Office for Nuclear Regulation

Safety Assessment Principles for Nuclear Facilities

2014 Edition
Revision 0

Version Control

The 2014 revision of the Safety Assessment Principles (SAPs) was completed in November 2014 and is reflected in this document.

Changes may need to be made to this document as time moves on, eg amending minor typing errors, or accommodating any significant changes affecting the Office for Nuclear Regulation (ONR).

For this reason the website version is the only authorised version.

To avoid any confusion and provide some form of version control over the guidance, every page in this paper copy is marked as 'uncontrolled if not viewed on ONR website. This signals that at a future date the information may change, and it is the responsibility of each individual to cross reference any copy with the most up to date version published on the ONR website.

Where amendments are made to the document, these will be published on the ONR website (www.onr.org.uk/saps/index.htm) with an audit trail and, where possible, stakeholders will be alerted to the changes.

The following documents are also available under the nuclear pages of the ONR website:

- A cross-reference table between the 2006 SAPs and the 2014 SAPs.
- ONR's response to comments received.

Revision History

No.	Date	Change summary

Page

Note

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

The Office for Nuclear Regulation (ONR) is the independent regulator of nuclear safety and security across the UK. ONR's inspectors use these Safety Assessment Principles (SAPs), together with supporting Technical Assessment Guides (TAGs), to guide their regulatory judgements and recommendations when undertaking technical assessments of nuclear site licensees' safety submissions. Underpinning these is the legal duty on licensees to reduce risks so far as is reasonably practicable, and this informs the use of these SAPs. In addition, the SAPs are used to guide our assessments of proposed new nuclear facilities designs that may come forward for eventual construction at sites in the UK.

The 2006 version of the SAPs built upon earlier publications (1979, 1983, 1988 and 1992) taking account of developments in nuclear safety and its regulation, both internationally and in the UK.

This 2014 revision of the SAPs was prompted by publication in 2011 of the Chief Nuclear Inspector's report on the implications of the Fukushima accident for the UK nuclear industry. That report concluded that there were no significant gaps in the 2006 safety assessment principles, but recommended a review to ensure that lessons learned were incorporated. That review is now complete and this document contains the results. For purposes of continuity and clarity the revised SAPs retain the 2006 identifiers.

In addition to the lessons from Fukushima, we have also taken account of recent work by the International Atomic Energy Agency (IAEA), in particular the development of IAEA's design standard on the safety of nuclear power plants (SSR 2/1). As with the previous version of the SAPs, we believe that they are fully in line with IAEA guidance and standards. We acknowledge that these SAPs cannot reflect the breadth and depth of the entire suite of IAEA publications and so we explicitly identify those documents as relevant good practices within our TAGs.

IAEA guidance recommends that regulatory bodies subject their principles, regulations and guidance to periodic review, and take account of internationally endorsed standards and guidance. Although the SAPs have been reviewed and revised a number of times over the years, we acknowledge the importance of regular reviews and will formalise arrangements to carry out future reviews of the SAPs at least every five years.

ONR is an active 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 levels of nuclear safety. To this end, WENRA has developed reference levels that represent good practices for existing civil nuclear power plants, radioactive waste management and decommissioning. ONR has previously acknowledged the reference levels as relevant good practice. It has now reviewed the most recent version of the reference levels, themselves recently revised to take account of learning from Fukushima, to ensure compatibility with the SAPs. These reference levels are also explicitly referenced in the ONR TAGs that support these SAPs.

The Defence Nuclear Safety Regulator (DNSR) the Environment Agency (EA) and the Scottish Environment Protection Agency (SEPA) have supported ONR in this revision of the SAPs and their contribution is gratefully acknowledged.

This revision of the SAPs has been informed by comments and views submitted to us in response to an open invitation on ONR's website. In many cases these have led us to modify the text. However, decisions on the final text and responsibility for the SAPs content are ours alone.

Dr A N Hall
Chief Nuclear Inspector
Office for Nuclear Regulation

November 2014

INTRODUCTION

The purpose of the Safety Assessment Principles (SAPs)

1. The SAPs apply to assessments of safety at existing or proposed nuclear facilities. This is usually through our assessment of safety cases in support of regulatory decisions. The term ‘safety case’ is used throughout this document to encompass the totality of the documentation developed by a designer, licensee or duty-holder to demonstrate high standards of nuclear safety and radioactive waste management, and any subset of this documentation that is submitted to the Office for Nuclear Regulation (ONR).

2. The principles presented in this document relate only to nuclear safety, radiation protection and radioactive waste management. Conventional hazards associated with a nuclear facility 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 primary purpose of the SAPs is to provide inspectors with a framework for making consistent regulatory judgements on the safety of activities. The principles are supported by Technical Assessment Guides (TAGs), and other guidance, to further assist decision making within the nuclear safety regulatory process (see the ONR website). Although it is not their prime purpose, the SAPs may also provide guidance to designers and duty-holders on the appropriate content of safety cases, clarifying our expectations in this regard. However, they are not sufficient on their own to be used as design or operational standards. Although in most cases the SAPs provide guidance, in those places where they refer to legal requirements they may 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 Energy Act 2013. 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 ONR has granted a licence. Additionally, section 4 of NIA enables ONR to attach conditions to a licence in the interests of safety or with respect to the handling, treatment and disposal of nuclear matter.

5. ONR regulates the safety of nuclear installations (including conventional safety) and the transport of radioactive materials in Great Britain. It also regulates nuclear security and safeguards in the United Kingdom. Our role in regulating nuclear safety 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 on nuclear licensed sites currently include: nuclear power stations (operational, decommissioning and under construction); research reactors being decommissioned; nuclear fuel manufacturing; uranium enrichment and isotope production facilities; nuclear fuel stores; nuclear fuel reprocessing facilities; sites for

building, maintaining and refuelling nuclear submarines[1]; sites for building, maintaining and dismantling nuclear weapons; radioactive waste stores; and sites for both the storage and disposal of radioactive waste.

7. NIA is not the only health and safety law that applies on nuclear licensed sites. Nuclear operators must also comply with the relevant statutory provisions of the Health and Safety at Work etc Act 1974 (HSW Act). In particular, radiation protection is regulated under the Ionising Radiations Regulations 1999 (IRR99) and emergency preparedness and associated radiation protection are regulated against the Radiation (Emergency Preparedness and Public Information) Regulations 2001 (REPPIR). Other relevant legislation includes the Management of Health and Safety at Work Regulations 1999 (the Management Regulations), which require, among other things, a suitable and sufficient risk assessment; the Provision and Use of Work Equipment Regulations 1998; the Lifting Operations and Lifting Equipment Regulations 1998; the Personal Protective Equipment at Work Regulations 1992; the Pressure Systems Safety Regulations 2000; the Control of Major Accident Hazards Regulations 1999; and the Dangerous Substances and Explosive Atmospheres Regulations 2002 (which require a risk assessment for any substance identified in the Chemicals (Hazard Information and Packaging for Supply) Regulations 2009). This list is not exhaustive. Nuclear operators must comply with these regulations in the same way as any other employer, and 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. Nuclear operators must also comply with other legislation which is not made under the HSW Act. Examples include: the Nuclear Reactors (Environmental Impact Assessment for Decommissioning) Regulations 1999 (EIADR), made under the European Communities Act 1972; the Energy Act 2013 and its relevant statutory provisions such as the Nuclear Industries Security Regulations 2013; the Electricity Act 1989; the Environmental Protection Act 1990; the Radioactive Substances Act 1993; Environmental Permitting Regulations 2010; various planning acts; and the Building Act 2000, relevant amendments and its subordinate Building Regulations. Again this list is not exhaustive.

SFAIRP, ALARP and ALARA

9. The SAPs are consistent with ‘Reducing Risks, Protecting People: HSE’s Decision-Making Process’ (R2P2, Ref. 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, Ref. 2). In R2P2, ‘hazard’ is defined as the potential for an intrinsic property or disposition of something to cause a detriment, and ‘risk’ is the chance that someone or something is adversely affected by the hazard. In these SAPs, anything that is capable of causing harm is termed a ‘hazard’. The relative importance of hazard and risk in determining the acceptability of control measures will vary according to the circumstances. In some cases, particularly where the hazard is particularly high, or knowledge of the risk is very uncertain, ONR may choose to concentrate primarily on the hazard.

