of operations, a new fault analysis is likely to be needed to cover the decommissioning phase.

Design basis analysis

512 *This sub-section presents established practice in the UK for DBA. Other approaches may be considered if they clearly achieve the purpose of DBA.*

Fault analysis: design basis analysis	Fault tolerance	FA.4
DBA should be carried out to provide a robust demonstration of the fault tolerance of the engineering design and the effectiveness of the safety measures.		

513 If possible, DBA should be carried out as part of the engineering design. Where this is not possible (eg for review of existing facilities), the analysis should be developed in line with the engineering analysis to demonstrate that the safety function is met. In either case, it is important that the analysis fully reflects the engineering and iterates with it to engender improvements. It should also take account of the key principles sub-section *(paragraph 135 ff.).*

Fault analysis: design basis analysis	Initiating faults	FA.5
The safety case should list all initiating faults that are included within the design basis analysis of the facility.		

514 Initiating faults identified in Principle FA.2 should be considered for inclusion in this list, but the following need not be included:

a) faults in the facility that have an initiating frequency lower than about 1 x 10^{-5} pa;

b) failures of structures, systems or components for which appropriate specific arguments have been made;

c) natural hazards that conservatively have a predicted frequency of being exceeded of less than 1 in 10 000 years;

d) those faults leading to unmitigated consequences which do not exceed the BSL for the respective initiating fault frequency in Target 4 *(paragraph 599 f.)*.

Note: The risks from initiating faults in d) should be shown to be as low as reasonably practicable by application of relevant good engineering practice supported by deterministic and probabilistic analysis as appropriate.

515 Initiating fault frequencies should be determined on a best-estimate basis with the exception of natural hazards where a conservative approach should be adopted.

Fault analysis: design basis analysis	Fault sequences	FA.6
For each initiating fault in the design basis, the relevant design basis fault sequences should be identified.		

516 Correct performance of safety-related and non-safety equipment should not be assumed where this would alleviate the consequences.

517 Each design basis fault sequence should include as appropriate:

a) failures consequential upon the initiating fault, and failures expected to occur in combination with that initiating fault arising from a common cause;

b) single failures in the safety measures in accordance with the single failure criterion;

c) the worst normally permitted configuration of equipment outages for maintenance, test or repair;

d) the most onerous permitted operating state within the inherent capacity of the facility;

Sequences with very low expected frequencies need not be included in the DBA.

518 The analysis should establish that adverse conditions that may arise as a consequence of the fault sequence will not jeopardise the claimed performance of the safety measures.

519 Operator actions can be claimed as part of safety measures only if sufficient time is available, adequate information for fault diagnosis is presented, appropriate written procedures exist and compliance with them is assured, and suitable training has been provided.

520 Initiating events leading to fault sequences protected by the same safety measures may be grouped, and their frequencies summed, for the purposes of the DBA. Conversely, initiating events leading to similar fault sequences should not be subdivided to evade requirements for design basis safety measures.

Fault analysis: design basis analysis	**Consequences**	**FA.7**
Analysis of design basis fault sequences should use appropriate tools and techniques, and be performed on a conservative basis to demonstrate that consequences are ALARP.		

521 The analysis should demonstrate, so far as is reasonably practicable, that:

a) none of the physical barriers to prevent the escape or relocation of a significant quantity of radioactivity is breached or, if any are, then at least one barrier remains intact and without a threat to its integrity;
b) there is no release of radioactivity; and
c) no person receives a significant dose of radiation.

522 Relocation means the material is no longer in its designated place of residence or confinement.

523 Where releases occur, then doses to persons should be limited. The numerical targets for doses to persons are set out in Target 4 *(paragraph 599 f.)*.

524 Design basis analysis may also contribute to accident management strategies and emergency plans.

Fault analysis: design basis analysis	**Linking of initiating faults, fault sequences and safety measures**	**FA.8**
DBA should provide a clear and auditable linking of initiating faults, fault sequences and safety measures.		

525 The analysis should demonstrate that:

a) the design basis initiating faults are addressed;
b) safety functions have been identified for the design;
c) the performance requirements for the safety measures have been identified; and
d) suitable and sufficient safety measures are provided.

Fault analysis: design basis analysis	**Further use of DBA**	**FA.9**
DBA should provide an input into the safety classification and the engineering requirements for systems, structures and components performing a safety function; the limits and conditions for safe operation; and the identification of requirements for operator actions.		

526 DBA should provide the basis for:

a) safety limits, ie the actuator trip settings and performance requirements for safety systems and safety-related equipment;
b) conditions governing permitted plant configurations and the availability of safety systems and safety-related equipment;
c) the safe operating envelope defined as operating limits and conditions in the operating rules for the facility; and
d) the preparation of the facility operating instructions for implementing the safe operating envelope, and other operating instructions needed to implement the safety measures.

Probabilistic safety analysis

527 *PSA provides an integrated, structured, safety analysis that combines engineering and operational features in a consistent overall framework. This in turn enables complex interactions to be identified and examined, and provides a logical basis for identifying any relative weaknesses. Hence it should be an integral part of design development and analysis. PSA also provides an input into risk-informed judgements both at the design stage and in operation.*

528 *The scope and depth of PSA may vary depending on the magnitude of the radiological hazard and risks, the novelty of the design, the complexity of the facility, and the nature of the decision that the safety case is supporting. For example, for some facilities qualitative arguments, application of good practice and DBA may be sufficient to demonstrate that the risk is ALARP. However, for a complex facility such as a power reactor or a reprocessing facility, a comprehensive PSA should be developed.*

Fault analysis: PSA	**Need for PSA**	**FA.10**
Suitable and sufficient PSA should be performed as part of the fault analysis and design development and analysis.		

529 PSA should assist the designers in achieving a balanced and optimised design, so that no particular class of accident or feature of the facility makes a disproportionate contribution to the overall risk, eg of the order of one tenth or greater. PSA should enable a judgement to be made of the acceptability or otherwise of the overall risks against the numerical targets and should help to demonstrate that the risks are, and remain, ALARP.

Fault analysis: PSA	**Validity**	**FA.11**
PSA should reflect the current design and operation of the facility or site.		

530 PSA should be directly related to existing facility and site information, data and documentation. Assumptions used in the absence of such information need to be justified and careful consideration taken of their impact on the analysis.

531 Low initiating fault frequencies need be included only in so far as the PSA results may contribute to design or operation of the facility. In particular, the initiating frequencies used for naturally occurring external hazards should be constrained by Principles EHA.4 (*paragraph 214 f.*) and EHA.7 (*paragraph 217 f.*).

Fault analysis: PSA	**Scope and extent**	**FA.12**
PSA should cover all significant sources of radioactivity and all types of initiating faults identified at the facility or site.		

Fault analysis: PSA	**Adequate representation**	**FA.13**
The PSA model should provide an adequate representation of the site and its facilities.		

532 The PSA should account for contributions to the risk including, but not necessarily restricted to:

a) random individual component failures;
b) components which are failed as a result of the initiating fault;
c) common cause failures (and, as necessary, other dependent and consequential failures);
d) unavailabilities due to testing and maintenance;
e) pre-fault human errors (eg misalignments and miscalibrations);
f) human errors that lead to initiating faults;

g) human errors during the course of the fault sequences; and

h) potential dependencies between separate human activities (either by the same or by different operators).

533 The level of detail of PSA should be sufficient to ensure that it is realistic, that dependencies are captured, and that the data used is applicable to each event in the PSA. Model simplifications (eg modelling of bounding sequences) should be clearly described and justified.

534 Where groups are used to represent several initiating faults or fault sequences, the group should be assigned a frequency equal to the summed frequency of the contributors to the group and should be represented by the most onerous one. A sufficient number of groups should be defined to ensure an adequate representation of the facility, while keeping the scope of the analysis manageable.

535 Best-estimate methods and data should be used for supporting transient analyses, accident progression analyses, source term analyses, and radiological analyses. Where this is not practicable, conservative assumptions should be made and the sensitivity of the risk to these assumptions should be established.

536 Facility-specific data should be used as far as possible for the calculation of the frequencies and probabilities used in PSA. However:

a) Where facility-specific data is not available, use of generic data may be acceptable provided its applicability is justified and the data sources selected are used in a consistent and systematic manner.

b) Where facility-specific data is not sufficient, it should be combined with applicable generic data using a well-established mathematical technique.

c) Where neither facility-specific nor generic data are available, use of expert judgement may be acceptable, provided that the basis for the judgement is justified and documented, and careful consideration given to the impact of these judgements on the PSA results.

537 When models are used for the calculations of input probabilities, for example, in human errors, or failures of computer-based systems (including software errors), common cause failures, or the failures of structures, then the methodologies used should be justified, and should account for key influencing factors.

538 Assumptions made regarding the behaviour of the facility or its operators should be justified, and the sensitivity to those assumptions should be assessed.

539 Due regard should be given to the uncertainties in input probability and frequency values used, and their impact on the results.

540 Steps should be taken to reduce significant uncertainties, ie those that potentially undermine confidence in the PSA results.

Fault analysis: PSA	**Use of PSA**	**FA.14**
PSA should be used to inform the design process and help ensure the safe operation of the site and its facilities.		

541 Appropriate use of PSA should be made in activities such as:

a) designing the facility;

b) supporting modifications to the design and operation during the life of the site and its facilities;

c) testing, inspection and maintenance planning, and management of plant configuration;

d) investigating significant abnormal occurrences; and

e) developing and changing operating procedures and associated training programmes for managing incidents and accidents (including severe accidents).

542 PSA studies may be undertaken to support particular safety submissions for applications such as those noted above. PSA models and data used should be suitable for their intended application, and sensitivity and uncertainty analyses undertaken as appropriate. In any safety submissions where the PSA is not full scope, due account should be taken of the impact of the safety submissions on aspects of the risk not covered in that PSA.

Severe accident analysis

543 *Severe accidents are defined as those fault sequences that lead either to consequences exceeding the highest radiological doses given in the BSLs of Target 4 (paragraph 599 f.), or to a substantial unintended relocation of radioactive material within the facility which places a demand on the integrity of the remaining physical barriers. A substantial quantity of radioactive material is one which if released could result in the consequences specified in the societal risk target (Target 9 (paragraph 623 f.)).*

544 *Rigorous application of DBA should ensure that severe accidents are highly unlikely. Nevertheless suitable and sufficient severe accident analysis is still required to ensure that risks are reduced so far as is reasonably practicable.*

Fault analysis: severe accident analysis	**Fault sequences**	**FA.15**
Fault sequences beyond the design basis that have the potential to lead to a severe accident should be analysed.		

545 This should include:

a) determination of the magnitude and characteristics of their radiological consequences, including societal effects; and

b) demonstration that there is no sudden escalation of consequences just beyond the design basis.

546 The analysis should consider failures that could occur in the physical barriers preventing release of radioactive material, or in the shielding against direct radiation.

547 A best estimate approach should normally be followed. However, where uncertainties are such that a realistic analysis cannot be performed with confidence, a conservative or bounding case approach should be adopted to avoid optimistic conclusions being drawn.

548 Where severe accident uncertainties are judged to have a significant effect on the assessed risk, research aimed at confirming the modelling assumptions should be performed.

Fault analysis: severe accident analysis	**Use of severe accident analysis**	**FA.16**
The severe accident analysis should be used in the consideration of further risk-reducing measures.		

549 The severe accident analysis should provide information:

a) to assist in the identification of any further reasonably practicable preventative or mitigating measures beyond those derived from the design basis;

b) to form a suitable basis for accident management strategies;

c) to support the preparation of emergency plans for the protection of people; and

d) to support the PSA of the facility's design and operation.

550 Measures identified under a) above need not involve the application of conservative engineering practices used in the DBA, but rather should be based upon realistic or best estimate assumptions, methods and analytical criteria.

Assurance of validity of data and models

551 *This sub-section contains further principles governing the methods and data for the transient, radiological and other analyses that may be used throughout the fault analysis.*

Fault analysis: assurance of validity of data and models	**Theoretical models**	**FA.17**
Theoretical models should adequately represent the facility and site.		

Fault analysis: assurance of validity of data and models	Calculation methods	FA.18
Calculational methods used for the analyses should adequately represent the physical and chemical processes taking place.		

552 Where possible, the analytical models should be validated by comparison with actual experience, appropriate experiments or tests.

553 The model should be validated for each application made in the safety analysis. The validation should be of the model as a whole or, where this is not practicable, on a module basis, against experiments that replicate as closely as possible the expected plant condition.

554 Care should be exercised in the interpretation of such experiments to take account of uncertainties in replicating the range of anticipated plant conditions. The limits of applicability of the analytical model should be identified.

555 Where validation against experiments or tests is not possible, a comparison with other, different, calculational methods may be acceptable.

556 Where possible, independent checks using diverse methods or analytical models should be carried out to supplement the original analysis.

557 The radiological analysis should include any direct radiation and any inhalation, absorption and ingestion of radioactive material and should also take account of the physical and chemical form of the radioactive material released.

Fault analysis: assurance of validity of data and models	Use of data	FA.19
The data used in the analysis of safety-related aspects of plant performance should be shown to be valid for the circumstances by reference to established physical data, experiment or other appropriate means.		

558 Where uncertainty in the data exists, an appropriate safety margin should be provided.

559 The limits of applicability of the available data should be identified and extrapolation beyond these limits should not be used unless justified.

Fault analysis: assurance of validity of data and models	Computer models	FA.20
Computer models and datasets used in support of the analysis should be developed, maintained and applied in accordance with appropriate quality assurance procedures.		

560 These procedures should identify measures and controls to provide confidence that safety-related calculations are undertaken without error, to a level commensurate with the importance of the analysis being performed.

561 The procedures should, where appropriate, address code and dataset verification, version control, testing, documentation, user training, peer review and endorsement.

562 The procedures should specify independent verification of computer codes and datasets to confirm consistency with the supporting documentation.

563 The process of inputting data into a model should be independently verified.

Fault analysis: assurance of validity of data and models	Documentation	FA.21
Documentation should be provided to facilitate review of the adequacy of the analytical models and data.		

564 The documentation should include for example:

a) information showing that models and data are not employed outside their range of application;
b) a description of the uncertainties in the model; and
c) user guidelines and input description.

Fault analysis: assurance of validity of data and models	Sensitivity studies	FA.22
Studies should be carried out to determine the sensitivity of the fault analysis (and the conclusions drawn from it) to the assumptions made, the data used and the methods of calculation.		

565 Where the predictions of the analysis are sensitive to the modelling assumptions, they should be supported by additional analysis using independent methods and computer codes.

Fault analysis: assurance of validity of data and models	Data collection	FA.23
Data should be collected throughout the operating life of the facility to check or update the fault analysis.		

566 This should include, but not be restricted to, plant performance and failure data such as statistical data on initiating fault frequencies, component failure rates and plant unavailability during periods of maintenance or test, and data on external hazards.

Fault analysis: assurance of validity of data and models	Update and review	FA.24
The fault analysis should be updated where necessary, and reviewed periodically.		

567 The updates and reviews should take into account:

a) changes to the facility or its operation since the design or construction stage and throughout its operating life;
b) any new relevant technical and scientific knowledge, and operational experience, concerning plant behaviour and fault potential, including incidents occurring at other facilities;
c) any material property changes and deterioration due to ageing not previously taken into account; and
d) advances in modelling techniques.

NUMERICAL TARGETS AND LEGAL LIMITS

568 *This section describes the numerical targets and legal limits that inspectors should use when judging whether the dutyholder is controlling radiological hazards adequately and reducing risks ALARP.*

569 *The structure of the targets and legal limits is based on the TOR[2] framework, which has been extended in the more recent R2P2[1]. In assessing the safety of nuclear facilities, inspectors should examine the safety case to judge the extent to which targets are achieved and legal limits met. Some of them are in the form of dose levels; others are expressed as frequencies or risks. The Basic Safety Level (BSL) and the Basic Safety Objective (BSO) are used in translating the TOR (R2P2) framework into targets. The BSO marks the start of the broadly acceptable level in R2P2.*

570 *The targets and legal limits are defined for normal operations, design basis analysis, individual risk and societal risk. The targets are not mandatory. However, some of the BSLs are legal limits in IRR; these are identified below as BSL(LL). The targets are guides to inspectors to indicate where there is the need for consideration of additional safety measures.*

Basic safety levels

571 *It is HSE's policy that a new facility or activity should at least meet the BSLs. However, in meeting the BSLs the risks may not be ALARP. The application of ALARP may drive risks lower. Deciding when the level of risk is ALARP needs to be made on a case-by-case basis. A proportionate approach should be used so that the higher the risk, the greater is the degree of disproportion needed before being considered ALARP, and a more robust argument would be needed to justify not implementing additional safety measures.*

572 *Some existing facilities may have been designed and constructed to different safety standards and may have deteriorated with the passage of time. Safety analyses of such facilities may show that a BSL is exceeded. Provided this BSL is not a legal limit, HSE's policy is that the level of gross disproportion in ALARP considerations would be very high; inspectors should assume it is highly likely that there will be available additional improvements to safety that are reasonably practicable. Inspectors should press dutyholders to demonstrate that a robust optioneering process has been undertaken, including considering the development of new options through research, if necessary, to control the radiological hazard. Continuing to operate while failing to meet a BSL would only be acceptable if this process demonstrated that there are no options that are reasonably practicable to reduce risks further in the short term. However, if operation is to continue then inspectors should require a clear longer-term plan to manage and reduce the risks within a period that is as short as is reasonably practicable. If these conditions cannot be met, consideration should be given to recommending regulatory action to shut down the facility or prohibit or curtail the activity, where possible. It must be remembered that the TOR[2] framework does not, in itself, provide inspectors with the basis for recommending such action, as it has no legal status. But it does help to identify when serious consideration should be given to formal enforcement action as a means of achieving compliance with legal requirements, ie reducing risks ALARP, in accordance with HSE's Enforcement Policy Statement (see the HSE website).*

Basic safety objectives

573 *The BSOs form benchmarks that reflect modern nuclear safety standards and expectations. The BSOs also recognise that there is a level beyond which further consideration of the case would not be a reasonable use of NII resources, compared with the benefit of applying the effort to other tasks. Inspectors need not seek further improvements from the dutyholder but can confine themselves to assessing the validity of the arguments that the dutyholder has presented. The dutyholder, however, is not given the option of stopping at this level. ALARP considerations may be such that the dutyholder is justified in stopping before reaching the BSO, but if it is reasonably practicable to provide a higher standard of safety, then the dutyholder should do so.*

Applying the targets and legal limits

574 *When comparing dutyholder estimates with targets, inspectors should take account of the assumptions and limitations of the analysis used.*

575 *The uncertainties in the dutyholder's safety analyses, and claims of accuracy and precision in numerical estimates, should be assessed, eg through sensitivity analysis, as appropriate.*

576 *In addition, the inspector should compare the assumptions used by dutyholders in determining their estimates against the assumptions built into the target.*

577 *When assessing safety cases against numerical targets and legal limits, inspectors should guard against being drawn into arguments about whether the calculation can be amended or the data refined to gain a small reduction in a number. This is no more than common sense: reducing an estimate by a small amount from one side of a target to the other does not suddenly make an unsafe situation safe – or a safe one unsafe. Additionally, as with any calculation, the estimates are subject to a degree of uncertainty.*

578 *Estimates of risk are often used in a cost benefit analysis (CBA) in support of an ALARP demonstration. CBA requires the costs of implementing further measures to improve safety to be compared with the costs from accidents both with and without the additional measures. These costs should include measures taken following the accident to reduce its effects on health and safety.*

The targets and TOR/R2P2

579 *The individual risk of death levels in R2P2[1] cover risks to workers and to members of the public from activities on the site, which are:*

- *Boundary between the 'tolerable' and 'unacceptable' regions for risk entailing fatality:*

  Worker: 1 in 1000 pa
  Member of the public: 1 in 10 000 pa

- *Boundary between the 'broadly acceptable' and 'tolerable' regions for risk entailing fatality:*

  Worker: 1 in 1 000 000 pa
  Member of the public: 1 in 1 000 000 pa

580 *Radiation risks arise from normal operational doses and from accidents. These contributions are treated separately.*

581 *TOR[2] discussed the effects on society of a major accident and suggested, based on the findings of the Barnes report on Hinkley Point C [11], that an event leading to one hundred to several hundred immediate and eventual deaths should not be more frequent than one in a hundred thousand years, allowing for the influence on the consequences of weather conditions. The TOR[2] approach is used in deriving the societal risk targets in these SAPs.*

582 *More detail on the rationale behind the numerical targets is found in an explanatory note[12], see the HSE website.*

Numerical targets and legal limits	Assessment against targets	NT.1
A safety case should be assessed against numerical targets and legal limits for normal operation, design basis faults, and radiological accident risks to people on and off the site.		

583 The targets in this section relate directly to the effects on people of normal operation and accidents. It may be useful to develop intermediate targets for potential accident sequences; for example many countries have a target for reactors based on core damage scenarios. Where such targets are proposed by dutyholders, they should be taken into account by inspectors, but it is essential that the overarching Principles EKP.1 to EKP.5 *(paragraph 135 ff.)* are not compromised.

584 Inspectors should not expect or require a detailed calculation for each and every target provided there is sufficient information to be able to judge that the target is likely to be achieved and the overall risk is ALARP.

Dose targets and legal limits from normal operation

585 *People may be exposed to risks from ionising radiation during the normal operation of the facility. The radiation doses may arise from direct radiation, inhalation and ingestion of radioactive material, and through the food chain as a result of discharges and disposals of radioactive waste liquids and solids.*

Normal operation – any person on the site	**Target 1**

The targets and a legal limit for effective dose in a calendar year for any person on the site from sources of ionising radiation are:

Employees working with ionising radiation:

BSL(LL): 20 mSv
BSO: 1 mSv

Other employees on the site:

BSL: 2 mSv
BSO: 0.1 mSv

Note that there are other legal limits on doses for specific groups of people, tissues and parts of the body (IRR).

Normal operation – any group on the site	**Target 2**

The targets for average effective dose in a calendar year to defined groups of employees working with ionising radiation are:

BSL: 10 mSv
BSO: 0.5 mSv

586 Dose predictions should make allowance for the uncertainties associated with calculations of internal and external exposure and make use of relevant operational data. Where dose predictions depend on dose rates from normal operations and those arising from build-up of contamination, the maximum values expected to occur during the life of the facility should be used.

587 The analysis of the predicted doses from normal operation of the facility by people working with ionising radiations should include:

a) the specific tasks involved in operating and maintaining the facility;

b) evaluations of the duration, frequency and numbers of people involved in each task; and

c) the highest individual annual dose and the group annual average dose.

588 There should be appropriate management controls in place for other people who may be in the facility or on the site, eg trainees under 18 years of age and members of the public visiting the site, to restrict their exposures in accordance with IRR. Persons under 16 years old should be prevented from working with ionising radiations (International Labour Organisation (ILO) Convention 115 (1960) Article 7.2).

589 The doses that could be received by people on the site not working with ionising radiations may be simple bounding estimates.

Normal operation – any person off the site	**Target 3**

The target and a legal limit for effective dose in a calendar year for any person off the site from sources of ionising radiation originating on the site are:

BSL(LL): 1 mSv
BSO: 0.02 mSv

Note that there are other legal limits to tissues and parts of the body (IRR).

590 Where there are multiple sites in close proximity, a dose constraint should be applied to each site to ensure that the overall dose to a person off the site is below the relevant dose limit. The IRR Guidance[10] advises constraining the dose to members of the public from each source to less than 0.3 mSv pa. HSE's view is that a single source should be interpreted as a site under a single dutyholder's control, in that it is an entity for which radiation protection can be optimised as a whole.

591 HSE is responsible for regulating the off-site doses received as a result of direct radiation shine from sources on the site. Off-site doses resulting from discharges and disposals from nuclear sites are regulated by the Environment Agency (EA) in England and Wales, and by the Scottish Environment Protection Agency (SEPA) in Scotland by means of authorisations granted under RSA.

592 The respective dose contributions from sources of radiation on and off the site will vary from site to site, but the total dose is subject to the legal dose limit above and other constraints that may be imposed by other regulatory bodies.

593 The predicted doses likely to be received from normal operation of the facility by people outside the site should be based on calculated doses to the relevant reference groups from direct radiation and from discharges of activity to air and other media.

Numerical targets for fault analysis

594 The Fault analysis section (paragraph 496 ff.) describes three forms of analysis used to establish the safety case for fault and accident conditions: design basis analysis (DBA); probabilistic safety analysis (PSA); and severe accident analysis (SAA). The results of these analyses should be judged against the numerical targets in this section.

595 The design basis analysis (DBA) is focused on the key safety measures for those initiating faults that are most significant in terms of frequency and unmitigated potential consequences. Principle FA.7 (paragraph 520 f.) sets out qualitative success criteria that the safety measures should ideally achieve in a design basis fault sequence (in accordance with the conditions specified in Principle FA.6 (paragraph 515 ff.)). The BSOs of Target 4 express clauses (b) and (c) of paragraph 521 in the form of mitigated radiological doses and have been set at a level comparable with the BSOs for operational doses in Targets 1 and 3.

596 PSA looks at the full range of fault sequences, including those where there are additional failures in the safety measures over and above those specified in Principle FA.6 (paragraph 515 f.), and including initiating faults as set out in Principle FA.12 (paragraph 531 f.). It allows full incorporation of the reliability and failure probability of the safety measures and other features of the design and operations, as described in paragraph 532. The analyses of fault progression leading to the radiological consequences of each fault sequence (whether in the design basis or not) should be carried out on a best estimate basis throughout (paragraph 535). The PSA results can be grouped to give estimates of the frequency of occurrence of consequences within specified ranges of dose, both on site and off site. Targets 6 and 8 provide BSOs and BSLs for a single facility with which these results may be compared to assist judgements on the overall adequacy of the safety measures and other plant features contributing to safety, and to identify areas in which further risk reduction may be reasonably practicable. The overall risk impact to individuals from all the facilities on a site is also to be assessed, using Targets 5 and 7.

597 The third element of the fault analysis, severe accident analysis (SAA), considers significant but unlikely accidents and provides information on their progression, both within the facility and also beyond the site boundary. This is used, for example, to inform emergency measures that may be taken to limit doses. SAA is particularly important in assessing the overall impact of the site in terms of the risks of major accidents that could lead to significant off-site consequence. This is addressed by Target 9 for societal risk.

Dose targets for design basis fault sequences

598 The BSOs are set at levels where the consequences determined from the analysis of the fault sequences are insignificant. Inspectors should expect that these levels will normally be met through installation of appropriately engineered safety measures rather than mitigating systems (see paragraph 142).

599 For 'frequent' faults (with an initiating fault frequency exceeding 1 x 10^{-3} pa), the BSLs are based on the legal limits for normal operation (see Targets 1 and 3). Higher potential doses may be shown to be ALARP for less frequent initiating faults, as indicated by the stepped relationships between BSL and frequency in Target 4. Other relationships between dose and frequencies can be used, but the model adopted should be justified. In addition to showing that adequate safety measures are in place, DBA should demonstrate that at least one physical barrier remains intact and without threat to its integrity (see paragraph 521).

Design basis fault sequences – any person	**Target 4**

The targets for the effective dose received by any person arising from a design basis fault sequence are:

On-site

BSL: 20 mSv for initiating fault frequencies exceeding 1 x 10^{-3} pa
200 mSv for initiating fault frequencies between 1 x 10^{-3} and 1 x 10^{-4} pa
500 mSv for initiating fault frequencies less than 1 x 10^{-4} pa

BSO: 0.1 mSv pa

Off-site

BSL: 1 mSv for initiating fault frequencies exceeding 1 x 10^{-3} pa
10 mSv for initiating fault frequencies between 1 x 10^{-3} and 1 x 10^{-4} pa
100 mSv for initiating fault frequencies less than 1 x 10^{-4} pa.

BSO: 0.01 mSv pa

600 For each design basis fault sequence or bounding case leading to a potential dose to any person, the radiological analysis to determine the maximum dose should be performed on a conservative basis.