10. R2P2 describes risks that are unacceptably high, where 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 with no further regulatory pressure

[1] While ONR regulates the activities on these sites under NIA, we do not regulate the designs of submarine reactors nor nuclear weapons

to reduce risks further being 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. The overall risk levels set out in R2P2 and TOR have been translated into specific numerical targets within the SAPs. The derivation and basis for the SAPs numerical targets are described in Annex 2.

11. Though R2P2, TOR and the SAPs set out indicative numerical risk levels, meeting relevant good practice in engineering and operational safety management is of prime importance. In general, ONR has found that meeting relevant good practice in engineering, operation and safety management leads to risks that are reduced SFAIRP and numerical risk levels that are at least tolerable, and in many cases broadly acceptable.

12. HSE and ONR guidance generally uses the term ‘as low as reasonably practicable’ (ALARP) as a convenient means to express the legal duty to reduce risks SFAIRP. 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 in relation to ionising radiation exposure by other bodies nationally and internationally.

13. The SAPs assist inspectors in judging whether, in their opinion, the designers or dutyholder’s safety case has satisfactorily demonstrated that the requirements of the law can be or have been met. The guidance associated with each principle gives further interpretation on their application.

14. The starting point for demonstrating that risks are ALARP and safety is adequate is that the normal requirements of good practice in engineering, operation and safety management are met. This is a fundamental expectation for safety cases. The demonstration should also set out how risk assessments have been used to identify any weaknesses in the proposed facility design and operation, identify where improvements were considered and show that safety is not unduly reliant on a small set of particular safety features.

15. The development of standards defining relevant good practice often includes ALARP considerations, so in many cases meeting these standards will be sufficient to demonstrate that legal requirements have 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 that the costs of any further measures would be grossly disproportionate to the reduction in risks achieved by their adoption.

16. The principles are used in helping to judge whether reducing risks to 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 met so far as is reasonably practicable. This has not been stated in each case to avoid excessive repetition. ONR’s inspectors need to apply judgement on the adequacy of safety in accordance with HSE guidance on ALARP (see HSE website) and ONR’s more detailed guidance written specifically for the nuclear context (Ref. 3).

17. In many instances it will be possible for dutyholders to demonstrate that the magnitude of the radiological hazard will result in doses that will be so low (eg in relation to legal limits) that detailed consideration of off-site effects and/or worker risks is unnecessary.

18. The application of the ALARP process should be carried out comprehensively and consider all applicable principles, with all relevant risks 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 and justify that an appropriate balance has been achieved.

Permissioning

19. Regulatory regimes requiring safety submissions and/or a licence are referred to as 'permissioning regimes'. ONR's approach to such regimes is set out in HSE's Permissioning Policy Statement, published in 2003 (Ref. 4). Most safety submissions to ONR arise from NIA licence condition requirements, but are also required for GDA as well as for other regulations such as IRR99 or REPPIR.

Interface with other regulatory bodies

20. Depending on the nature of the safety case being assessed, there may be other regulators whose requirements and processes ONR needs to take into account when coming to a regulatory decision. These interactions are covered by relevant joint statements. The regulatory bodies whose processes ONR most frequently interfaces with are:

    (a) The Environment Agency (EA), Scottish Environment Protection Agency (SEPA) and Natural Resources Wales (NRW); and

    (b) The Defence Nuclear Safety Regulator (DNSR).

21. Annex 1 gives further details on the regulatory interfaces between ONR and other regulatory bodies.

International framework

22. The UK is a member state of the International Atomic Energy Agency (IAEA) and contributes actively to the development of Safety Standards that the IAEA publishes. The UK applies these Safety Standards and ensures that its own regulations, regulatory requirements and guidance are consistent with them. This includes the SAPs, which were benchmarked for the 2006 issue against IAEA's Safety Standards and have been updated to reflect subsequent changes in these standards since 2006 for this issue.

23. In addition to working with IAEA on Safety Standards, ONR assists the UK Government on 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 ONR is active in the promotion of improvements to nuclear safety include participation in the Western European Nuclear Regulators Association (WENRA), the European Nuclear Safety Regulators Group (ENSREG), the International Nuclear Regulators Association and the Organisation for Economic Cooperation and Development's Nuclear Energy Agency (NEA). ONR's guidance to inspectors seeks to take account of developing advice and guidance arising from the work of all these and other relevant organisations. In particular, the WENRA safety reference levels are explicitly incorporated as relevant good practice within ONR's technical assessment guides.

Application of the SAPs

General

24. 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.

25. 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 should choose those relevant to the particular situation.

26. The SAPs are used to assess the safety of defence-related nuclear and radiological activities that fall within ONR's responsibilities. Nuclear and radiological safety legislation does not apply to defence-related nuclear activities, or where exemptions are in place. Reflecting this, an annex to the MOD/HSE agreement[2] recognises that these SAPs may not apply to the design of a naval reactor plant or a nuclear weapon[3]. The extent of application of these principles to the safety of defence-related activities will nevertheless be judged on a basis consistent with SFAIRP. Moreover, ONR will take due account of the unique operating purpose of defence-related activities and that ONR's regulatory remit only applies to discrete periods of their operating lifecycles.

Proportionality

27. The Management Regulations define three levels of risk assessment: low, intermediate and high. Nuclear installations are in the high category, and so 'the most developed and sophisticated techniques' should be used. However, there is 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 still vary considerably. This is consistent with ONR's Enforcement Policy Statement (Ref. 5) 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 hazard. Similarly, subject to other legal duties or public policy requirements, ONR regulatory attention should likewise be commensurate with the magnitude of the hazard, although issues such as novelty and uncertainty will also be factors.

28. Safety cases, and the analyses and assessments contained within them, must be fit for purpose, in accordance with nuclear site licence condition requirements and with Regulation 3 of the Management Regulations, and IRR 1999 Regulation 7. They must, among other things, be suitable and sufficient for the purpose of identifying all measures to control the risk.

[2] The referenced annex to the MOD/HSE General Agreement remains in place for the purposes of MoD/ONR working relationships until superseded by any separate agreement made between the ministry of Defence and the Office for Nuclear Regulation, expected to take place in the near future

[3] 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 weapon

29. Inspectors must be proportionate in what they require from designers and dutyholders. The higher the hazard, the more rigorous and comprehensive the analysis which would be expected, leading to greater defence in depth to protect people. In contrast, a low hazard facility will likely require a more limited analysis and be provided with fewer or less extensive safety provisions.

30. In some cases, the magnitude of the radiological hazard may be uncertain. In these cases a precautionary approach should be applied (R2P2) by erring on the side of safety. Where the absence of a radiological hazard cannot be shown, an appropriate radiological hazard and magnitude should be assumed and the justification given.

Lifecycle

31. The SAPs are designed to support regulatory assessments throughout the lifecycle of nuclear facilities. Specific sections are, however, devoted to individual stages, eg siting and decommissioning. In general, not every principle in every section will apply to every lifecycle stage. Instead the principles are a reference set from which the inspector should select those relevant to the particular stage in the lifecycle. For instance, the sections on Leadership and Management for Safety (paragraph 53 ff.) and the Regulatory Assessment of Safety Cases (paragraph 79 ff.) include aspects covering the entire lifecycle of the facility. The Engineering Principles (paragraph 140 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 should also be considered at all lifecycle stages.

New facilities

32. One of the aims of the SAPs is to support the regulatory safety assessment of new (proposed) nuclear facilities. They represent ONR's view of good practice and we would expect modern facilities to satisfy their overall intent.

Facilities built to earlier standards

33. Inspectors should assess safety cases against the relevant SAPs when judging if a dutyholder has demonstrated that legal requirements have been met and risks have been controlled to ALARP. The extent to which the principles ought to be satisfied must also take into account the age of the facility or plant. For facilities designed and constructed to earlier standards, the issue of whether suitable and sufficient measures are available to satisfy ALARP will need to be judged case by case.

Transient Risks

34. For certain activities, such as decommissioning, it is recognised that some principles may not be met transiently; 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

35. As a facility ages, safety margins may be eroded and a dutyholder may argue that making improvements is not worthwhile. The short remaining lifetime of the facility may be invoked as part of the ALARP demonstration. However, this factor should not be accepted to justify the facility operating outside legal requirements, or at levels of risk that are unacceptably high (see SAPs Numerical Targets). A safety case which

argues for not making an improvement based predominantly on limited future lifetime should only be accepted where the maximum extent of the future operational life is irrevocably fixed and provides a suitable margin of safety. In cases where the planned lifetime is not irrevocably fixed, a minimum period of ten years (or the unavoidable necessary life of the facility, if longer) should be considered for the purposes of judging whether the ALARP demonstration is acceptable.