601 In addition to the general requirements of Principle FA.3 *(paragraph 504 f.)*, it should be assumed for off-site releases that:

a) the person remains at the point of greatest dose for the maximum duration, although for extended faults a more realistic occupancy may be assumed after a suitable interval;
b) the conditions under which the fault is analysed has characteristics which produce the highest dose to that person; and
c) no emergency countermeasures are implemented, other than those whose implementation is shown to be highly likely.

Assessment of individual risk to people on the site from accidents

602 Targets 6 and 8 provide BSOs and BSLs for a single facility with which the PSA results may be compared to assist judgements on:

a) the overall adequacy of the safety measures and other plant features contributing to safety; and

b) identifying areas in which further risk reduction may be reasonably practicable.

603 The overall risk impact to individuals from all the facilities on a site should be assessed using Targets 5 and 7.

604 The majority of the risk to people on the site is associated with normal operation, and hence the BSL for accidents in Target 5 is set at 1 x 10^{-4} pa. The BSO value is chosen as 1 x 10^{-6} pa as being reasonably consistent with the broadly acceptable level in R2P2[1]. However, the BSL and BSO risk levels in Target 5 are substantially lower than the risk levels associated with Target 1 for employees working with ionising radiation. In those cases where the risk from normal operation is predicted to be well below the BSL of Target 1, it may be acceptable for a trade-off to be made between the normal operation risk and the accident risk, provided the dutyholder makes an acceptable case for doing so.

605 *The estimation of individual risk is subject to assumptions regarding occupancy, shift-working etc and does not clearly emphasise the importance of prevention rather than mitigation. Hence, inspectors should also consider, particularly where estimated risks are low because of such factors, whether the event incidence is ALARP. Target 6 sets reasonable expectations for event frequency against dose, where it is assumed a worker could be present.*

606 *Care should also be taken when assessing risks based on short-term exposure. Provided sufficient controls and/or alarms are in place, inspectors can take into account countermeasures. This target also provides some measure of the safety of groups of workers who might be affected in a single incident.*

Individual risk of death from on-site accidents – any person on the site	**Target 5**

The targets for the individual risk of death to a person on the site, from on-site accidents that result in exposure to ionising radiation, are:

BSL: 1×10^{-4} pa
BSO: 1×10^{-6} pa

Frequency dose targets for any single accident – any person on the site	**Target 6**

The targets for the predicted frequency of any single accident in the facility, which could give doses to a person on the site, are:

Effective dose, mSv	**Predicted frequency per annum**	
	BSL	**BSO**
2 – 20	1×10^{-1}	1×10^{-3}
20 – 200	1×10^{-2}	1×10^{-4}
200 – 2000	1×10^{-3}	1×10^{-5}
> 2000	1×10^{-4}	1×10^{-6}

607 For a fault sequence, the maximum effective dose is the predicted dose to the worker who could potentially be most exposed to ionising radiation and may be calculated using a best estimate approach. Where this is not practicable, reasonably conservative assumptions may be made. Simple assumptions about the radiation source(s), the location where the maximum potential exposure occurs, the exposure pathways and the exposure times, should generally be sufficient to give reasonable dose estimates. The effects of any mitigating action may also be taken into account if a satisfactory case has been made for them. For each fault sequence, the risk of death can then be determined using appropriate dose risk conversion factors and by taking account of the probability that an employee will be in the location where the potential exposure is greatest.

608 There should be checks to ensure that the overall BSL level of 1×10^{-4} pa in Target 5 is not exceeded, particularly if there are dose bands where the predicted frequencies approach the BSL levels. In determining the risk to the most exposed worker on site, due account should be taken of risk contributions from other facilities, where appropriate. Alternative methods and data, including different dose and frequency bands, may be used by the dutyholder to determine worker risks. Where this is done the case should be assessed in a similar way to that given above.

609 This target is not intended to include the risks associated with personnel returning to perform recovery actions after a radiation accident or emergency.

Individual risk to people off the site from accidents

610 *The basis of Target 7 is that the individual risk to people off the site from accidents on the site should be analysed. This requirement is supported by Target 8, which is facility-based, in the form of a dose ladder. The facility-based target allows consideration of safety cases where the overall effect on the risk from the site is small. However, should there be a significant change to the risks from single facilities or a major new risk is added to the site, the individual risk from the site should also be considered.*

611 The individual risk levels in R2P2[1] include the risks arising from normal operational doses. Although the legal limit of 1 mSv equates to a risk of death of a few times 1 x 10^{-5} pa, in general the normal operational doses received are significantly lower. Therefore this risk is not significant in setting the individual risk for accidents.

612 To estimate the individual risk to a person outside the site, it is necessary to take account of a wide range of parameters such as the probability that a hypothetical person will receive the dose given that the accident has occurred, allowing for wind and weather conditions and the effect of countermeasures. A particular issue is the physical position of the hypothetical person.

613 The dose ladder in Target 8 is based on the premise that the larger the potential consequences of an accident, the smaller should be its frequency. The severity of the accident is represented by the effective dose that would be received by a hypothetical person. The BSL and BSO dose bands in Target 8 relate, in an approximate fashion, to the off-site actions that could be expected in the event of an accident leading to those doses (see box after paragraph 621). These demonstrate that the dose bands are a suitable surrogate for a range of events, including risk of death, which could affect the individual from different levels of accident.

614 A single facility which just met the BSLs in the dose ladder, allowing for variability of wind direction, would give a maximum individual risk of death to a person outside the site of about 1 x 10^{-5} pa, ignoring countermeasures. This is consistent with the recommendations in the Barnes Report for Hinkley Point C[11].

615 A similar estimate can be made for a facility that just met the BSO frequencies, giving an individual risk of the order of 1 x 10^{-7} pa. These frequencies are less than the individual risk target for a site of 1 x 10^{-4} pa and 1 x 10^{-6} pa, which are in line with the levels proposed in TOR[2] and R2P2[1] for industrial hazards.

Individual risk to people off the site from accidents	**Target 7**
The targets for the individual risk of death to a person off the site, from on-site accidents that result in exposure to ionising radiation, are: BSL: 1 x 10^{-4} pa BSO: 1 x 10^{-6} pa	

616 In comparing Target 7 with Target 5, the worker on the site is also exposed to the risk from normal operational doses which are a more significant fraction for persons on-site than persons off-site.

617 In determining the individual risk from a site that contains several facilities that have been assessed independently, the inspector should refer to Principle ST.6 *(paragraph 122 f.)*.

Frequency dose targets for accidents on an individual facility – any person off the site	**Target 8**

The targets for the total predicted frequencies of accidents on an individual facility, which could give doses to a person off the site, are:

Effective dose, mSv	**Total predicted frequency per annum**	
	BSL	**BSO**
0.1 – 1	1	1 x 10^{-2}
1 – 10	1 x 10^{-1}	1 x 10^{-3}
10 – 100	1 x 10^{-2}	1 x 10^{-4}
100 – 1000	1 x 10^{-3}	1 x 10^{-5}
> 1000	1 x 10^{-4}	1 x 10^{-6}

618 The facility safety should be balanced, that is, no single class of accident should make a disproportionate contribution to the overall risk, eg of the order of one tenth of the frequency in each dose band.

619 As doses increase above about 1000 mSv then deterministic effects including the possibility of prompt death will become important. At sufficiently high doses, prompt death will dominate. At these dose levels the dose risk factor used should be 1. However, as the dose to the individual reaches levels where deterministic effects are important, the effects are likely to be wider than to a particular individual. In this case, the analysis should be assessed against the societal risk levels defined in Target 9.

620 The risks and frequencies in these numerical targets should, as far as possible, be realistic estimates for the specified accidents occurring on the facility.

621 Radiological analysis to evaluate maximum effective dose in PSA should be carried out for a hypothetical person located at the distance of the nearest habitation or one kilometre from the facility, whichever is nearer, or at the point of greatest dose if that is further away. The person should be assumed to remain directly downwind of the release point for the duration of the release. The best estimate dose should be calculated as the expected value over the possible weather conditions.

The BSL/BSO dose bands in Target 8 can be related in an approximate fashion to the off-site actions which could be expected following an accident, namely:

0.1-1 mSv

- additional off-site radiation and contamination surveys;
- possibility of advice being given to restrict the use of foodstuffs produced close to the site;

1-10 mSv

- increased off-site surveys; restrictions on the use of foodstuffs likely to be implemented;
- sheltering or issue of stable iodine may be considered in areas very close to the site;

10-100 mSv

- restrictions on foodstuffs likely to be implemented many kilometres from the site;
- sheltering or issue of stable iodine likely to be implemented;
- evacuation may be considered in areas immediately adjacent to the site;

100-1000 mSv

- restrictions on foodstuffs likely to be extensive;
- sheltering or issue of stable iodine likely to be implemented to several kilometres from the site;
- evacuation of nearby population likely to be implemented.

Societal risk

622 Severe accident analysis (SAA) considers major but very unlikely accidents and provides information on their progression, both within the facility and also beyond the site boundary. As the SAA forms an input to the PSA, it does not have a separate numerical target. However the SAA will be important in assessing the overall impact of the site in terms of the risks of major accidents that could lead to significant off-site consequences The nature of radioactive release from a major accident at a nuclear site will mean that long term, large distance stochastic effects are important, and the effect of the weather should be considered. This is addressed by Target 9 for societal risk.

623 As a measure of the societal concerns that would result from a major accident, a representative target has been defined, It is based on an accident leading to an immediate or eventual 100 or more fatalities, mainly from very low doses to very large populations leading to stochastic deaths. The target does not in itself cover all the factors related to societal concerns. In making an ALARP demonstration the consequences in terms of other societal effects must also be considered.

Total risk of 100 or more fatalities	Target 9
The targets for the total risk of 100 or more fatalities, either immediate or eventual, from on-site accidents that result in exposure to ionising radiation, are: BSL: 1×10^{-5} pa BSO: 1×10^{-7} pa	

624 The safety case should identify accidents that result in source terms that could cause 100 or more deaths. The total risk should be calculated taking account of the frequency distribution of the source terms together with probabilistic weather conditions. In estimating the risks fatalities both on-site and off-site should be included.

625 It is expected that a significant proportion of the fatalities resulting from these accidents will involve stochastic deaths, which are typically estimated using collective dose calculations. Based on studies carried out by the Health Protection Agency (HPA), the integration of these effects should be over 100 years and restricted to the UK population. These assumptions are implicit in the targets.

626 Weather conditions should be based on meteorological data appropriate to the site. Population data should be based on current demography, but reasonable expectations for changes in the future should be considered in a sensitivity analysis.

627 The ability to implement off-site countermeasures should be based on current UK and relevant international advice and should be demonstrated in the safety case. Similarly, assumptions that the on-site effects will be limited by the implementation of accident management and emergency preparedness arrangements should be demonstrated.

628 This target should be used as a guide to the extent to which more detailed analysis is warranted. Accidents where the consequences are less than 100 deaths should also be considered in the overall ALARP demonstration if their frequency is above the BSO. If accidents can occur with the potential to exceed 100 deaths, ALARP considerations must include them. In particular, if the key assumption in framing the target - that a significant proportion of the fatalities will involve stochastic deaths - is not met, inspectors should consider the implications when making regulatory decisions.

Dealing with time at risk situations

629 The risk targets set out above are given as frequencies based on annual averages. Circumstances will arise where a higher risk will exist for shorter periods of time that make the use of annualised frequency targets unrealistic. A decision has to be made as to whether additional safety measures are needed to maintain ALARP. Generally, the increased risk exists for periods much shorter than a year, but clean-up and decommissioning activities may also entail periods of elevated risk where arguments related to the timescale of the activity may be relevant.

Numerical targets and legal limits	Time at risk	NT.2
There should be sufficient control of radiological hazards at all times.		

630 An important factor in assessing short-term risks is the degree of independence between the reason for the risk being only present for a short period and the fault or hazard causing the risk. In particular, consideration should be given to:

a) independence between the initiating event and the activity or operation being undertaken;
b) the degree of control that the dutyholder has over the initiating event and the activity or operations; and
c) the degree to which the risk only arises due to the activity being undertaken (eg lifting operations).

631 Any period in which the risk is elevated (eg due to equipment unavailability or occupancy of hazardous areas) must be subject to a specific demonstration that risks are controlled ALARP. The period of elevated risk should be as short as reasonably practicable.

632 The safety case should not rely solely on numerical risk estimates or on averaging risk over a longer period of time. Good engineering and operational practices should be prominent in the case.

633 Sufficient protection based on engineering and operational considerations should be retained. If this is not reasonably practicable, adequate substitution arrangements should be considered. The extent of protection should be commensurate with the level of risk at the time that it is present.

634 Any reasonably practicable step that can be taken to eliminate or mitigate a radiological hazard should normally be taken even though the time at risk may be short.

635 During operations which impose a planned short term risk, means for monitoring the actual facility state should be in place to ensure that the mode of operation and the time during which it persists meet the assumptions in the safety case. Where possible, means to reverse the process should be in place in the event that it becomes apparent that the safety case is not being met.

636 Where reasonably practicable, contingency measures should be identified that could cope if the situation deteriorates further, including accident management arrangements.

637 High risks that would exceed BSLs if evaluated as continuous risks should be avoided except in special circumstances. These circumstances should be justified in advance. They may include situations not originally foreseen in the design of the facility, or which are unavoidable because of the need to increase risks for a short time to reach a safer state in the long term.

638 The extent of the time for which the risk is increased should not be the sole argument for acceptability that a situation is ALARP.

ACCIDENT MANAGEMENT AND EMERGENCY PREPAREDNESS

639 A nuclear facility should be so designed and operated that defence in depth against potentially significant faults or failures is achieved by the provision of several levels of protection (see Principle EKP.3, paragraph 139 f.). Accident management and emergency preparedness provides the final levels of defence (see Table 1, paragraph 143 f.) to ensure that all reasonably practicable steps have been taken to minimise the radiological consequences of any accident. Principle FP.7 (paragraph 42 f.) states that arrangements must be made for emergency preparedness and response in the case of nuclear and radiological incidents. For licensees these are addressed through various licence conditions, including Licence Condition 11, see the HSE website. In addition, for all dutyholders, the emergency preparedness regulatory framework is set out in REPPIR. Siting will also impact on emergency preparedness.