Continuous improvement and Periodic Safety Reviews

36. The principle of continuous improvement is central to achieving sustained high standards of nuclear safety. The legal requirements for risk reduction SFAIRP, and for Periodic Safety Reviews (PSRs) (as required by Licence Condition 15), underpins this principle. Application of this principle ensures that, no matter how high the standards of nuclear design and subsequent operations are, improvements should always be sought. Seeking and applying lessons learned from events, new knowledge and experience, both nationally and internationally, must be a fundamental feature of the safety culture of the nuclear industry.

37. The SAPs are intended to be applied in the assessment of PSRs. A PSR includes a comprehensive assessment of the facility's condition, operating experience, safety case, and management arrangements and culture, looking forward at least the next ten years and normally to the end of life. The review is carried out at appropriate intervals through the different lifecycle phases of the facility usually every ten years starting at the commencement of active commissioning.

38. PSRs are more wide ranging than a restatement of the safety case and instead provide a systematic review of whether the safety case remains adequate for all operations that may affect safety. This entails reviews that consider all levels of Defence in depth (see Principle EKP.3) from the robustness of the facility's design through to the resilience of its emergency preparedness arrangements.

Safety and security assessments

39. Safety and security legislation imposes separate, specific duties on licensees / dutyholders. Sometimes these duties overlap, as in REPPIR where Hazard Identification and Risk Evaluation (HIRE) assessments need to consider both safety-derived initiators and potential unauthorised behaviour of employees or the public. On other occasions they are inter-related. For instance, while malicious acts such as theft or sabotage would not normally be considered when determining the reasonably practicable preventative or protective measures needed in the interests of safety, what might be done to mitigate (etc) the consequences from such acts should nevertheless be considered within safety assessments.

40. In general, the aims of safety and security legislation should be complementary, in that both are intended to lead to measures that reduce the risk of harm to the public and workers arising from nuclear facilities, and so measures that adequately address the requirements of one set of legislation will often satisfy the requirements of the other. On other occasions a common solution will not be possible, and designers or dutyholders will need to determine a solution that separately addresses the requirements of safety and security legislation. In practical terms this may mean (for instance to reduce the total amount of documentation required) that designers or dutyholders may choose to combine safety- and security-derived assessments into single documents, or choose to keep those parts of the safety case which are also needed to meet security duties separate from the rest of the safety case. Such approaches are perfectly acceptable provided the totality of these documents addresses all of ONR's expectations and requirements in the two areas. In particular,

the combining of assessments in this way should not be taken to imply that security assessments lie within the remit of safety legislation, or vice versa.

41. Given this complementary relationship between safety and security, these SAPs include guidance on how to assess security-related matters where these fall within the vires of safety legislation, ie because of overlap or inter-relation. This guidance is provided in the specific sections of the principles where this applies. Detailed information on security aspects can be found in the National Objectives, Requirements and Model Standards document, which supports implementation of the Nuclear Industries Security Regulations 2003.

Multi-facility sites

42. When assessing the 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 applied in relation to single facilities and so the control of risks is also generally considered on a facility basis. However, there is sometimes also a need to consider the totality of risks from a site and how these are controlled, for example when a single initiating event can affect multiple facilities. The licensee has a duty to manage all the risks within its control so that total risks are ALARP, including risks from multi-facility events. In some locations there are multiple sites, governed by different licensees, ie there are neighbouring sites. In this circumstance, ONR expects licensees and others in control of major nuclear hazards to co-operate with one another so that the overall risks in the location, taking into account all neighbouring sites, are kept ALARP

43. Individual sites with multiple facilities often produce individual safety cases for each facility. Shared services are also generally dealt with by separate cases. The division of a site's safety case 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 assessments to provide an overall site safety case which accounts for the interactions and interdependencies between facilities and services.

Alternative approaches

44. The SAPs express ONR's expectations for the content of safety cases submitted to us However, designers and/or dutyholders may wish to put forward safety cases that differ from these expectations. As in the past, ONR inspectors should consider such submissions on their individual merits. However, where the approach being followed differs substantially from the expectations set out here, inspectors should advise designers and/or dutyholders to discuss the method of demonstration with ONR beforehand. ONR will need to be assured that such cases 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 that assurance.

Structure of the principles

45. 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 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 effective delivery of nuclear safety.

- The regulatory assessment of safety cases. This section sets out principles applicable to assessments of the content of safety cases and the processes governing their production.
- Siting aspects. This section sets out principles relating to ONR's role in siting decisions and to how the physical location of a facility can affect safety.
- 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 links to BSS and IRR99 and sets out principles for assessing whether exposures to ionising radiation are as low as reasonably practicable.
- Fault analysis. This section describes the principles to be applied when assessing the adequacy of measures to prevent, protect against and/or mitigate the consequences of faults and accidents.
- Numerical targets and legal limits. This section is based predominantly on Tolerability of Risk (TOR) and sets out targets to assist in making regulatory judgements, on the acceptability of the estimated numerical risks.
- Accident management and emergency preparedness. This section provides principles for assessing arrangements for the control and mitigation of radiological consequences following a significant release of radioactivity.
- Radioactive waste management.
- Decommissioning.
- Control and remediation of radioactively contaminated land.

46. The glossary at the end of the principles is provided to assist in understanding some of the terms used. Where relevant, the glossary includes the sources of the definitions adopted.

FUNDAMENTAL PRINCIPLES

47. *The following fundamental principles are considered to be the foundation for the subsequent safety and radioactive waste management principles in this document. They reflect UK law and accepted international good practice and in recognition of their legal standing, use the 'must' form rather than 'should'.*

48. *The IAEA safety standards also include fundamental principles, but these cover a wider scope than safety assessment. ONR's principles have therefore been drawn from the aspects of IAEA's principles that are relevant to the remit of the SAPs[4].*

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.		

49. The licensee retains the prime responsibility for safety throughout the lifetime of facilities and activities, and this responsibility cannot be delegated. Other groups, such as designers, manufacturers and constructors, employers, contractors, and consignors and carriers, also have legal, professional or functional responsibilities with regard to safety.

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.		

50. The next section of the SAPs deals explicitly with ONR's expectations for leadership and management of safety.

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

Fundamental principles	Safety assessment	FP.4
Dutyholders must demonstrate effective understanding and control of the hazards posed by a site or facility through a comprehensive and systematic process of safety assessment.		

51. The regulatory assessment of safety cases (paragraphs 79 ff) is covered in detail in the SAPs including expectations for the nature and content of safety cases.

[4] The IAEA fundamental principles were adopted by the IAEA Board in 2006. Of the ten principles, three are not covered, relating to the role of Government, the justification of facilities and activities, and to radiation risks in situations outside the NIA (these are addressed through the UK's wider regulatory framework). Furthermore, FP.8 is narrower than the analogous IAEA principle as environmental aspects are beyond the scope of this document and are addressed through the UK's wider regulatory framework. However, the SAPs include a further fundamental principle on safety assessment, rather than considering this as a subset of preventing accidents.

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.		

52. ONR's expectations for accident management and emergency preparedness are set out in paragraphs 768 ff.

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

LEADERSHIP AND MANAGEMENT FOR SAFETY

53. *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 these principles proportionately, reflecting the radiological hazards and the scale and complexity of the dutyholder's undertaking.*

54. *The section contains four high-level inter-related principles: leadership, capable organisation, decision making and learning. These set the outcomes to be achieved for effective leadership and management for safety, and identify the characteristics of a positive safety culture, rather than describing the systems, processes and procedures for achieving safety. Because of their inter-connected nature there is some overlap between the principles. They should therefore be considered as a whole and an integrated approach will be necessary for their delivery.*

55. *The principles have wide application to all aspects of licensees' leadership and management for safety. This includes, but is not limited to, application to those licence conditions that require licensees to make and implement 'adequate arrangements'. Arrangements for complying with licence conditions and other legal duties will normally need to include policies, systems and procedures together with identification of the associated roles, responsibilities, competence levels and monitoring arrangements. The principles are also intended to be used for other aspects of the nuclear permissioning regime, eg the assessment of a safety management prospectus, as required of a new licence applicant (see Licensing nuclear installations, Ref. 6).*

56. *The principles combine the key features of effective safety management arising from current national law and guidance; in particular the nuclear site licence conditions, the HSW Act, the Management Regulations and Successful health and safety management HSG65 (Ref.7). They also draw on international guidance including IAEA safety standards, relevant good practice in safety management, the lessons learned from serious incident investigations in a range of sectors, for example the official investigation reports on the Columbia (Ref. 8) and Fukushima (Ref. 9) accidents, and the work of researchers who have examined the operation of resilient and high reliability organisations.*

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

    (a) the emphasis ONR gives to leadership and management for safety, the role of directors and worker involvement;

    (b) the pivotal role played by good and effective leadership, people management and processes; and

    (c) *the need to consider the management of safety at all levels 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.		

58. 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 strategies, policies, plans, goals and standards for safety and ensuring that they are delivered throughout the organisation;

    (b) providing direction, governance and oversight to establish and foster a positive safety culture that underpins safe operation;

    (c) demonstrating a visible commitment to safety through their activities;

    (d) recognising and resolving conflict between safety and other goals (eg production and commercial pressures);

    (e) ensuring that management of safety is participative, actively drawing on the knowledge and experience of all staff;

    (f) ensuring that any reward systems promote the identification and management of risk, encourage safe behaviour and discourage unsafe behaviours or complacency;

    (g) understanding that apparent past success is no guarantee of future success and that fresh perspectives on ways to enhance safety should be sought and acted upon; and

    (h) monitoring and regularly reviewing safety performance and culture.

59. 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 responsibility and accountability to each other and external stakeholders to ensure high standards of safety. The licensee should ensure that this extends to contractors down the supply chain as required.

60. Oversight of safety performance, led by the board of the organisation, 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 utilise diverse sources of information, including feedback from independent challenge and reviews, in order to provide confidence (by means of governance, monitoring and auditing processes) that safety and quality policies, strategies, plans, goals, standards, systems and procedures are being implemented through the application of an effective management system.

61. The management system should give due regard to safety, and safety should be considered explicitly when developing and implementing any new arrangements for managing the organisation. An integrated management system should be adopted so that the potential for conflicts between the organisation’s goals and responsibilities is minimised. The management system should:

    (a) be based on national or international standards or equivalent;

(b) be aligned with the goals of the organisation and contribute to their achievement;

(c) be subject to regular review, seeking continual improvement; and

(d) support a positive safety culture.

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

62. The organisation should have adequate human resources. This includes having the necessary competences and knowledge in sufficient numbers to provide resilience and maintain the capability to govern, lead and manage for safety at all times.

63. The organisation's structure and baseline staffing levels should be based on appropriate organisational design principles. Human resources baseline provisions should be established, controlled and reviewed regularly through robust, auditable processes. Changes to the organisation (including to structure, staffing, resources or competences) should be subject to systematic evaluation to ensure that they do not adversely affect the capability of the organisation to deliver safety. There should be succession planning arrangements (especially where there is limited or singleton expertise). Succession planning should take into account expected changes (eg retirements) and make contingencies for the unexpected (eg resignations).

64. 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. The organisation should ensure that proportionate governance 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.

65. Processes and systems should secure and assure maintenance of appropriate technical and behavioural competence of directors (both executive and non-executive), managers, leaders and all other staff and contractors with safety roles and responsibilities.

66. Being a capable organisation requires the retention and use of knowledge so that safety requirements are understood and risks are controlled throughout all activities, including those undertaken by contractors at all levels within the supply chain. An 'intelligent customer' capability should therefore be maintained to ensure that the use of contractors in any part of the organisation does not adversely affect its ability to manage safety.

67. The organisation should sustain a design authority capability that includes suitable and sufficient experts with a detailed and up-to-date understanding of the safety of its facilities and their design, operation and safety cases. 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 and so retain knowledge from experienced staff leaving the organisation.

68. Knowledge should be captured and communicated within the organisation in a systematic, appropriate and reliable manner to all those who need to make safety decisions. There should be provision for identifying, updating and preserving documents and records relevant to safety. Such documents and records should be stored securely and should be retrievable and readable throughout their anticipated useful life (including statutory retention periods). Documents and records relevant to safety should include those:

(a) of value throughout the whole life of a facility;

(b) that would assist in the event of an incident;

(c) relevant to making future modifications or to decommissioning (see paragraph 816); or

(d) that could contribute to improvements in safety.

Leadership and management for safety	Decision making	MS.3
Decisions made at all levels in the organisation affecting safety should be informed, rational, objective, transparent and prudent.		

69. Safety should be given a high priority and this should be evident in all decision making processes. The processes should ensure that all relevant 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. Safety decisions should not be delayed unnecessarily (eg for commercial reasons) and personnel should be duly empowered to take timely decisions in the interests of safety.

70. Decisions affecting safety should consider the following factors (where relevant):

(a) the quality and sufficiency of the information;

(b) the significance of uncertainties;

(c) the questioning of assumptions;

(d) exploration of all relevant scenarios that may threaten safety;

(e) the range of options to minimise risk in the short and long term;

(f) the criteria and standards that should be applied.

71. Decision making should be based on processes that ensure that conflicts between safety and other business goals are recognised and appropriately resolved.

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

73. Active challenge should be part of decision making throughout the organisation including at board and senior management levels. The organisation should encourage a questioning attitude from all staff and contractors. Though the form and function of the challenge will vary between different areas, designing-in appropriate active challenge mechanisms should be an inherent part of all decision making processes affecting safety. Active challenge should:

    (a) occur routinely as a result of a questioning attitude in the culture of staff and contractors;

    (b) occur by design, and transparently, in all key decision making processes that may affect safety;

    (c) not originate solely from independent safety assessment or peer review;

    (d) assume that failure through inadequate design or implementation is possible, and be proactive in looking for ways that things could go wrong;

    (e) be applied to technical/facility-based and management decisions; and

    (f) be used in operational decision making in normal, fault and accident situations.

74. Indicators should be used to monitor nuclear safety performance, correct adverse trends before safety is impacted and inform decision making. Analysis and interpretation of data are important in developing meaningful indicators. The set of indicators should draw from an appropriately wide and diverse range of sources, chosen so that the indicators provide meaningful information. Both leading and lagging indicators should be included. Reliance solely on quantitative indicators should be avoided since the picture they create can be over-simplistic, and appropriate qualitative information should also be sought.

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

75. Organisations 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 does not necessarily indicate that risks are being adequately controlled and should not breed complacency. Near misses should be seen as opportunities to learn and a culture of open reporting should be fostered.

76. Learning should drive improvement throughout the organisation. Information should be collected from a range of sources inside the organisation, including from:

    (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 governance, 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 operational and fault conditions;

(e) inspections of sites, facilities, plant and equipment and other operational feedback systems;

(f) investigations of incidents and accidents, specifically to ascertain immediate and underlying causes, including organisational, safety management and cultural factors;

(g) self assessments; and

(h) external assessments commissioned by the organisation.

77. Information should be sought actively and systematically from external sources, including from beyond the nuclear industry, to identify learning and improvement opportunities. 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;

(c) benchmarking safety performance, safety management and learning methods and processes against those of other organisations from both within and outside the nuclear industry;

(d) safety data, eg reliability data and general operating experience feedback; and

(e) feedback on safety performance and issues from regulators.

78. Information from both internal and external sources should be analysed to identify trends and issues, eg common cause failures (CCFs) or the influence of human or organisational factors, such as leadership and culture. The lessons learned should be embedded through a structured system for implementing corrective actions in a timely manner, which is rigorously applied and actively followed up to confirm completion. Effectiveness reviews should be undertaken to confirm that the changes have delivered the desired improvements. The learning processes and systems for implementation should themselves be subject to review and improvement.