640 The objective of REPPIR and its supporting guidance is to establish a framework for the protection of workers and the public through emergency preparedness for radiation emergency. The regulations place specific duties on both dutyholders and local authorities. These duties include, among other things, the need for hazard identification and risk evaluation (HIRE), and the development and testing of dutyholders' and off-site emergency plans.

Accident management and emergency preparedness	**Design and operation**	**AM.1**
A nuclear facility should be so designed and operated to ensure that it meets the needs of accident management and emergency preparedness.		

641 Accident management strategies should be developed to reduce the risk of accidents. Fault analysis should be used to form a suitable basis for the development of these strategies. The strategies should primarily aim to prevent the breach of barriers to release or, where this cannot be achieved, to mitigate the consequences. The ultimate objective should be to return to a controlled state in which it can be maintained in a safe condition.

642 The strategies should identify any instrumentation needed to monitor the state of the plant and the level of severity of the accident, and any equipment to be used to control the accident or mitigate its consequences. Where additional hardware would facilitate accident management, this should be provided if reasonably practicable. It may also be of a different type, robustness and in a different location to that provided for normal operations.

643 Provision should be made for training plant personnel in accident management procedures and implementing the accident management strategies, utilising appropriate instrumentation and items of plant that are qualified for operation in accident environments.

644 Further guidance on accident management can be found throughout this document under the relevant technical sections.

645 Fault analysis should also be used to support the preparation of emergency plans as required by REPPIR. Further guidance on emergency plans, HIREs and detailed emergency planning zones (DEPZ) can be found in the REPPIR guidance.

RADIOACTIVE WASTE MANAGEMENT

646 The management of radioactive waste is a function potentially spanning all the stages in the life-cycle of a facility, and most of the rest of the SAPs are relevant. Some radioactive waste is also nuclear matter, and therefore the principles in the sub-section Control of nuclear matter of the engineering principles are particularly relevant (paragraph 392 ff.).

647 This section recognises that the minimisation and control of waste should be taken into account at all stages in the life-cycle of a facility, starting at the planning and design stage through operation, decommissioning and site clearance. Other principles in this section are concerned with topics such as strategies, waste characterisation, segregation, passive safety (in relation to the form of the waste itself and its storage conditions), and the requirement for records.

648 The principles in this section may also be relevant to nuclear matter, particularly where nuclear matter may be classified as waste in the future, or is to be stored on site for a significant period of time. The application of these principles to nuclear matter should be considered on a case-by-case basis taking account of the specific circumstances.

Strategies for radioactive waste

649 A strategy is an essential prerequisite for the safe and timely management of radioactive waste on a site. It is also a requirement of Government policy. It should demonstrate that relevant factors have been taken into account and should be integrated with other relevant strategies. The timescale for the achievement of passive safety is an important aspect of strategy.

650 Relevant factors when considering radioactive waste management include the quantity of waste involved, the magnitude of radiological hazard, the potential for the hazard to be realised, the potential dose uptake and the cost. There may also be considerations in respect of having to balance requirements between different waste streams.

Radioactive waste management	Strategies for radioactive waste	RW.1
A strategy should be produced and implemented for the management of radioactive waste on a site.		

651 The strategy should:

a) be consistent with Government policy, including the Government's overall policy aims on sustainable development;
b) be integrated with the decommissioning strategy and other relevant strategies, and should demonstrate that the radiological hazards posed by historic wastes are reduced progressively;
c) include a description of the dutyholder's policy and objectives for the management of radioactive waste;
d) ensure that the generation of radioactive waste is prevented or minimised;
e) cover the current and future inventory of radioactive waste, including waste arising from proposed new facilities;
f) encompass the anticipated timescales for the management of radioactive wastes, from production to disposal (where appropriate), including intermediate management steps;
g) consider a full range of options during its development. The optioneering process should take account of relevant factors, which may include those listed in Principle RW.6 concerned with timing;
h) describe, or refer to, the different options that were considered during its development and the case for the chosen option(s);
i) contain, or refer to, the plan for the management of each radioactive waste stream from generation to the final management step, including nuclear matter that may be categorised as waste in the future;
j) identify the optimum waste management route;
k) take account of off-site and on-site interdependencies, eg between waste processing facilities;
l) ensure that radioactive waste is managed in a manner that minimises the need for future processing;

m) ensure that the generation of radioactive waste of a type or form incompatible with currently available storage or disposal technology is prevented or minimised;

n) ensure that waste that cannot be managed using current techniques, or techniques under current development, is not created;

o) take account of biological, chemical and other hazards that may influence the management of radioactive waste;

p) ensure that the adequacy of the storage capacity is reviewed at appropriate intervals taking account of current and future arisings, the expected life of existing stores, and planned additional stores;

r) be compatible with facility safety cases;

s) include an outline of the safety management system and the general approach to ensure that radioactive waste will continue to be managed safely;

t) describe the significant assumptions, uncertainties and project risks associated with the achievement of the strategy, and how these will be managed;

q) be compatible with the requirements of authorisations granted by the environment agencies;

r) be reviewed at appropriate intervals and kept up to date.

Waste minimisation

652 *Radioactive waste is a product of many operations within the nuclear industry. Avoiding the creation of radioactive waste in the first instance and, secondly, minimising the generation of unavoidable waste is one of the foremost principles of good waste management. This is embodied in international standards and Government policy and should be considered and applied during the planning, design, construction, manufacture, commissioning, operational and decommissioning stages of a facility.*

Radioactive waste management	Generation of radioactive waste	RW.2
The generation of radioactive waste should be prevented or, where this is not reasonably practicable, minimised in terms of quantity and activity.		

653 Licence Condition 32 (see the HSE website) requires the rate of production of radioactive waste to be minimised. The safety case should describe specific design provisions for waste minimisation and include a demonstration that the rate of production of radioactive waste has been minimised.

654 Process and materials selection, construction methods, and commissioning, operational and decommissioning arrangements should be such so as to avoid the creation of radioactive waste or reduce to the minimum radioactive waste generated throughout the facility lifetime.

655 Factors to be considered in assessment against this principle include:

a) the facility layout and service infrastructure;

b) secondary waste generation;

c) recycling and re-use of materials;

d) decontamination of materials.

Note: The choice between re-use, decontamination, and direct disposal of waste should take account of relevant factors, including the form and disposability of the resultant waste, dose to operators, and other waste arisings and resultant discharges.

656 Trends in radioactive waste generation should be monitored and the effectiveness of applied waste minimisation measures demonstrated. There should be reviews of the opportunity for radioactive waste reduction.

Radioactive waste management	Accumulation of radioactive waste	RW.3
The accumulation of radioactive waste on site should be minimised.		

Note: this principle is mandatory under Licence Condition 32 (see the HSE website) and must be applied throughout the life-cycle of a facility.

657 The safety case should include a demonstration that the accumulation of radioactive waste has been minimised. Also, volume reduction should be considered during all stages of a facility's life-cycle.

658 Full use should be made of appropriate disposal routes to authorised sites for radioactive waste, where disposal is the most appropriate management option. This includes routes that are both authorised and covered by Exemption Orders under the Radioactive Substances Act (RSA). Authorisations under RSA require discharges of radioactive waste made into the environment to use the best practicable means to minimise the activity discharged.

Characterisation and segregation

659 The development and application of good characterisation and segregation practices for radioactive wastes provide a sound foundation for safe and effective management of these wastes from generation through to disposal. It should be recognised that for existing wastes the extent to which this may be applied could be limited.

Radioactive waste management	Characterisation and segregation	RW.4
Radioactive waste should be characterised and segregated to facilitate subsequent safe and effective management.		

660 The safety case should demonstrate provision of suitable and sufficient design features, locations, equipment and arrangements to support radioactive waste characterisation, segregation and other waste management operations.

661 Radioactive waste should be identified and an inventory established which should be reviewed and kept up to date.

662 Radioactive waste should be characterised at appropriate stages in terms of physical, chemical, radiological and biological properties so as to properly inform decisions about its subsequent management. Where waste is being packaged into a form that is intended to be suitable for final disposal, it should be sufficiently characterised to properly inform subsequent decisions about its suitability for disposal.

663 Where fissile material is present in the waste, it may be appropriate to characterise waste streams according to their intrinsic neutron absorption properties. Reduction in the uncertainty in the quantities of fissile material, neutron absorbers and moderators present in the waste may in turn lead to an increase in permissible levels of fissile material for a given waste stream.

664 Provision should be made for identifying, assessing and dealing with radioactive waste that does not meet existing process specifications or disposal criteria.

665 The requirements of subsequent radioactive waste management steps through to disposal should be considered before making a decision to mix radioactive waste streams. Mixing of radioactive waste streams, with other radioactive or non-radioactive wastes (or materials) with dissimilar or incompatible properties, should be prevented where it might compromise their future management. Mixing of radioactive wastes may be undertaken where this facilitates subsequent management, or is necessary for safety considerations.

Storage of radioactive waste and passive safety

666 The following principle addresses characteristics of the waste form and the storage facility, as both contribute to the achievement of passive safety. It is recognised that for some radioactive wastes, it will not be possible to meet in all respects this principle until the waste is retrieved and processed into a passively safe form.

Radioactive waste management	Storage of radioactive waste and passive safety	RW.5
Radioactive waste should be stored in accordance with good engineering practice and in a passively safe condition.		

667 The safety case should identify any operational limits and conditions required for safe storage. These should take account of relevant factors which may include:

a) environmental conditions, including temperature, humidity, and contaminants;
b) heat generation (from individual items and the whole store);
c) gas generation (pressurisation, flammable mixtures, deformation); and
d) radiological and criticality hazards (taking account of on-site storage and long term management, which may include disposal).

668 The safety case should be compatible with the strategy and demonstrate that radioactive waste is managed in accordance with good practice and good engineering principles. It should address radioactive waste stored in a facility and should encompass the safety-related features of both the packages and container, and the storage facility, under normal and accident conditions.

669 The safety case should demonstrate the continued safe storage of radioactive waste for the planned storage period. This should include:

a) radioactive waste for which further treatment is planned; and
b) radioactive waste in a passively safe state.

670 The safety case should include the monitoring, examination, inspection, and testing arrangements and results for the facility and the stored radioactive waste.

671 Radioactive waste storage should include the following characteristics:

a) The waste form and its container should be physically and chemically stable.
b) The package should be compatible with the long-term management strategy for the waste, which may include the need for further characterisation, treatment or conditioning, a prolonged period of storage, or disposal.
c) The radioactive waste should be immobile.
d) The need for active safety systems to ensure safety should be minimised.
e) The need for monitoring to ensure safety should be minimised.
f) There should be no need for prompt intervention to maintain the facility in a safe condition.
g) The design, construction standards, construction materials, and maintenance and inspection provisions of the storage facility should take account of the anticipated storage duration (including ageing and degradation) to ensure that the facility continues to meet its safety function.
h) The storage environment should avoid degradation that may render the waste unsuitable for long-term management or disposal.
i) The storage facility should be designed and operated so that individual packages can be inspected and retrieved within an appropriate period of time. This may include the need for reserve storage space.
j) The storage facility should be designed and operated to enable timely intervention in the event of unexpected faults or accidents.
k) Appropriate provisions should be available for dealing with radioactive waste or its packaging that shows signs of unacceptable degradation.

672 The design of packages should take account of the relevant requirements including compatibility with handling, retrieval, transport, storage and disposal..

673 Each package of radioactive waste should be uniquely identified with a marking system that will last for the storage duration.

674 Acceptance criteria should be established for admitting waste to the storage facility. These should take account of relevant factors which may include requirements for:

a) storage, handling, and retrieval;

b) the overall management strategy, including disposal where appropriate.

675 Arrangements should be made and implemented (which may include examination, testing and auditing) to ensure that incoming radioactive wastes meet the acceptance criteria. Arrangements should also be established for the safe management of any incoming radioactive waste that fails to meet the acceptance criteria.

676 Appropriate and sufficient capacity should be provided for temporary storage of radioactive waste and should include allowance for waste resulting from abnormal events.

677 Where fissile material is present in the waste, no external controls should be relied upon to prevent criticality. The safety case should demonstrate acceptable sub-criticality margins for long-term storage taking account of the uncertainties that may exist.

Passive safety timescales

678 The rationale for deciding when the radioactive waste is processed into a passive state needs to be transparent, and should be based on an appropriate balance of relevant factors. Radiological hazards should be reduced progressively, in line with Government policy.

Radioactive waste management	**Passive safety timescales**	**RW.6**
Radioactive waste should be processed into a passively safe state as soon as is reasonably practicable.		

679 The factors that influence timing may include:

a) worker and public safety, including normal operations and potential accident conditions;

b) environmental impact;

c) security;

d) the availability of disposal routes, the disposability of the proposed waste package, and the potential that reworking may be required;

e) technical practicability;

f) continuing waste arisings;

g) interaction and dependencies with other facilities;

h) possible burdens on future generations;

i) maintenance of corporate memory and records;

j) cost;

k) the precautionary approach;

l) ongoing or proposed research and development;

m) the magnitude of the radiological hazard, and progressive hazard reduction;

n) the current state and rate of deterioration of the radioactive waste, associated containers and packages, and existing storage facilities;

o) the need to minimise dependence on active safety systems, maintenance, monitoring and human intervention to ensure safety;

p) radionuclide decay or in-growth.

680 Where it is proposed to defer the processing of radioactive waste into a passively safe state, the reason for the deferral should be substantiated.

Records for management of radioactive waste

681 In addition to the need for records to adequately manage radioactive waste at present, future generations should be provided with the information they need to manage, and eventually dispose of, the radioactive waste safely. Dutyholders will need to make and maintain adequate records of the inventory of radioactive waste and management actions associated with the waste.

Radioactive waste management	Records for management of radioactive waste	RW.7
Information that might be required now and in the future for the safe management of radioactive waste should be recorded and preserved.		

682 Records should contain the information that might be required both now and in the future. Such information includes:

a) details of the ownership of radioactive waste;
b) characteristics of the radioactive waste including the radionuclide inventory, the amount, radioactive waste category, physical, biological and chemical form and associated uncertainties in the estimates of the radioactive wastes. For waste containing fissile material this should include criticality-relevant information;
c) the origin of the waste;
d) the location on site;
e) research and development;
f) development and specification of conditioning recipes and packages;
g) details of packaging;
h) operational history of processes and stores;
i) records of non-compliances with specifications;
j) records of waste disposals;
k) the safety case(s) relevant to the waste and its storage;
l) record of incidents;
m) regulatory interactions; and
n) records that might reasonably be foreseen to be required by an authorisation granted under RSA.

683 Licence Condition 32 (see the HSE website) requires records to be kept of radioactive wastes accumulated on nuclear licensed sites. The records should be maintained in a secure and accessible form for as long as the information could be of value. Records should be kept in such a way that sufficient information could be identified for both current and future needs for each individual waste package. Given the currently expected timescales for decommissioning and the provision of long-term management facilities, the storage duration for many records associated with on-site radioactive waste management might be greater than one hundred years.

DECOMMISSIONING

684 *Licence Condition 35 (see the HSE website) requires licensees to make adequate arrangements for decommissioning facilities on a nuclear licensed site. Although decommissioning is the last stage in the overall life-cycle of a facility, the need for decommissioning should be taken into account at all stages in the life-cycle, starting at the planning and design stage.*

685 *As decommissioning proceeds the radiological hazards posed by a facility will eventually reduce, particularly once the bulk of radioactive substances has been removed (although in some cases there may be a short-term increase in risk as a result of specific operations, such as when the removal of radioactive substances takes place). The need to apply the principles in a proportionate manner is therefore particularly important when each decommissioning phase is being considered (see paragraph 25 ff.). Progressively more detailed decommissioning strategies and plans would be expected as the facility moves towards, and enters, the decommissioning stage.*

686 *For civil nuclear reactors, consent must be obtained from HSE under EIADR before decommissioning can commence. In applying for consent the dutyholder must submit an Environmental Statement, which reports upon its environmental impact assessment. HSE will consult publicly on the Environmental Statement and take the views of consultees into account when deciding whether to grant consent. If any changes or extensions to a decommissioning project may result in significant adverse effects on the environment, the dutyholder must halt the relevant part of the project and apply to HSE under EIADR regulation 13 for a determination as to whether a further environmental impact assessment is required. These principles and associated guidance do not apply to assessing submissions under EIADR but to permissioning and other regulatory activities under the nuclear licensing regime.*

Design and operation

Decommissioning	Design and operation	DC.1
Facilities should be designed and operated so that they can be safely decommissioned.		

687 Account should be taken during the planning, design, construction and operational stages of the need for decommissioning and waste retrieval. This should include:

a) design measures to minimise activation and contamination, etc;
b) physical and procedural methods to prevent the spread of contamination;
c) control of activation;
d) design features to facilitate decommissioning and to reduce dose uptake by decommissioning workers;
e) consideration of the implications for decommissioning when modifications to and experiments on the facility are proposed;
f) identification of reasonably practicable changes to the facility to facilitate or accelerate decommissioning;
g) minimising the generation of radioactive waste.

Decommissioning strategies

Decommissioning	Decommissioning strategies	DC.2
A decommissioning strategy should be prepared and maintained for each site and should be integrated with other relevant strategies.		

688 The initial strategy should be produced during the planning stage of a new site or facility.

689 The overall strategy should:

a) be consistent with Government policies and strategies, including the Government's overall policy aims on sustainable development, and identify and explain any differences;
b) contain information of a type and level of detail commensurate with the site and its associated radiological hazard and the anticipated decommissioning timescale;
c) state the decommissioning policy and objectives;
d) encompass the full extent of the decommissioning liabilities on the site, including existing and planned facilities.

690 Interdependencies between plants within facilities, and between individual facilities for a multi-facility site, should be taken into account. This should include interactions between any decommissioning work and continuing facility operations.

691 The strategy should be integrated with other relevant strategies. Depending on the site concerned these might include strategies for:

a) radioactive substances, including fissile materials and radioactive wastes;
b) control and remediation of radioactively contaminated land; and
c) services, utilities and transport.

692 The strategy should describe the assumed end-state for the site.

693 The strategy should describe, or refer to, the process by which stakeholder views will be taken into account to enable confirmation or otherwise of the end-state assumed in the strategy.

694 The decommissioning strategy should describe or refer to:

a) the decommissioning options and the timescales considered;
b) the reasons for the chosen option(s); and
c) the methodology for determining the relative priority of decommissioning projects.

695 The strategy should take account of relevant factors, and show how these factors have been addressed. Such factors are likely to include those listed with Principle DC.3 (Timing of decommissioning). Other factors to be taken into account include the magnitude of radiological hazard remaining, the duration of the work, the overall status of the facility, the availability of suitably qualified and skilled workforce for each stage, and the fact that the overall objective of the work is to remove, or significantly reduce, the radiological hazard.

696 The strategy should encompass the anticipated timescales for the future operation, shutdown and decommissioning of facilities on the site, including proposed new facilities.

697 If it is proposed to defer decommissioning, the strategy should demonstrate that earlier decommissioning options are still capable of being implemented and have not been technically foreclosed.

698 The strategy should be reviewed at appropriate intervals and kept up to date.

699 The management of decommissioning wastes should be covered by the waste management strategy.

700 The strategy should describe the significant assumptions and project risks associated with its achievement, and how these will be managed.

Timing of decommissioning

701 The timing of decommissioning is an important aspect of decommissioning strategies. Many factors influence the optimum timing of decommissioning. The rationale for the timing of decommissioning should be transparent and based on an appropriate balance of relevant factors.

Decommissioning	**Timing of decommissioning**	**DC.3**
Decommissioning should be carried out as soon as is reasonably practicable taking relevant factors into account.		

702 Prompt decommissioning is the preferred option, and timing of decommissioning should be rigorously demonstrated and justified.

703 The timing of decommissioning should be considered on a case-by-case basis. Factors to be considered for their relevance should include:

a) worker and public safety;
b) environmental impact;
c) security;
d) progressive hazard reduction;
e) technical practicability;
f) radionuclide decay or in-growth;
g) ageing of facilities;
h) the volumes and categories of decommissioning wastes and the availability of waste management routes;
i) the presence of radioactively contaminated land, its potential impact on the site and the wider environment, the possibility of dispersion during the decommissioning stage and any threat that this might pose to the achievement of the assumed end-state for the facility or site:
j) interactions and dependencies with other facilities;
k) the maintenance of an appropriate safety management organisational structure;
l) the maintenance of site infrastructure;
m) the maintenance of corporate memory and records;
n) the availability of suitably qualified and experienced personnel;
o) costs, including care and maintenance and infrastructure costs;
p) future uncertainties including climate change;
q) the precautionary approach;
r) possible burdens on future generations;
s) the potential for re-use;
t) interim storage facilities.

704 Deferral of decommissioning should not be considered acceptable unless it can be substantiated that the facility can be maintained in a safe condition and can be safely decommissioned in the future.

Planning for decommissioning

705 Account needs to be taken, throughout the life-cycle of a facility, of the need to decommission the facility and to manage the wastes. This requires a strategy for a facility/site and a plan.

Decommissioning	**Planning for decommissioning**	**DC.4**
A decommissioning plan and programme should be prepared and maintained for each nuclear facility throughout its life-cycle to demonstrate that it can be safely decommissioned.		

706 If a decommissioning plan has not already been produced for an existing facility, the plan should be produced without undue delay.

707 The decommissioning plan should:

a) define the decommissioning end-state for the facility and any interim states required to achieve it; and
b) be supported by appropriate evidence, which demonstrates that decommissioning can be undertaken safely, and that the end-state (and any interim state) can be met.

708 The plan should be reviewed, updated and developed at appropriate intervals.

709 The plan should be updated before the cessation of normal operations. This should include a detailed characterisation survey to determine the extent and type of radioactive contamination,

activation, waste and other materials in the facility. In the case of unplanned early shutdown of a facility, the plan should be reviewed and, where necessary, updated as soon as is reasonably practicable.

710 The type of information and level of detail contained in the plan should be commensurate with the type and status of the facility, the associated radiological hazard, the decommissioning timescales and the practicability of obtaining the information.

711 The plan should optimise the use of existing facilities and plant during decommissioning and ensure that such facilities and plant will be available when needed. It should address any necessary changes to the existing safety systems, and the need for replacement or new facilities and plant to carry out the decommissioning operations.

712 The plan should address the type and quantity of wastes to be managed (including solid, liquid and gaseous wastes), the timescale over which the wastes will arise, and should be consistent with the waste management strategy. The plan should provide information on the proposed treatment, packaging, storage and disposal of wastes, including how decisions have been, or will be, made.

713 Institutional knowledge of the facility (including capturing the knowledge of staff) should be generated and maintained throughout its life-cycle so that it is accessible during decommissioning. This is to ensure that the design, modifications and operating history of the facility (including the impact of past operations and incidents), are identified and taken into account decommissioning plans.

714 If it is proposed to defer decommissioning, the plan should be developed sufficiently to ensure that the relevant factors to facilitate safe decommissioning in the future have been taken into account.

Passive safety

715 If decommissioning of a facility is deferred at any time, the following principle applies.

Decommissioning	**Passive safety**	**DC.5**
The facility should be made passively safe before entering a care and maintenance phase.		

716 Bulk process materials including fissile material, process liquors, and operational wastes should normally be removed from the facility.

717 The facility should undergo post-operational clean out. This may include:

a) the removal of any residual nuclear matter;
b) the immobilisation of any potentially mobile nuclear matter;
c) the removal of readily removable contaminated or activated items.

718 The facility, or parts of the facility, should be decontaminated where appropriate.

719 Before the start of a care and maintenance phase, an adequate regime should be established. It should include any requirements for maintenance, examination, inspection, and testing, and should ensure that:

a) the need for active safety systems to ensure safety is minimised;
b) the need for monitoring to ensure safety should be minimised; and
c) there should be no need for prompt intervention to maintain the facility in a safe condition.

720 Access to the facility should be controlled and entry points provided for response to incidents. Provision should be included to prevent access by flora and fauna etc.

721 The storage of any remaining radioactive substances and radioactive wastes should comply with Principle RW.5 *(paragraph 666 f.)*.

Records for decommissioning

722 Licence Condition 6 (see the HSE website) requires licensees to make adequate records to demonstrate compliance with licence conditions. This requirement includes records of decommissioning. It may be necessary for decommissioning operations to involve two or more separate phases. These phases may span a number of decades. The records required for decommissioning operations, in both the short and long term, should therefore be generated and retained over appropriate timescales. The records should be retained in a manner and form that allows them to be accessible over the required timescales.

Decommissioning	Records for decommissioning	DC.6
Throughout the whole life-cycle of a facility the documents and records that might be required for decommissioning purposes should be identified, prepared, updated and retained.		

723 Particular attention should be given to the following records:

a) the as-built facility design and subsequent modification;
b) operational history;
c) incidents;
d) radiological surveys;
e) radioactive substances and radioactive waste quantities, locations, condition and ownership, with specific focus at the end of normal operations;
f) safety cases;
g) regulatory interactions;
h) physical condition of the facility, including examination, inspection, and testing records;
i) decommissioning history;
j) decommissioning reports to show how the objectives of the decommissioning plan, including the planned end-state for the facility, have been achieved.

724 Documents and records for decommissioning purposes should be generated, retained and owned in an appropriate manner and form, taking due account of the timescales over which they may need to be retained and accessed.

725 In cases where decommissioning operations span significant periods of time, arrangements for maintaining the dutyholder's corporate memory of a facility should include retention of the knowledge of relevant staff.

Decommissioning organisation

726 Decommissioning can be a time of considerable change for an organisation and its personnel, particularly during the transition from normal operations to decommissioning. It may involve changes to staffing levels and structures, reflecting the different activities which need to be performed, and may entail an increasing use of contractors. If not properly conceived and managed, such changes may affect the dutyholder's capability to decommission the facility safely and effectively, and may create a climate of uncertainty that could challenge staff morale. Special consideration needs to be given, therefore, to the human and organisational factors that are necessary to ensure that decommissioning is undertaken safely, and in accordance with good nuclear industry decommissioning practices. The following principle applies to all phases of decommissioning, including care and maintenance, and should be read in conjunction with the section on Leadership and management for safety (paragraph 43 ff.).

Decommissioning	Decommissioning organisation	DC.7
Organisational arrangements should be established and maintained to ensure safe and effective decommissioning of facilities.		

727 The safety case should demonstrate an appropriate management organisation, and adequate personnel resources, to ensure that decommissioning can be completed safely. The continued suitability of these should be demonstrated through an organisation and staffing baseline. The design of the organisational structure will depend upon the activities to be carried out and will need to be determined on a case-by-case basis.

728 Suitable and sufficient capability to function as an intelligent customer should be demonstrated for work carried out by external contractors.

729 Competence needs for personnel responsible for undertaking decommissioning activities, including contractors, should be identified. Personnel should receive suitable training, and be suitably qualified and experienced, to carry out their duties, in accordance with the requirements of Licence Conditions 10 and 12 (see the HSE website).

Safety arrangements

730 The following principle is of particular relevance because the safety arrangements may need to be modified during decommissioning to ensure that they remain proportionate to the changing status of the facility.

Decommissioning	Safety arrangements	DC.8
The safety management system should be periodically reviewed and modified as necessary prior to and during decommissioning.		

731 The safety management system should take account of changes to the facility and associated hazards during decommissioning. Any changes should be substantiated before implementation.

732 Particular aspects for consideration include:

a) safety function categorisation of safety-related structures, systems and components;
b) safety function categorisation of administrative controls;
c) examination, inspection, maintenance and testing arrangements;
d) on-site and off-site emergency plans;
e) on-site and off-site monitoring programmes;
f) organisational structure;
g) radioactive and hazardous waste handling arrangements.

Decommissioning safety case

733 General requirements for safety cases are covered in the section on The regulatory assessment of safety cases (paragraph 70 ff.). Particular considerations arise because of the need for a decommissioning safety case to be kept up to date to demonstrate the safe decommissioning of the facility. The safety case should take account of the changes to the status of the facility and the radiological hazards posed as decommissioning progresses.

734 An outline decommissioning safety case should be prepared in conjunction with the updated decommissioning plan prior to the end of normal operations.

735 Activities that are essential to enable decommissioning to take place may increase risks temporarily (for example, remedial work, and equipment installation or waste retrievals). Such activities should be fully considered, substantiated and monitored. Principle NT.2 *(paragraph 629 f.)* provides general guidance on short-term risk.