THE REGULATORY ASSESSMENT OF SAFETY CASES

79. *The principles in this section set the foundation for effective safety cases. If the principles are adopted by dutyholders it will help them achieve 'right first time safety cases' which will more easily be accepted by ONR assessment. During assessment, inspectors should use the principles proportionately commensurate with the radiological hazards presented. There are eight safety case inter-related principles that address the production process: outputs; lifecycle aspects; characteristics; optimism, uncertainty and conservatism; content and implementation; maintenance; and ownership.*

80. *ONR's assessment process consists of examining safety submissions to enable a judgement to be made that risks from an existing or proposed facility are ALARP and that appropriate attention has been paid to aspects important to safety and to radioactive waste management and decommissioning. ONR's assessment covers an examination of the claims, arguments and evidence for both normal operation and fault conditions, including internal and external hazards and human errors, all of which have the potential to cause the exposure of workers or the public to significant unplanned doses of ionising radiation or releases of radioactivity. A submission assessed by ONR 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.*

81. *ONR's assessment involves the examination of documentation and arrangements that set out the claims, arguments and evidence that demonstrate the safety of a facility and its processes, operations and organisation. In addition, it can also involve inspection of the facility to verify the accuracy of the safety case as a description of the facility, its assumptions, safety provisions and requirements. ONR also undertakes compliance inspections to determine whether the procedures needed to implement these provisions and requirements have been followed. These examinations and inspections are important in establishing confidence in the reliability of the information and conclusions presented in the safety case.*

82. *ONR uses a sampling approach in deploying its resources and not every safety case is assessed fully in every respect. The extent of our sample and any subsequent permissioning decision taken in light of the safety case will take into account:*

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

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

    (c) the risks and hazards associated with the activities covered by the safety case; and

    (d) recent events or operating experience at the facility, or similar facilities.

83. *Other important factors in ONR's permissioning decisions include:*

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

    (b) the extent to which the dutyholder has demonstrated that the safety objectives and regulatory requirements have been met, including the

application of relevant good practice in engineering, operation and safety management;

(c) 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;

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

(e) the confidence ONR has in the conclusions reached by the dutyholder.

84. *ONR will use the findings from its assessment of the safety case to inform its inspection priorities.*

85. *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 ONR'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.*

86. *A safety case is a logical and hierarchical set of documents that describes risk in terms of the hazards presented by the facility, site and the modes of operation, including potential faults and accidents, and those reasonably practicable measures that need to be implemented to prevent or minimise harm. 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 the hazards are to be controlled successfully. The safety case clearly sets out the trail from safety claims through arguments to evidence.*

87. *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 of 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.*

88. *The production of a safety case does not in itself ensure the safety of a facility. Instead, starting with a proper understanding of the safety case, the technical requirements deriving from it (ie its limits and conditions – operating rules) must be properly implemented so that the facility can be operated and maintained in a safe manner.*

Safety case processes

89. *The process of analysing safety requires creativity, where people can envisage the variety of routes by which radiological risks can arise from the technology. A range of risk prevention or reduction options can then be identified, from which the reasonably practicable ones can be selected and implemented. Safety analysis requires an*

extensive understanding of the facility, both in the present and foreseeable future, its behaviour in a variety of conditions and experience of failures (including at other facilities, see paragraph 110) together with the measures adopted to prevent their recurrence. It also requires an understanding of how people and organisations may affect safety. Imagination is required to identify potential failure modes arising in plant, people or processes 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 safety case and implementing its requirements. The inspector should look for evidence of all these attributes.

90. *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 production 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.		

91. Application of this principle should result in:

(a) a clear specification for the purpose, standards and expectations of each element of the 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 the training and qualifications needed for the formal roles within the process (to ensure that those who undertake the roles are suitably qualified and experienced).

92. 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 reliable or highly unlikely to fail, the process used to derive such claims needs to have commensurate reliability.

93. The different elements of the 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 seek to identify defects in the safety case process, not just address issues relating to the content of the safety case itself.

94. 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, including those from outside the nuclear industry. 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.

95. During times of high stress (eg tight deadlines, intense commercial or operational pressure), additional measures should 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 just be restricted to normal situations.

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

96. 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 (see paragraph 87). This includes designers, operations and maintenance staff, technical personnel and managers who are accountable for safety.

97. 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	Lifecycle aspects	SC.3
For each lifecycle stage, control of the hazard should be demonstrated by a valid safety case that takes into account the implications from previous stages and for future stages.		

98. Control of hazards should be demonstrated in a safety case before any associated risks materially exist. The safety case for each stage should take account of future lifecycle stages, ie it should build on the safety case for previous stages and show that the safety intent for subsequent stages will be achieved. Any constraints that 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 lifecycle stages. In the case of early, unplanned permanent shutdown of a

facility, the safety case should be revised to address any safety implications arising from the early shutdown and to identify any changes to the strategy and timescales for decommissioning.

99. 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 the particular stage and inter-relationships with other stages. For example, in the early stages (eg design concept), the safety case will be more a statement of future intent, claims and principles, whereas a safety case for an operational stage needs to contain far more detail, evidence 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.		

100. A safety case should:

(a) explicitly set out the argument for why risks are ALARP; and

(b) link the information necessary to show that risks are ALARP, and what will be needed to ensure that this can be maintained over the period for which the safety case is valid;

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

(d) accurately and realistically reflect the proposed activity, facility and its structures, systems and components;

(e) identify all the limits and conditions necessary in the interests of safety (operating rules); and

(f) identify any other requirements necessary to meet or maintain the safety case such as surveillance, maintenance and inspection.

101. To achieve these, a safety case should:

(a) identify the facility's hazards by a thorough and systematic process;

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

(c) demonstrate that the facility conforms to relevant good engineering practice and sound safety principles. (For example, 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.) Instances where good practice has not been met should be identified and a demonstration provided to justify why these are considered to grossly disproportionate;

(d) provide sufficient information to demonstrate that engineering rules have been applied in an appropriate manner. (For example, it should be clearly demonstrated that all structures, systems and components have been

designed, constructed, commissioned, operated and maintained in such a way as to enable them to fulfil their safety functions for their projected lifetimes.);

(e) analyse normal operations and 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) analyse identified faults and severe accidents, using complementary fault analysis methods to demonstrate that risks are ALARP;

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

(h) provide the basis for the safe management of people, plant and processes. (For example, the safety case should address management and staffing levels, training requirements, maintenance requirements, operating and maintenance instructions, and contingency and emergency instructions).

Further guidance on these topics is set out in the relevant section(s) of these principles.

102. To demonstrate that risks have been reduced to ALARP, the safety case should:

(a) identify and document all the options considered for risk prevention or reduction;

(b) provide evidence justifying the criteria used in decision making or option selection;

(c) justify the options chosen in terms of meeting relevant good practice, and discard any options as being either less effective than the chosen option(s) or grossly disproportionate.

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

103. The safety case should present a balanced view of the level of knowledge and understanding, and of the resultant risks. It should provide a proportionate justification that includes appropriate conservatism but without undue pessimism. 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 the operating regime or procedures). This principle encompasses optimism and uncertainties in the design of a facility (eg material properties, defects and 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 should be offset by appropriate levels of conservatism.

104. 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 content and implementation	SC.6
The safety case for a facility or site should identify the important aspects of operation and management required for maintaining safety and how these will be implemented.		

105. Aspects of operation and management likely to be important for maintaining safety are highlighted in individual sections of these principles. These have not been written to be exhaustive (see paragraph 3).

106. The safety case should justify how the requirements identified within it will be implemented effectively. The means of implementation considered should include:

(a) the operating limits and conditions (operating rules) required to ensure that the facility is operated safely at all times;

(b) the procedures and instructions that need to be followed;

(c) the required examination, inspection, maintenance and testing regimes justified in or assumed by the safety case;

(d) control, supervision, qualification and training and other safety management requirements; and

(e) inputs to emergency planning.

The regulatory assessment of safety cases	Safety case maintenance	SC.7
A safety case should be actively maintained throughout each of the lifecycle stages, and reviewed regularly.		

107. A safety case should be:

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

(b) managed through formal processes; and

(c) reviewed periodically on a defined basis.

108. The safety case needs to be kept up to date so that it continuously meets the needs of all its users (see paragraph 87). In particular, the knowledge used at the time of writing the safety case needs to be supplemented by subsequent monitoring of the facility and data, eg from commissioning, operation, periodic inspection and testing, research or experience from other facilities. The safety case will also need to be

updated to take account of changes at the facility, the site and its surroundings, for instance:

(a) changes arising from modifications or revised operating methods or processes;

(b) changes arising from incidents, operating experience, examination or testing results,

(c) changes from updated design or analysis methods, research findings or other new information;

(d) the outcome from periodic and interim safety reviews (see paragraph 109);

(e) changes due to plant or facility ageing (see paragraph 212 ff.); and

(f) changes in the immediate vicinity of the facility (eg from external hazards or siting aspects, see paragraph 228 ff. and paragraph 127 ff.).

109. Both periodic safety reviews (PSRs) and interim safety reviews are required for compliance with Licence Condition 15. Interim safety reviews ensure that the cumulative impact of recent modifications and changes have been considered so that the safety case remains valid and up to date. These would normally be expected every few years, depending on the nature of the facility. PSRs are a deeper and more searching review which includes comparison with current modern standards. As such they are carried out on a longer timescale as specified in licensee arrangements (for which the normal expectation is no more than every ten years, in line with wider international good practice). The PSR as a review requires a comprehensive assessment of the facility's condition, operating experience, safety case and management arrangements. The review should identify reasonably practicable improvements to plant or processes and timescales for implementing them.

110. 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 nationally and internationally.

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.		

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

112. Ownership and responsibility require:

(a) an understanding of the safety case, the standards applied in it, its assumptions and the limits and conditions (operating rules) 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 ensure that the risks from activities are ALARP; and

(d) that users of safety cases be involved in their preparation to ensure that they reflect operational needs and reality.

113. The responsibility for ownership of a safety case may change within the dutyholder as the facility moves through its lifecycle, or if the dutyholder changes. Such changes of ownership are important to safety and so need to be properly managed and controlled in accordance with Licence Condition.

SITING ASPECTS

114. *This section is in two parts. The first part focuses on ONR's role in siting decisions, where our principal duty is to provide advice. The second part relates to safety case assessments and sets out principles addressing more general aspects of how the physical location of a facility can affect its safety. These aspects will be relevant both to ONR's normal permissioning work and to decisions on whether or not to grant a new site licence.*

The regulatory assessment of siting

115. *ONR's processes for the licensing and delicensing of nuclear sites, including siting requirements, are set out in the document 'Licensing Nuclear Installations' which is published on ONR's website.*

116. *IAEA safety requirements for siting are set out in the document 'Site Evaluation for Nuclear Installations' (Safety Standards Series No. NS-R-3) and also in a wide range of supporting guidance specific to nuclear power plants covering such topics as:*

- *site survey and selection;*
- *geotechnical aspects and foundations;*
- *dispersion of radioactive material;*
- *consideration of population distribution;*
- *meteorological events;*
- *external human-induced events;*
- *evaluation of seismic hazards; and*
- *flood hazard on coastal and river sites.*

117. *Many of these topics are discussed elsewhere in these principles and will be addressed in ONR safety case assessments rather than as part of siting. Others relate to areas for which ONR is not responsible but where we advise the relevant competent authority as appropriate. These areas include:*

- *authorising the construction of a nuclear facility in a particular location, which falls to the relevant national and local planning authorities;*
- *dispersion of radioactive materials which, for authorised discharges and radioactive waste disposal during normal operations, is regulated by the environment agencies;*
- *national siting policy, which falls to the UK Government; and*
- *the UK Government's submission to the European Commission of general data relating to a new nuclear installation (or a change in use of an existing installation) as required under Article 37 of the Euratom Treaty. Here ONR's advice is essentially limited to matters related to the radiological consequences of accidents.*

118. *The principles in the first part of this section focus on ONR's development control arrangements to protect the public near nuclear sites. In particular they focus on assessment activities relating to our interfaces with local authorities through which we help implement the Government's policy of managing population levels around nuclear sites to prevent them from rising to undesirable levels.*

119. *Government policy, in turn, takes into account and aligns with international conventions and agreements on nuclear safety, including IAEA Safety Standards and, where relevant, WENRA Safety Reference Levels.*

Land use planning

120. *Operators are legally required to operate their facilities in such a way that risks to employees and to the general public are reduced so far as is reasonably practicable. ONR judges compliance with this legal duty through our various regulatory activities, including our assessments of safety cases.*

121. *Although operators must have arrangements to minimise the chances of a fault leading to a release of radioactivity, the risk of an accident cannot be fully eliminated. Therefore, in order to minimise the impact of accidents, the Government has applied a policy of siting new nuclear power plants in areas where the population density does not exceed certain thresholds, and where the growth of that population can be monitored and controlled.*

122. *At the time of writing, the Government's policy on managing populations around nuclear sites is delivered by means of administrative arrangements involving ONR as a non-statutory consultee. Under these arrangements, ONR provides development control advice to planning authorities who make the planning decisions. In forming this advice, ONR consults with, and takes into account the recommendations of, the local authority emergency planners (see paragraph 770).*

Siting	Development control planning advice	ST.1
Development control planning advice provided by ONR should align with siting criteria set by Government policy.		

123. The advice should consider the potential impact of the proposed development on facilities and the operability of local emergency plans. ONR would normally only advise against a development that:

    (a) represents a significant, new external hazard to a facility; or

    (b) cannot readily be accommodated within existing off-site emergency plans; or

    (c) would have an impact on the extendibility of countermeasures beyond the REPPIR Off-site Emergency Planning Area.

124. ONR should only provide advice in circumstances consistent with our roles and responsibilities within the planning framework described above.

Dispersion of radioactive material

125. In protecting the public near nuclear sites, ONR provides regulatory oversight of radiological hazards during potential accident conditions and, for normal operations, from direct radiation shine (see Radiation protection, paragraph 576 ff.). The impact of radiation doses arising from authorised discharges and radioactive waste disposals during normal operations is regulated by the environment agencies and by the Food Standards Agency.

126. ONR consults these agencies and other bodies before granting a licence for the use of a site under NIA, as amended by the Environment Act 1995 Schedule 22 paragraph 7.

Other siting aspects affecting safety

127. *The second part of this section sets out general principles relating to how the physical location of a facility can affect its safety.*

Siting	Local physical aspects	ST.3
The safety case should take account of local physical aspects of the facility and site relevant to the dispersion of released radioactivity and its potential effects on people.		

128. Consideration should be given to aspects that might affect the movement of people and goods, including nuclear matter, into and out of the site, which have implications for safety during normal operation (see the sub-section on Control of nuclear matter (paragraph 469 ff.)).

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

130. The safety case should address all relevant aspects of local or regional topography, hydrology, geology, hydrogeology and meteorology affecting radioactivity dispersion.

Siting	Suitability of the site	ST.4
The suitability of the site to support safe nuclear operations should be assessed prior to granting a new site licence.		

131. Such assessments will normally focus on external hazards and civil engineering issues. These should consider the potential vulnerability of the site to external hazards and the extent to which construction of new facilities can be safely accomplished. These assessments should be performed according to the principles set out in paragraphs 228ff and 320ff. Wider guidance on licensing of new sites is provided in ‘Licensing Nuclear Installations’ which is published on ONR’s website.

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

132. Damage to other installations may exacerbate the consequences of accidents or impact upon the emergency response, and so will affect reasonable practicability arguments in the safety case. This principle should be applied to transport infrastructure in the vicinity of the facility as well as to fixed installations.

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.		

133. This aspect of the safety case should include consideration and analysis of:

(a) all potential radiological hazards on the site;

(b) all facilities on the site: for completeness, this should include facilities that do not contain radioactive material; and

(c) all services on the site.

134. Interactions between facilities, between facilities and shared services and between shared services, where events in one may adversely affect others, should be considered explicitly. This entails analyses of events that can have physical effects outside the boundaries or limits for the particular facility or service. These may be, for example:

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

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

(c) interactions between shared services that affect several facilities.

135. Facilities should have their own dedicated safety systems to protect against design basis faults escalating to an accident. Such safety systems should not be shared between facilities. However, safety equipment designed to assist with controlling or mitigating accidents (ie at Level 4 of Principle EKP.3) may be shared where this is justified to be in the interests of safety (eg if this provides a diverse, alternative means of restoring a lost safety function). Where equipment is shared, the safety case should demonstrate that the sharing does not increase either the likelihood or the consequences of an accident at any of the facilities.

136. 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.

137. 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 the facilities are totally independent from one another. Independence in this context means there are no common shared services, no interactions between the facilities or the services supplying them and no fault or accident at any one facility should have repercussions at any other. Where such independence cannot be demonstrated, the overall site risk should be compared with Numerical targets 5, 7 and 9 (paragraphs 695ff) and reduced so far as is reasonably practicable.

138. Consistent with the above principles, multi-facility sites should have emergency arrangements which recognise the potential for multi-facility accidents. See also paragraph 772.

139. 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 and emergency arrangements. Formal mechanisms should be established and demonstrated to be working effectively.

ENGINEERING PRINCIPLES

140. These principles comprise the major part of the SAPs. Engineering standards need to be high to achieve the necessary high levels expected for nuclear safety, including under fault conditions. As such, these principles need to be used in parallel with the Fault Analysis SAPs (paragraph 605 ff.), mirroring the iterative nature of licensees' engineering design and fault analysis processes.

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

(a) key principles;

(b) general principles; and

(c) engineering principles for specific areas.