736 Adequate records should be available to support decommissioning activities in accordance with Principle DC.6 and these should be taken into account in the decommissioning safety case. Specific focus should be given to records requirements at the end of normal operations.

737 The depth and rigour of decommissioning safety cases should be proportionate to the associated radiological hazard and should address any new or unusual activities arising during decommissioning.

738 The decommissioning safety case should be updated at appropriate points in the decommissioning programme to reflect the impact of modifications to the facility and facility state, and to address the changing nature of the radiological hazard.

739 Where there is incomplete information about the state of facility internals, and an inability to produce a reliable safety case in advance of decommissioning activities, a managed process should be devised that allows the necessary information to emerge in a controlled manner. In such cases, a staged decommissioning safety case may be appropriate to allow decommissioning progress.

CONTROL AND REMEDIATION OF RADIOACTIVELY CONTAMINATED LAND

740 The principles in this section are concerned with the safe management of radioactively contaminated land on nuclear licensed sites. HSE treats radioactively contaminated land and emplaced radioactive substances on nuclear licensed sites as accumulations of nuclear matter, unless they are, or arise from, authorised disposals.

741 The environment agencies are responsible for the regulation of disposals on, and from, nuclear licensed sites in accordance with RSA, and for the regulation of other environmental legislation. The principles therefore need to be applied in a manner that is in accordance with the Memoranda of Understanding.

Strategies for radioactively contaminated land

742 A strategy should be prepared that sets out measures to detect radioactively contaminated land and to manage any such land identified. It should be integrated with all other relevant strategies.

Control and remediation of radioactively contaminated land	**Strategies for radioactively contaminated land**	**RL.1**
Where radioactively contaminated land exists, a strategy should be produced for its control and remediation.		

743 The strategy should take account of the circumstances of known and suspected instances of radioactive contamination on the site.

744 The type of information and level of detail contained within the strategy should be commensurate with the extent, nature, and potential harm posed by the radioactive contamination.

745 The strategy should:

a) be consistent with Government policy, including the Government's overall policy aims on sustainable development;
b) include arrangements to identify any restrictions necessary to properly protect people and the environment;
c) include a process for considering options for management of the radioactively contaminated land. The strategy should describe, or refer to, the options and timescales that were considered during its development and substantiate those chosen.

746 The optioneering process should take account of factors that might have a bearing on the management of radioactively contaminated land. Examples of such factors include:

a) worker and public safety, including individuals and groups who may be currently exposed, those who may be exposed as a result of control and remediation actions, and those potentially exposed in the future;
b) the prevention or reduction of the environmental impact, now or in the future;
c) waste minimisation (see Principle RW.2 *(paragraph 652 f.)*);
d) the results of investigation, monitoring, surveillance and characterisation work;
e) continuing radioactive contamination from known sources;
f) the availability of waste treatment plant and disposal routes;
g) future requirements for investigation, monitoring, surveillance and characterisation;
h) technical practicability and the availability of technology;
i) interaction and dependencies with other facilities and other areas of radioactive contamination;
j) the means of demonstrating the effectiveness of control and remediation measures;
k) possible burdens on future generations;
l) the maintenance of corporate memory and records;
m) costs;
n) the precautionary approach;

o) future plans for the use of the site, or part of the site, and the associated timescales;

p) the biological, chemical and other hazards relating to the radioactively contaminated land;

q) past and present management actions, including any emergency response actions, eg the clean up of any spills or other known contamination events.

747 The strategy should include a description of the dutyholder's policy and objectives for the management of radioactively contaminated land, from the current time up to any de-licensing. In order of preference, the strategy should aim to:

a) retrieve contaminated material for appropriate management;

b) establish measures to achieve in-situ stabilisation; or

c) prevent and, where not practicable, minimise the migration of radioactive contamination on-site, thereby minimising radioactive waste volumes and, if this is not fully effective, minimise its spread off-site.

748 The strategy should describe the extent and nature of the radioactively contaminated land, and should be integrated with the site waste management strategy (Principle RW.1 *(paragraph 650 f.)*) and other relevant strategies.

749 The strategy should define and substantiate the proposed end-state(s) and any interim state(s) for any areas of radioactively contaminated land, and set out the anticipated timescales to achieve these states.

750 The strategy should describe the means by which radioactively contaminated land will be controlled and remediated to achieve the end-states. This may involve remedial work at various times, or leaving the radioactively contaminated land in situ where justified. Any proposed restrictions related to the end-states should be described.

751 The strategy should describe the significant assumptions and project risks associated with its achievement, and how these will be managed.

752 The strategy should be reviewed and kept up to date.

Actions to establish the existence of radioactively contaminated land

753 This principle relates to the need for dutyholders to be knowledgeable about radioactive contamination on and around the licensed site.

Control and remediation of radioactively contaminated land	**Actions to establish the existence of radioactively contaminated land**	**RL.2**
Steps should be undertaken to detect any areas of radioactively contaminated land on or adjacent to the site.		

754 A programme of ongoing investigation, monitoring and analysis should be undertaken to establish whether radioactively contaminated land is present on the site.

755 The programme should be proportionate and should take account of the current and previous use of the site (or areas of the site), records of any previous incidents or leaks (as required under Licence Condition 34, see the HSE website), any previous management actions, and any areas of suspected radioactive contamination.

Discovery of radioactively contaminated land

756 In the event of the discovery of radioactively contaminated land, priority should be given to establishing the source and terminating or minimising any leak. The radioactive contamination should be prevented from dispersing further, and appropriate measures should be taken to recover the contamination where appropriate.

Control and remediation of radioactively contaminated land	Discovery of radioactively contaminated land	RL.3
Where radioactively contaminated land is discovered, appropriate arrangements should be in place to ensure the source is identified and controlled.		

757 The arrangements should ensure that:

a) the source of the radioactive contamination is established;
b) any ongoing leakage of the nuclear matter is terminated or minimised, and measures are taken to prevent a recurrence;
c) measures are taken to prevent the radioactive contamination from dispersing, including measures to minimise the arisings of radioactive waste;
d) restrictions necessary to properly protect people and the environment are implemented;
e) the leakage is notified, recorded, investigated and reported in accordance with the requirements of the nuclear site licence; and
f) the relevant environment agency is informed.

Characterisation of radioactively contaminated land

758 The general requirements for the characterisation of radioactive waste covered in Principle RW.4 (paragraph 659 f.) might apply to radioactively contaminated land. In addition, the following principle also applies.

Control and remediation of radioactively contaminated land	Characterisation of radioactively contaminated land	RL.4
Radioactively contaminated land should be characterised to facilitate its safe and effective control and remediation.		

759 Radioactively contaminated land should be characterised so that informed decisions can be made about its management. Information may include, for example:

a) source;
b) location;
c) volume;
d) radioactive inventory;
e) physical and chemical form;
f) any associated biological, chemical or other non-radioactive contamination;
g) concentration distributions in the ground;
h) geochemical and hydro-geological properties of the subsurface including permeability, porosity, hydraulic gradients, ground-water flows, geological structure and rock fractures;
i) whether the contamination has recently arisen or whether it is historic;
j) the extent to which the contamination is spreading or has the potential to spread;
k) potential pathways and receptors associated with human or environmental exposure.
l) other potential including commercial impacts.

760 The characterisation of radioactively contaminated land should include the taking and analysis of soil, rock etc and ground-water samples from suitable locations and depths. It might also include development or use of models to predict dispersion of the contamination.

Survey, investigation, monitoring and surveillance

Control and remediation of radioactively contaminated land	Survey, investigation, monitoring and surveillance	RL.5
Radiological survey, investigation, monitoring and surveillance of radioactively contaminated land should be carried out at suitable intervals so that its characterisation is kept up to date.		

761 The objectives of the survey, investigation, monitoring and surveillance should be defined, and might include:

a) confirmation of levels and type of radioactive contamination, and rates of migration;
b) confirmation of the effectiveness of remediation measures;
c) confirmation of continued compliance with the safety case;
d) compliance with the requirements for waste management.

762 The arrangements for, and frequency of, survey, investigation, monitoring and surveillance should take account of:

a) the extent, nature, and potential harm posed by the radioactive contamination;
b) uncertainties in the characteristics of contaminated land, such as those listed in Principle RL.4;
c) the extent to which the properties of radioactively contaminated land may be changing;
d) the proximity to the site boundary;
e) dose uptake to operators undertaking the work.

763 The survey, investigation, monitoring and surveillance arrangements should be reviewed and modified to reflect changing circumstances.

Plan for control and remediation

Control and remediation of radioactively contaminated land	Plan for control and remediation	RL.6
A plan should be prepared and implemented to ensure that radioactively contaminated land is being safely controlled or remediated.		

764 The plan should describe the proposed end-state of the site, or area of the site, and any interim states required to achieve it.

765 The type of information and level of detail contained within the plan should be commensurate with the extent, nature, and potential harm posed by the radioactive contamination.

766 The plan should cover the control and remedial measures for the site, or area of site, which may include:

a) retrieval;
b) soil treatment;
c) in situ stabilisation;
d) surface caps or covers;
e) natural or artificial containment barriers;
f) hydro-geological and hydraulic controls;
g) ground-water treatment;
h) control of personal access;
i) control of local flora and fauna;
j) restrictions necessary to properly protect people and the environment.

767 The plan should be substantiated by appropriate safety and environmental analyses; identify the type and quantity of waste to be managed; and be consistent with the site waste management strategy (see Principle RW.1 *(paragraph 650 f.)*).

768 The plan should describe the arrangements for investigation, monitoring, surveillance and characterisation work to verify the extent and levels of radioactively contaminated land, both before and after remediation work. These arrangements should be substantiated.

769 The plan should be reviewed and kept up to date.

Records for radioactively contaminated land

Control and remediation of radioactively contaminated land	**Records for radioactively contaminated land**	**RL.7**
Arrangements should be made for recording and preserving the information that may be required both now and in the future for the safe control and remediation of radioactively contaminated land.		

770 Licence Condition 34 (see the HSE website) requires that the leak or escape of radioactive material or radioactive waste is detected, notified, recorded, investigated and reported. The following records need to be maintained and preserved to facilitate the control and remediation of radioactively contaminated land:

a) results of investigation, characterisation and monitoring work;
b) records of any incidents, leakages etc resulting in radioactively contaminated land, and of any management actions;
c) reports on the remediation of contaminated land;
d) any other relevant information related to the history and use of the site.

771 Some of the requirements in Principle RW.7 *(paragraph 681 f.)*, which addresses records for radioactive waste, may also be relevant.

Safety cases for radioactively contaminated land

772 General requirements for safety cases are covered in the section on The regulatory assessment of safety cases (paragraph 70 ff.). The safety cases should be prepared to address radioactively contaminated land that is compatible with the strategy. Existing safety cases that might be affected by the presence of radioactively contaminated land should be reviewed so as to take the contamination's existence into account. A safety case should be proportionate taking into account of the extent, nature and potential harm posed by the radioactive contamination, and the extent to which it may be spreading or have the potential to spread.

773 Information contained in the safety case should include the following, where relevant:

a) details of the extent and nature of the radioactively contaminated land, and geological and hydro-geological conditions, taking account of investigation, monitoring, surveillance and characterisation results (see Principle RL.4);
b) a demonstration that modern standards and good engineering practice have been applied in the control and remediation of contaminated land;
c) an assessment of potential harm taking account of environmental pathways. Such routes might include: personal contamination; direct radiation, exposure to airborne activity; and water-borne activity beyond the site boundary. The assessment should take account of uncertainties;
d) a substantiation of any restrictions necessary to properly protect people and the environment;
e) investigation, monitoring and surveillance arrangements (including sampling devices and the location of boreholes);
f) a description of any restrictions associated with the management of radioactively contaminated land eg arising from potential dose uptake during monitoring;
g) reference to any requirements of the relevant environment agency, and environmental law.

774 The safety case should be consistent with the strategy and plan for radioactively contaminated land and should take account of biological, chemical and any other hazards that may be associated with the control and remediation of radioactively contaminated land.

Avoidance of construction or installation on radioactively contaminated land

Control and remediation of radioactively contaminated land	Avoidance of construction or installation on radioactively contaminated land	RL.8
Radioactively contaminated land should first be remediated before any construction of new facilities takes place.		

775 Where new facilities are proposed to be constructed on, or in the vicinity of, an existing nuclear licensed site:

a) it should be surveyed to establish if there is any radioactive contamination in the vicinity of the proposed construction site;

b) any radioactively contaminated land should be remediated to appropriate standards prior to construction;

c) any construction in a location that would impede the control and remediation of any radioactively contaminated land should be avoided; and

d) any proposals not to remediate prior to construction should be substantiated and demonstration provided that alternative options have been properly considered and rejected.

GLOSSARY

Absorbed dose

The quantity of energy imparted by ionising radiation to unit mass of matter such as tissue. Measured in Grays, 1 Gray (Gy) = 1 joule per kilogram (NRPB[13]).

Accident

Any unintended event, including operator errors, equipment failures or other mishaps, the consequences or potential consequences of which are not negligible from the point of view of protection or safety (IAEA Safety Glossary[14]).

In this document, and when used generally, the term 'accident' includes any undesired circumstances which give rise to ill health or injury; damage to property, plant, products or the environment; production losses or increased liabilities.

When referring to nuclear safety, 'accident' refers to a fault sequence resulting in a dose greater than 0.1 mSv to a worker, or greater than 0.01 mSv to a person outside the site, or in a substantial unintended relocation of radioactive substances within the facility.

Accident management

The strategies which are developed to reduce the risks arising from accidents, and bring the facility to a safe, controlled, state.

Alarm

An automatic visual or audible indication to personnel of when a specific plant variable or condition has reached a pre-set limit or state.

Availability

The fraction of time for which a system is capable of fulfilling its intended purpose (IAEA Safety Glossary[14]).

Barrier

A means to:

- prevent or inhibit the movement of people or radioactive substances, or some other phenomenon (eg fire);
- provide shielding against radiation;
- protect against some other potentially hazardous event.

Best estimate

When used to describe analysis, this refers to an analysis expected to provide the most accurate description of the fault and its consequences that could be achieved within the limitations of the analytical model employed without any deliberate bias being introduced.