142. Collectively, this section brings together a range of engineering topics that should be considered when assessing the safety case for a facility and/or site.

143. The requirement for ALARP is discussed in the Introduction (paragraph 9ff) and must be applied in assessments made against the engineering principles. Similarly, the engineering principles apply across a wide range of facilities of differing type and magnitude of hazard and so the guidance on adopting a proportionate approach set out in paragraph 27ff should be followed. Applying these principles therefore requires judgement in deciding which principles are relevant to the situation being assessed and then whether enough has been done in relation to each applicable principle.

144. When using these principles, inspectors should consider their relevance to all stages of a facility's lifecycle. For example, facilities should be designed and operated so that they may be decommissioned safely 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.		

145. 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 which ensures that the harm cannot happen, for example a criticality safe vessel. Inherent safety is not the same as 'passive safety' (see Glossary). Where inherently safe design is not achievable, the design should be fault tolerant.

146. Achieving an 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; and

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

147. 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.		

148. 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, however, 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
Nuclear facilities should be designed and operated so that defence in depth against potentially significant faults or failures is achieved by the provision of multiple independent barriers to fault progression.		

149. 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 independent barriers (inherent features, equipment and procedures) aimed at preventing faults in the first instance, and ensuring appropriate protection or mitigation of accidents in the event that prevention fails.

150. Defence in depth should prevent faults, or if prevention fails should ensure detection, limit the potential consequences and stop escalation.

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

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

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

(c) inherent safety features of the facility, failsafe design and safety measures are provided to protect against fault conditions progressing into accidents; and

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

152. Defence in depth is generally applied in five levels, which should be, as far as practicable, independent from one another. The methodology should ensure that if one level fails, it will be compensated for, or corrected by, the subsequent level. The aims for each level are described in detail in IAEA Safety Requirements SSR2/1 (Ref. 10) 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	Defence/Barrier
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 to protect against escalation to an accident	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 protecting against further fault escalation and mitigation of the consequences of severe accidents	Additional measures and procedures to protect against or mitigate fault progression and for accident management
Level 5	Mitigation of radiological consequences of significant releases of radioactive material	Emergency control and on- and off-site emergency response

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

154. The identification of safety functions should be based on an analysis of normal operation and all significant fault sequences arising from possible initiating faults determined by fault analysis (see paragraph 605 ff.). It should also include faults initiated by internal and external hazards (see paragraph 228ff).

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

155. 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 a fault or accident.

(d) Administrative safety measures (see paragraph 446 ff.).

(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.

156. The availability and reliability of the safety measures should be commensurate with the significance of the radiological hazards being controlled and their safety functions within the defence in depth hierarchy (Principle EKP.3). In particular, mitigating safety measures (Level 4) should not be regarded as a substitute for fault prevention (Levels 1 and 2) or protection (Level 3) barriers, but as further defence in depth. More generally, priority should be given to providing reliable and effective barriers (inherent features, equipment and procedures earlier in the hierarchy) so that later barriers, though in place, need not be called upon.

157. Where the safety functions might be affected by security considerations, the design process should seek to treat safety and security in a complementary manner (see paragraph 39), The process should aim to ensure that the measures designed for one will also serve the interests of the other. In particular, safety and security measures should be designed and implemented in such a manner that they do not compromise one another.

Safety classification and standards

158. *Effective implementation of the safety aspects sought by the Key Engineering Principles relies upon a number of general principles and related measures aimed at ensuring the reliability and capability of the facility's safety measures. For instance, it is important that structures, systems and components, including software for instrumentation and control, are classified on the basis of their safety significance as determined by the fault analysis of the facility (see Principle FA.1). For designs under development, the safety classification may be an iterative process, with preliminary assignments of the safety class of structures, systems and components needing to be finalised using fault analysis. It is important that all structures, systems and components are designed, manufactured, installed and then subsequently commissioned, operated and maintained to a level of quality commensurate with their classification. The principles given within this section are intended to apply to all levels of defence in depth listed in Table 1).*

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 identified and then categorised based on their significance with regard to safety.		

159. The identification should follow a systematic approach linked to the fault analysis for the facility (see paragraph 605 ff.). For power reactors, the set of safety functions should address the three fundamental safety functions listed in paragraph 540. For other facilities, an analogous list of fundamental safety functions should be derived appropriate to the prevailing risks and hazards and then used as part of the safety function identification. The safety functions identified should be sufficiently detailed to support subsequent safety classification activities (see Principle ECS.2) and to facilitate a clear demonstration in the safety case of their effective delivery.

160. The safety categorisation scheme employed should be linked explicitly with the licensee's design basis analysis (see paragraph 607). Various schemes are in use in the UK; these principles have been written assuming categorisation 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 contributing to nuclear safety.

161. The method for categorising safety functions should take into account:

(a) the consequence of failing to deliver the safety function;

(b) the likelihood that the function will be called upon; and

(c) the extent to which the function is required, either directly or indirectly, to prevent, protect against or mitigate the consequences of initiating faults.

162. 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 that deliver the safety functions.

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

164. Where safety functions are delivered or supported by human action, these human actions should be identified and classified on the basis of those functions and their significance to safety (see Principle EHF. 3). The methods used for determining the

classification should be analogous to those used for classifying structures, systems and components outlined in the following paragraphs.

165. Methods for classifying the safety significance of structures, systems or components should be based primarily 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 probability that the item will be called upon to perform a safety function;

(c) the potential for a failure to initiate a fault or exacerbate the consequences of an existing fault, including situations where the failure affects the performance of another system, structure or component (see paragraphs 167 and 168); and

(d) the time following any initiating fault at which, or the period throughout which, it will be called upon to operate in order to bring the facility to a stable, safe state.

166. A number of different safety classification schemes are in use in the UK. The following scheme, linked to the categorisation scheme outlined in paragraph 160, is recommended in these principles:

(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 contributing to a categorised safety function.

167. Appropriately designed interfaces should be provided between (or within) 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.

168. Auxiliary services (including essential services, see paragraph 436 ff.) 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 its safety functions.

Engineering principles: safety classification and standards	Codes and 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 codes and standards.		

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

170. Codes and standards should be preferably nuclear-specific, leading to a conservative design commensurate with the importance of the safety function(s) being delivered. Each code or standard adopted should be evaluated to determine its applicability, adequacy and sufficiency and should be supplemented or modified as necessary to a level commensurate with the importance of the relevant safety function(s).

171. Appropriate nuclear industry-specific, national or international codes and standards should be adopted for Class 1 and 2 structures, systems or components. For Class 3, if there is no appropriate nuclear industry-specific code or standard, an appropriate non-nuclear-specific code or standard should be applied instead.

172. Where a single item (ie a structure, system or component) needs to deliver multiple safety functions, and these can be demonstrated to be delivered by the item independently of one another, then separate codes and standards should be used appropriate to the parts of the item providing each safety function. Where such independence cannot be demonstrated, codes and standards should be appropriate to the class of the item (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 item, the compatibility between these codes and standards should be demonstrated.

173. The combining of different codes and standards for a single aspect of a structure, system or component should be avoided. Where this cannot be avoided, the combining of the codes and standards should be justified and their mutual compatibility demonstrated.

Engineering principles: safety classification and standards	Absence of established codes and standards	ECS.4
Where 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, should be adopted.		

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 structure, system or component 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 applied to confirm that structures, systems and components will perform their allocated safety function(s) in all normal operational, fault and accident conditions identified in the safety case and for the duration of their operational lives.		

174. The qualification procedures should provide a level of confidence commensurate with the safety classification of the structure, system or component.

175. The qualification procedures should address all relevant operational, environmental, fault and accident conditions (including severe accidents).

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

177. The procedures should ensure that adequate arrangements exist (Licence Condition 6) 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

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

179. *Ideally, the structures, systems and components should be failsafe, ie they should have no unsafe failure modes.*

180. *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, 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.*

181. *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 protect against 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 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.		

182. Consideration should be given to spurious operation, unsafe failure modes and how modes of failure can be predicted or revealed and then repaired.

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.		

183. 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 addressed explicitly where a structure, system or component employs redundant or diverse components, measurements or actions to provide high reliability.		

184. CCF claims should be substantiated.

185. 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 ONR 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.

186. 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.

187. Where required reliabilities cannot be achieved due to CCF considerations, the 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.		

188. 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 SSG-2 (Ref. 11).