When used to describe the data, it refers to the most accurate value of the data item derived from experiment, operating experience, judgement etc as appropriate. Where there is inadequate evidence, and no credible best estimate is possible, then bounding or conservative values should be used.

Bounding case

The case that represents the extreme consequences of a class of accidents.

Capability

The description in qualitative and quantitative terms of the complete function(s) provided by a component, sub-system or system, including information on:

(a) the operating limits within which the function(s) can be sustained; and

(b) the damage limits beyond which permanent degradation of functions must be assumed.

Care and maintenance

A phase within the decommissioning stage of a facility, for which the deferral of further decommissioning has been substantiated, and for which safety is maintained by passively safe means and an appropriate maintenance, examination, inspection and testing programme.

Class of accident

A group of fault sequences that follow paths that are sufficiently similar to justify analysis of the sequences together as a class.

Collective effective dose

The quantity obtained by multiplying the average effective dose by the number of people expose to a given source of ionising radiation. Measured in man-Sieverts (Sv) (NRPB[13]).

'Collective effective dose' is frequently abbreviated to 'collective dose'.

Commissioning

The process by means of which systems and components of facilities and activities, having been constructed, are made operational and verified to be in accordance with the design and to have met required performance criteria (IAEA Safety Glossary[14]).

Common cause failure (CCF)

Failure of two or more structures, systems or components due to a single specific event or cause (IAEA Safety Glossary[14]).

Common mode failure (CMF)

Failure of two or more structures, systems or components in the same manner or mode due to a single event or cause (IAEA Safety Glossary[14]).

Conservative estimate

The use of models, data and assumptions which would be expected to lead to a result that bounds the best estimate (where known) on the safe side. The degree of conservatism should be proportionate to the level of uncertainty, and the overall significance of the estimate to the safety case.

Containment

Methods or physical structures designed to prevent the dispersion of radioactive substances (IAEA Safety Glossary[14]).

Countermeasures

An action aimed at alleviating the radiological consequences of an accident (IAEA Safety Glossary[14]).

Criticality incident

The accidental occurrence of a fission chain reaction.

Decommissioning

Administrative and technical actions taken to reduce hazards progressively and thereby allow the removal of some or all of the regulatory controls from a facility.

Decommissioning strategy

A document providing an overview of the approach to the decommissioning of a site (or a group of similar sites) encompassing all existing and proposed new facilities, setting down the overall decommissioning objectives as far as the assumed end-state, taking account of relevant factors, and integrated with other relevant strategies.

Design basis

The range of conditions and events that should be explicitly taken into account in the design of the facility, according to established criteria, such that the facility can withstand them without exceeding authorised limits by the planned operation of safety systems (IAEA Safety Glossary[14]).

Design basis fault

A fault (sequence) which the plant is designed to take or can be shown to withstand without unacceptable consequence, by virtue of the facility's inherent characteristics or the safety systems.

Design life The period of time during which a facility or component is expected to perform according to the technical specifications to which it was produced (IAEA Safety Glossary[14]).

Detailed emergency planning zone The defined zone surrounding an installation, within which emergency arrangements to protect the public are planned in detail, see REPPIR regulation 9 and associated guidance.

Diversity The presence of two or more systems or components to perform an identified function, where the systems or components have different attributes so as to reduce the possibility of common cause failure, including common mode failure (IAEA Safety Glossary[14]).

Dose See Effective dose.

Dutyholder A person or corporate body who has a duty in law.

Effective dose The quantity obtained by multiplying the equivalent dose to various tissues and organs by a weighting factor appropriate to each and summing the products. Measured in Sieverts (Sv) (NRPB[13]).

'Effective dose' is frequently abbreviated to 'dose'.

Emergency preparedness The capability to take actions that will effectively mitigate the consequences of an emergency for human health and safety, quality of life, property, and the environment (IAEA Safety Glossary[14]).

Employees working with radiation The term 'employees' is used in IRR. Working with ionising radiation has the same interpretation as in IRR, namely work involving the production, processing, handling, use, holding, storage, transport or disposal of radioactive substances (IRR).

For the purposes of assessment, employees can be regarded as the same as workers.

Essential service Essential services are all those resources necessary to maintain the safety systems in an operational state at all times and may include electricity, gas, water, compressed air, fuel and lubricants.

Equivalent dose The quantity obtained by multiplying the absorbed dose by a factor to allow for the differing effectiveness of the various ionising radiations in causing harm to tissue Measured in Sieverts (Sv) (NRPB[13]).

Equipment qualification Generation and maintenance of evidence to ensure that equipment will operate on demand, under specified service conditions, to meet system performance requirements (IAEA Safety Glossary[14]).

External hazard External hazards are those natural or man-made hazards to a site and facilities that originate externally to both the site and the process, ie the dutyholder may have very little or no control over the initiating event.

Facility A facility is that part of a nuclear site identified as being a separate unit for the purposes of nuclear or radiological risk. This may be a single reactor, a group of processing plants as on a nuclear fuel-cycle facility or a dock and its support systems containing a naval reactor plant.

The term 'facility' includes both the terms 'nuclear installations' as defined in the Nuclear Installations Act 1965 (as amended) and the term 'plant' as used in nuclear site licences granted by HSE.

Failure	A failure has occurred when a structure, system or component fails to meet its safety function, or functions spuriously.
Failure modes	The manner or state in which a structure, system or component fails (IAEA Safety Glossary[14]).
Fault	Any unplanned departure from the specified mode of operation of a structure, system or component due to a malfunction or defect within the structure, system or component or due to external influences or human error.
Fault condition	When used without qualification, this means design basis fault conditions and includes, where appropriate and as far as reasonably practicable, beyond design basis conditions.
Fault sequence	A combination of an initiating fault and any additional failures, faults and internal or external hazards which have the potential to lead to accidents.
Government	For the purposes of this document, the term 'the Government' means the 'the UK Government and/or the Devolved Administrations, as appropriate'.
Guaranteed/non-interruptible Supply	Guaranteed, non-interruptible (or no-break) supplies are those systems that are designed to ensure that in the event of grid/mains failure there is a seamless transition of electrical supply to an alternative supply, with no voltage drop.
Geometrical constraint (criticality safety)	Control of the geometrical configuration in such a way that the neutron leakage of the system is sufficient to prevent criticality.
Hazard	The potential for harm arising from an intrinsic property or disposition of something to cause detriment (R2P2[1]). *See also internal and external hazards.*
Hazard potential	The propensity for the harm from a hazard to be realised.
Hypothetical person	An individual who is in some fixed relation to the (radiological) hazard, eg the person most exposed to it, or a person living at some fixed point or with some assumed pattern of life (R2P2[1]).
Incident	An undesired circumstance or 'near miss' that has the potential to cause an accident.
Individual risk	The risk to any individual of premature death from cancer or other radiation effects as a result of exposure to ionising radiation during any one year, whether the death occurs during the year of exposure or subsequently.
Inherent safety	Preventing a specific harm occurring by using an approach, design or arrangement that ensures that the harm cannot happen, for example a criticality safe vessel. *This is not the same as passive safety.*
Initiating fault	The starting event of a fault sequence. This may be an internal failure or a fault caused by an internal or external hazard or by human action. This does not include pre-existing latent failures that may be revealed when safety equipment is called upon to function during a fault sequence.
Intelligent customer	An intelligent customer is the capability of an organisation to have a clear understanding and knowledge of the product or service being supplied.
Internal hazard	Internal hazards are those hazards to plant and structures that originate within the site boundary and over which the dutyholder has control over the initiating event in some form.

Ionising radiations

For the purposes of radiation protection, radiation capable of producing ion pairs in biological materials (IAEA Safety Glossary[14]).

Licensed site

A site in respect of which a Nuclear Site Licence has been granted by HSE under the Nuclear Installations Act 1965 (as amended), whether or not that Licence remains in force (NIA).

Licensee

The body corporate that has been granted a Nuclear Site Licence under the Nuclear Installations Act 1965 (as amended), which permits it to carry out a defined scope of activities on a delineated site (NIA).

Life-cycle

Includes all the stages in the life of an undertaking in the nuclear industry requiring a nuclear licence under NIA, or other authorisation.

This includes activities from conception through design, build, commissioning, operation, maintenance, closure, decommissioning, disposal of waste, to the return of a site to a safe state and de-licensing.

Normal operation

Operation within specified operational limits and conditions. (IAEA Safety Glossary[14]).

Nuclear matter

Subject to any exceptions prescribed in NIA and the Nuclear Installations (Excepted Matter) Regulations 1978, nuclear matter is:

(a) any fissile material in the form of uranium metal, alloy or chemical compound (including natural uranium), or of plutonium metal, alloy or chemical compound, and any other fissile material which may be prescribed; and

(b) any radioactive material produced in, or made radioactive by exposure to the radiation incidental to, the process of producing or utilising any such fissile material as aforesaid.

Operating modes

The states that the facility may be in during the course of normal operation.

Passive safety

Providing and maintaining a safety function without the need for systems to be actively initiated or for operator intervention, or other safety system support features.

In the context of decommissioning and the storage of nuclear matter, providing and maintaining a safety function by minimising the need for active safety systems, monitoring or prompt human intervention.

A passive safety system is not necessarily inherently safe.

Physical barrier

See Barrier.

Precautionary approach

In line with UK Government policy, the Precautionary Principle is interpreted in practice as a flexible precautionary approach.

In relation to assumptions placed on likelihood and consequences, the degree of conservatism adopted should be proportionate and responsive to:

- the level of complexity and uncertainty;
- developments and progress in understanding and knowledge aimed at reducing the complexity and uncertainty;
- the particular circumstances surrounding the technology and its application eg managerial, operational, societal;
- the benefits and opportunities accruing from the application of this technology.

Primary/secondary containment

The primary containment is the barrier that is likely to experience the first and most severe safety functional demand in the event of normal, abnormal or accident conditions. Other containments (secondary, tertiary etc) are additional defence in depth provisions considered necessary to meet overall containment system functionality requirements.

Protection system

A system that monitors the operation of a facility and which, on sensing an abnormal condition, automatically initiates actions to prevent an unsafe or potentially unsafe condition (based on IAEA Safety Glossary[14]).

Qualification

The process of demonstrating that a structure, system or component is fit for its intended purpose.

Quality assurance

The function of a management system that provides confidence that specified requirements will be fulfilled (IAEA Safety Glossary[14]).

Quality management system

A management system to direct a unit and control an organisation with regard to quality; a combination of resources and means with which quality is realised (ISO 9000).

Radiation accident

An accident where immediate action would be required to prevent or reduce the exposure to ionising radiation of employees or any other persons and includes a radiation emergency (REPPIR).

Radiation emergency

Any event (other than a pre-existing situation) which is likely to result in any member of the public being exposed to ionising radiation arising from that event in excess of any of the doses set out in Schedule 1 (of REPPIR) and for this purpose any health protection measure to be taken during the 24 hours immediately following the event shall be disregarded (REPPIR).

Radioactively contaminated land

Land containing radioactive contamination that would preclude HSE giving notice in writing that in its opinion there ceases/has ceased to be any danger from ionising radiations on the site, or part of the site.

Radioactively contaminated land plan

A document containing detailed information on the control and remediation of the areas of radioactively contaminated land on a site.

Radioactively contaminated land strategy	A document providing an overview of the identification, control and remediation of radioactively contaminated land on a site, setting down the overall objectives as far as the assumed end-state, taking account of waste minimisation, other relevant factors, and integrated with other relevant strategies.
Radioactive material	Radioactive material is as defined in RSA.
Radioactive substance	Radioactive substance is as defined in IRR.
Radioactive waste	Radioactive waste is as defined in RSA.
Radioactive waste strategy	A document providing an overview of the management of existing and future radioactive waste on a site as far as the final management step, demonstrating that radiological hazards posed by historic wastes will be progressively reduced, taking account of interdependencies between different waste streams, waste minimisation, and other relevant factors, and integrated with other relevant strategies.
Redundancy	Provision of alternative (identical or diverse) structures, systems or components, so that any one can perform the required function regardless of the state of operation or failure of any other (IAEA Safety Glossary[14]).
Reference group	A group comprising individuals whose exposure to a source is reasonably uniform and representative of that of the individuals in the population who are the more highly exposed to that source (EURATOM[16]).
Reliability	The probability that a system or component will meet its minimum performance requirements when called upon to do so (IAEA Safety Glossary[14]).
Remediation	As applied to radioactively contaminated land, any measure that may be carried out to reduce the radiation exposure from existing contamination of land areas through action applied to the contamination itself (the source) or to the exposure pathways to humans (IAEA Safety Glossary[14]).
Risk	Risk is the chance that someone or something is adversely affected in a particular manner by a hazard (R2P2[1]).
Safety	In this document, 'safety' refers to the safety of persons in relation to radiological hazards in this document.
Safety actuation system	The collection of equipment required to accomplish the necessary safety actions when initiated by the protection system (IAEA Safety Glossary[14]).
Safety case	In this document, 'safety case' refers to the totality of a licensee's (or dutyholder's) documentation to demonstrate safety, and any sub-set of this documentation that is submitted to NII.
Safety culture	The assembly of characteristics and attitudes in organisations and individuals which establishes that, as an overriding priority, protection and safety issues receive the attention warranted by their significance (IAEA Safety Glossary[14]).
Safety function	The safety function of a structure, system or component is the specific function required to maintain the facility within the safe operating limits and conditions determined by the fault analysis.

Safety measure

A safety system, or a combination of procedures, operator actions and safety systems that prevents or mitigates a radiological consequence, or a specific feature of plant designed to prevent or mitigate a radiological consequence by passive means.

Safety-related system

An item important to safety that is not part of a safety system (IAEA Safety Glossary[14]).

Safety system

A system that acts in response to a fault to prevent or mitigate a radiological consequence.

Safety schedule

A schedule or other suitable means that identifies the minimum safety system requirements for each of the initiating faults, including internal and external hazards, identified within the design basis.

A safety schedule may also be called a safety system or engineering or protection or fault and protection schedule. Other suitable means may include the use of configuration diagrams.

Safety system support features

The collection of equipment that provides services such as cooling, lubrication and energy supply required by the protection system and the safety actuation systems (IAEA Safety Glossary[14]).

Secondary waste

Waste that results from applying treatment, handling or storage technology to a waste or product stream of a process.

Segregation

Dependent on context:

1. The physical separation of components and systems, by distance or by some form of barrier that reduces the likelihood of common cause failures.
2. An activity where waste or materials (radioactive or exempt) are separated or kept separate according to radiological, chemical and/or physical properties which will facilitate waste handling and/or processing. (IAEA Safety Glossary[14])

Service

A support service or utility serving one or more facilities, such as health physics and emergency services, or utilities such as steam, electricity, water, nitrogen or compressed air, that is required for the maintenance of safety.

Severe accident

A fault sequence which leads either to consequences exceeding the highest radiological doses given in the BSLs of Target 4, or to a substantial unintended relocation of radioactive material within the facility which places a demand on the integrity of the remaining physical barriers.

Shielding

A structure or material placed around a source of radiation to reduce the radiation dose rate in the vicinity.

Societal concerns

Societal concerns are the risks or threats from hazards which impact on society and which, if realised, could have adverse repercussions for the institutions responsible for putting in place the provisions and arrangements for protecting people.

Societal effects

A term used to describe those societal concerns that are capable of quantitative prediction such as numbers of deaths or injuries, numbers of people evacuated, area of land contaminated and general economic loss.

Societal risk

The risk of an accident causing the death of a specified number of people in a single event from a single major industrial activity, ie an activity from which risk is assessed as a whole and is under the control of one company in one location, or within a site boundary.

Source term

Data on quantities of radioisotopes released in an accident, location of release and other related parameters needed as an input into radiological consequence calculations, as distinct from the ambient conditions determining the dispersion.

Structure, system and component (SSC) important to safety

In this document a structure, system or component (SSC) important to safety is interpreted as one which provides a safety function (direct role), or one whose failure could adversely affect an SCC which provides a safety function (indirect role).

Task analysis

Systematic delineation and examination of the psychological and physical demands placed upon a human operator by specified task requirements.

Type-testing

A comprehensive set of tests applied to equipment that:

a) demonstrates that the equipment does not have any inherent design faults that could adversely affect its performance, life or reliability;

b) checks that the manufacturer's production processes, including testing, setting-up and quality assurance, are satisfactory;

c) establishes the stability of the equipment when subjected to various influence factors such as supply voltage changes, temperature and humidity changes, electromagnetic interference;

d) provides evidence that it meets its specification.

Validation

Dependent on context:

1. The process of determining whether a product or service is adequate to perform its intended function satisfactorily.

   Computer system validation: The process of testing and evaluation of the integrated computer system (hardware and software) to ensure compliance with the functional, performance and interface requirements.

   Model validation: The process of determining whether a model is an adequate representation of the real system being modelled, by comparing the predictions of the model with observations of the real system.

   System code validation: Assessment of the accuracy of values predicted by the system code against the relevant experimental data for the important phenomena expected to occur.

2. Confirmation by means of objective evidence that the requirements for a specific intended purpose and use or application have been fulfilled (IAEA Safety Glossary[14]).

Verification

Dependent on context:

1. The process of determining whether the quality or performance of a product or service is as stated, as intended or as required.

   Computer system verification: The process of ensuring that a phase in the system life-cycle meets the requirements imposed on it by the previous phase.

   Model verification: The process of determining whether a computational model correctly implements the intended conceptual model or mathematical model.

   System code verification: Review of source coding in relation to its description in the system code documentation.

2. Confirmation by means of objective evidence that specified requirements have been fulfilled (IAEA Safety Glossary[14]).

Veto

Inhibition of a safety system.

Whole body dose

The sum of the effective dose from external radiation and the committed effective dose from intakes of radioactive material.

ABBREVIATIONS

ACoP	Approved code of practice
ALARA	As low as reasonably achievable
ALARP	As low as reasonably practicable
Bq	Becquerel. Unit of activity of a quantity of radioactive material. 1 Bq is equal to 1 disintegration per second
BPEO	Best practicable environmental option
BSL	Basic safety level
BSL(LL)	Basic safety level (legal limit)
BSO	Basic safety objective
CBA	Cost benefit analysis
CCF	Common cause failure
CID	Criticality incident detection
CSCA	Component and structure condition assessment
DBA	Design basis analysis
DBE	Design basis event
DEPZ	Detailed emergency planning zone
DNSR	Defence Nuclear Safety Regulator
EA	Environment Agency
EIADR	The Nuclear Reactors (Environmental Impact Assessment for Decommissioning) (Amendment) Regulations 2006
EMIT	Examination, maintenance, inspection and testing
ILO	International Labour Organisation
HIRE	Hazard identification and risk
HPA	Health Protection Agency
HSE	Health and Safety Executive
HSC	Health and Safety Commission
The HSW Act	The Health and Safety at Work etc Act 1974
IAEA	International Atomic Energy Agency
IRR	Ionising Radiations Regulations 1999
The Management Regulations	The Management of Health and Safety at Work Regulations 1999
MOD	Ministry of Defence
NDA	Nuclear Decommissioning Authority
NEPLG	Nuclear Emergency Planning Liaison Group
NII	Nuclear Installations Inspectorate
NIA	The Nuclear Installations Act 1965 (as amended)
NSD	Nuclear Safety Directorate
OBE	Operating basis earthquake
OCNS	Office of Civil Nuclear Security
pa	Per annum
PSA	Probabilistic safety analysis
PSR	Periodic safety review
QA	Quality assurance
R2P2	Reducing risks, protecting people: HSE's decision making process[1]

RPV	Reactor pressure vessel
REPPIR	Radiation (Emergency Preparedness and Public Information) Regulations 2001
RSA	Radioactive Substances Act 1993
SAP	Safety assessment principle(s)
SFAIRP	So far as is reasonably practicable
SEPA	Scottish Environment Protection Agency
SSC	Structures, systems and components
Sv	Sievert(s). The unit of equivalent dose and its derivatives, eg effective dose and committed effective dose
TAG	Technical assessment guide
TOR	The tolerability of risk from nuclear power stations[2]
WENRA	Western European Nuclear Regulators' Association

ANNEX 1: NII REGULATORY INTERFACES

Depending on the nature of a safety case being assessed, there may be other regulatory processes that need to be taken into account when recommending a permissioning or enforcement action. The regulatory bodies whose processes NII most frequently interface with during assessment are listed in this annex, together with details of the nature of the regulatory interface.

Environment Agency/Scottish Environment Protection Agency

HSE is responsible for regulating nuclear safety, including the safe management, conditioning and storage of radioactive waste on nuclear licensed sites. EA and SEPA are responsible in England and Wales, and in Scotland respectively, for regulating the discharges to the environment and disposal of radioactive waste on or from nuclear licensed sites.

HSE, EA and SEPA have a number of areas of mutual interest, for example:

a) siting of any new facility for the disposal of radioactive waste;
b) construction of new facilities on nuclear licensed sites, or modification of existing facilities, which have implications for discharges to the environment or for the disposal of solid radioactive waste;
c) authorisation of radioactive discharges;
d) decommissioning and de-licensing of existing facilities, including Quinquennial Reviews;
e) HSE's Periodic Safety Reviews;
f) EA/SEPA Periodic Authorisation Reviews;
g) radioactive waste management (both short and long term);
h) inspections, enforcement and incident investigation on matters which may affect the other regulator.

Each regulator takes full account of the others' regulatory responsibilities during regulatory decision making. The separate but complementary responsibilities for the protection of the public and the workforce from ionising radiation can be expressed as follows: HSE's responsibilities being centred on the regulation of the source of direct radiation shine from normal operations and of the prevention of accidental releases of radioactivity; and EA and SEPA's responsibilities being centred on the regulation of discharges and disposals from normal operations.

Separate, but similar, Memorandums of Understanding (MoU) provide frameworks for the ways of working, and the interaction between HSE and each of the environmental regulators.

Office of Civil Nuclear Security (OCNS)

OCNS conducts its regulatory activity on behalf of the Secretary of State for Trade and Industry under the authority of the Nuclear Industries Security Regulations 2003 (NISR). The security regime's purposes are to prevent theft of nuclear material or sabotage of nuclear facilities, to safeguard sensitive nuclear technology and information and thereby to help prevent nuclear proliferation, and to safeguard other protectively-marked Government information held by the civil nuclear industry. In pursuit of these purposes, OCNS sets and promulgates standards to the nuclear industry in the areas of physical, personnel, information and IT security, and carries out inspections to check for compliance with these standards.

HSE and OCNS have a common interest in ensuring that security and safety arrangements are adequate and effective in preventing the theft or misuse of nuclear material, and actions by individuals or groups, causing harm or damage. These arrangements contribute to the wider aims of protecting the health and safety of employees, contractors and general public from the hazards of ionising radiation, promoting the Government's nuclear non-proliferation obligations and the protection of national security.

In pursuit of this common interest:

a) NII provides information to OCNS, derived from its knowledge of nuclear licensed sites and their safety cases, to enhance the latter's awareness of nuclear safety and radiological safety, both generally and in relation to vulnerable high-risk plant and systems at particular sites. OCNS provides security information in its possession to NII relevant to health and safety considerations at licensed nuclear sites, subject to any statutory or confidentiality restrictions; and
b) NII and OCNS consult and exchange information at the earliest practicable stage in the consideration of relevant new projects or proposed changes at licensed nuclear sites, or following a significant breach of licence conditions or regulated security arrangements, with a view to identifying the necessary safety and security arrangements or changes before requirements are placed on licensees.

The Defence Nuclear Safety Regulator

The Defence Nuclear Safety Regulator (DNSR) is the MoD regulator of nuclear and radiological safety for the defence nuclear programmes (comprising the Naval Nuclear Propulsion Programme and the Nuclear Weapons Programme) with a primary focus on regulating those aspects of the defence nuclear programmes that are exempt from legislation (including the design and operational deployment of propulsion plant and weapons). In so doing, DNSR provides assurance to the Secretary of State for Defence, through the Defence Nuclear Safety Board, that standards of nuclear and radiological safety throughout the defence nuclear programmes are, so far as reasonably practicable, at least as good as those required by legislation. In carrying out this role, DNSR works very closely with the relevant statutory regulators, particularly HSE/NII, EA, SEPA and the Department for Transport, and similarly empowered MoD regulators.

DNSR has introduced a system of Authorisation of dutyholders in direct control of nuclear activities within these programmes, which closely parallels NII's licensing system. Authorisation provides a similar permissioning regime to DNSR as that afforded to NII by the licence conditions and provides assurance that the Secretary of State's Policy Statement is being complied with.

Accordingly, NII and DNSR have agreed to work together to regulate the defence nuclear programmes to:

- Maximise the effectiveness of joint regulation.
- Minimise the duplication of regulatory resource.
- Achieve the most effective use of available regulatory resource.
- Develop a single coherent set of safety standards and goals.
- Improve the regulatory decision making process.
- Improve communications with stakeholders.

The general framework of this relationship is covered within the MoD/HSE agreement and the associated Letter of Understanding, which describes the principles and practices of the working level relationship between NII and DNSR and the joint regulatory framework.

REFERENCES

1 *Reducing risks, protecting people: HSE's decision making process* HSE Books 2001 ISBN 0 7176 2151 0. Web version: www.hse.gov.uk/risk/theory/r2p2.pdf

2 *The tolerability of risk from nuclear power stations* The Stationery Office 1992 ISBN 0 11 886368 1 Web version: www.hse.gov.uk/nuclear/tolerability.pdf

3 *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 0 7176 2488 9

4 *Safety assessment and verification for nuclear power plants* IAEA Safety Standards Series No. NS-G-1.2 2001

5 *Periodic safety review of nuclear power plants safety guide* IAEA Safety Standards Series No. NS-G-2.10 2003

6 *Fundamental safety principles* Draft IAEA Safety Standard DS 298 draft 32 IAEA 2006

7 *Successful health and safety management* HSG65 (Second edition) HSE Books 1997 ISBN 0 7176 1276 7

8 *Columbia Accident Investigation Board Report* August 2003. Web version: www.nasa.gov/columbia/home/CAIB_Vol1.html

9 *Safety of nuclear power plants: design* IAEA Safety Standards Series No. NS-R-1 2000

10 *Work with ionising radiation. Ionising Radiations Regulations 1999. Approved Code of Practice and guidance* L121 HSE Books 2000 ISBN 0 7176 1746 7

11 *The Hinkley Point Public Inquiries: A Report by Michael Barnes QC* The Stationery Office 1990 ISBN 0 11 412955 X

12 *Numerical targets and legal limits in Safety Assessment Principles for Nuclear Facilities. An explanatory note.* HSE November 2006. Web version: www.hse.gov.uk/nuclear/saps/

13 *Living with radiation* NRPB 1998

14 *IAEA Safety Glossary. Terminology used in nuclear, radiation, radioactive waste and transport safety* IAEA Safety Glossary V2.0 2006

15 *Evaluation of seismic hazards for nuclear power plants, Safety Guide* IAEA Safety Standards Series No. NS-G-3.3 2002

16 *Council Directive 96/29/EURATOM*

While every effort has been made to ensure the accuracy of the references listed in this publication, their future availability cannot be guaranteed.

FURTHER INFORMATION

HSE priced and free publications are available by mail order from HSE Books, PO Box 1999, Sudbury, Suffolk CO10 2WA Tel: 01787 881165 Fax: 01787 313995 Website: http://www.hsebooks.co.uk (HSE priced publications are also available from bookshops and free leaflets can be downloaded from HSE's website: www.hse.gov.uk).

For information about health and safety ring HSE's Infoline Tel: 0845 345 0055 Fax: 0845 408 9566 Textphone: 0845 408 9577 e-mail: mailto:hse.infoline@natbrit.com or write to HSE Information Services, Caerphilly Business Park, Caerphilly CF83 3GG.

The Stationery Office publications are available from The Stationery Office, PO Box 29, Norwich NR3 1GN Tel: 0870 600 5522 Fax: 0870 600 5533 e-mail: mailto:customer.services@tso.co.uk, Website: www.tso.co.uk. (These are also available from bookshops.)

This document is available web-only at: www.hse.gov.uk/nuclear/saps/.

Published by the Health and Safety Executive, 2006.