189. A system that is the principal means of fulfilling a Category A safety function (see paragraph 160) should, other than in exceptional circumstances, always be designed to meet the single failure criterion. However, other systems which make a contribution to fulfilling the same safety function, but are independent of the principal system, do not necessarily need to meet the single failure criterion.

Reliability claims

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

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

191. 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) where warranted, eg for complex items, an independent third-party assessment; and

(d) periodic review of further developments in technical information, precedent and relevant good practice.

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.		

192. Evidence should be provided to demonstrate the adequacy of these 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.

193. Where data is inadequate, appropriate measures should be taken to ensure that the onset of failures will be detected, and that the consequences of failure are minimised. Such measures may, for example, include planned replacement after a fixed lifetime, or be achieved through a programme of examination, maintenance, inspection and/or testing.

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

194. For requirements that are less demanding, or on a longer timescale, administrative safety measures, ie those involving operator actions based on procedures, may be acceptable. The choice of the safety measure should take into account the hierarchy in paragraph 155 and the category of safety function to be delivered (see Principles ECS.1 and ECS.2).

Engineering principles: reliability claims	Margins of conservatism	ERL.4
Where safety-related systems and/or other means are claimed to reduce the frequency of a fault sequence, the safety case should include a margin of conservatism to allow for uncertainties.		

195. 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 paid to potential common cause failures, uncertainties in assigned reliability values, availability, and measures to ensure that the system's safety significance will continue to be recognised throughout its life. This is particularly important where claims are made on combinations of safety-related systems.

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 defined in the safety case.		

196. The commissioning tests should:

(a) demonstrate that, as built, the design intent claimed in the safety case has been achieved;

(b) collect baseline data for equipment and systems for future reference;

(c) validate those operating instructions (etc) for which the commissioning tests provide representative activities and/or conditions; and

(d) familiarise the operators with the operation of the facility or process.

197. The commissioning tests should be designed to identify any errors remaining following the design, manufacture, or construction/installation stages. However, the commissioning tests should not be used as the main means of identifying such errors – robust processes at these earlier stages should be applied to drive out any errors so that the commissioning tests can be used to confirm, as far as practicable, the absence of errors.

198. 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. 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. Equipment designed to mitigate severe accident scenarios should be tested as far as reasonably practicable during commissioning testing.

199. The safety case should be reviewed and updated in the light of the results of the commissioning tests and of any modifications made to the design or intended operating procedures that result.

200. The tests should be divided into stages to complete as much (inactive) testing as practicable before the introduction of radioactive material. Inactive testing should demonstrate that the facility or plant has been constructed, manufactured, and installed correctly and that it is functioning to specification (eg instrumentation is correctly calibrated). The tests should begin with component and system testing prior to performing integrated tests. Where any deviation from the documentation is found, this should be demonstrated not to conflict with the safety case, or the safety case should be updated accordingly.

201. 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 validated during active commissioning. Before active commissioning can begin, the necessary arrangements to satisfy Principles MS.2 and SC.6, especially in relation to operating rules, 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.		

202. The testing, inspection and maintenance should be carried out in a manner, governed by procedures, and apply codes and standards appropriate to the class of the structure, system or component (see Principle ECS.3).

203. Appropriate and sufficient locations should be provided within the facility 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 should receive regular and systematic examination, inspection, maintenance and testing as defined in the safety case.		

Engineering principles: maintenance, inspection and testing	Type-testing	EMT.3
Structures, systems and components should be type tested before they are installed to conditions equal to, at least, the most onerous for which they are designed.		

204. The term type testing describes 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; and

(d) provides evidence that it meets its specification.

205. For components of particular concern and where it is not possible to confirm their ability to operate under the most onerous design conditions, additional analysis should be carried out which utilises available test results and justifies the component's performance and reliability.

206. Reference data should be taken from type testing to establish a baseline for in-service performance.

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

207. Maintenance and other invasive activities should be carried out according to procedures that ensure that foreign material (eg debris, tools etc) is excluded, or detected and removed. Procedures for avoiding foreign material should likewise be adopted during initial installation activities.

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.		

208. 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 (including portable equipment) in service or at intervals throughout their life, commensurate with the reliability required of each item.		

209. 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 adequate long-term performance would be achieved without additional measures.

209.1 Where test equipment, or other engineered means, is used for in-service or periodic testing, maintenance, monitoring or inspection, the extent to which they reveal failures affecting safety functions should be justified. The test equipment, or other engineered means, should itself be tested at intervals sufficient to uphold the reliability claims of the equipment under test.

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

210. Examination, inspection, maintenance 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. Where equipment important to safety is taken out of service for examination, inspection, maintenance or testing, the continuing safety of operations should be justified. Furthermore, the potential for the examination, inspection maintenance or testing to initiate a fault should be analysed and the risks so arising justified.

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

Engineering principles: maintenance, inspection and testing	Continuing reliability following events	EMT.8
Structures, systems and components should be inspected and/or re-validated after any event that might have challenged their continuing reliability.		

Ageing and degradation

212. *Effective management of ageing is needed so that the safety functions of structures, systems and components are delivered throughout the period needed, which may be the full lifetime of the facility. This may be achieved through a specific ageing management programme or through other arrangements appropriate to the structure, system or component.*

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.		

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

214. 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.		

215. 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.

216. 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.

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

218. 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.

219. Timely mitigation of ageing and its effects should be undertaken to ensure that adequate 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.		

220. The properties should be obtained from fully representative samples of the material especially when the component or structure performs a principal role in 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.		

221. 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

222. *The following principles address the layout of the facilities on a site, of the plant within facilities and of structures, systems and components at the facility.*

223. *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. The layout may have an*

influence upon the ability to meet the duty to reduce radiation exposures to ALARP and can be a factor in providing means of preventing unauthorised access. Layout can also affect the consequences of faults, particularly from internal and external hazards, and the access conditions following faults or accidents.

Engineering principles: layout	Access	ELO.1
The design and layout should facilitate access for necessary activities and minimise adverse interactions while not compromising security aspects.		

224. The layout should:

(a) make provision for construction, assembly, installation, erection, decommissioning, maintenance and demolition;

(b) ensure that sufficient access, lighting etc is available to carry out all necessary operational, maintenance, inspection and testing activities;

(c) ensure that radiation doses to workers carrying out operational, maintenance, inspection and testing activities are ALARP;

(d) minimise adverse interactions with other structures, systems or components during operational, maintenance, inspection and testing activities and during fault or accident conditions;

(e) provide an alternative means of access to facilities and control functions essential to safety that may require local manual intervention;

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

(g) provide for alternative access to rescue equipment in all normally manned areas; and

(h) make provision for equipment and services required for accident management and emergency preparedness.

Engineering principles: layout	Unauthorised access	ELO.2
Unauthorised access to, or interference with, structures, systems and components or their reference data (including Building Information Modelling (BIM)) should be prevented.		

225. Unauthorised access includes remote access to computer programs and reference data.

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

Engineering principles: layout	Minimisation of the effects of incidents	ELO.4
The design and layout of the site, its facilities (including enclosed plant), support facilities and services should be such that the effects of faults and accidents are minimised.		

226. For example, the design and layout should:

(a) minimise the direct effects of initiating events, particularly from internal and external hazards, on structures, systems or components;

(b) not compromise the safety of the site, or its facilities, structures, systems and components;

(c) minimise any interactions between a failed structure, system or component and other structures, systems or components;

(d) ensure that site personnel are physically protected from direct and indirect effects of faults; and

(e) facilitate access for necessary recovery actions and re-supply of essential stocks, materials, equipment and personnel following an accident.

227. Essential services and support facilities important to the safe operation and/or safe shutdown of the facility should be designed and routed so that, in the event of a fault or accident, sufficient capability to perform their safety functions will remain. Support facilities and services include access roads, water supplies, fire mains, flood defences and drainage, essential services and site communications.

External and internal hazards

228. *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 under duties deriving from security legislation (see paragraph 39).*

229. *Internal hazards are those hazards to the facility or its structures, systems and components that originate within the site boundary and over which the dutyholder has control in some form. The term is usually limited to apply to hazards external to the process, in the case of nuclear chemical plant, or external to the primary circuit in the case of power reactors. Internal hazards include internal flooding, fire, toxic gas release, dropped loads or impact and explosion/missiles. Again, this list is not exhaustive.*

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

Engineering principles: external and internal hazards	Identification and characterisation	EHA.1
An effective process should be applied to identify and characterise all external and internal hazards that could affect the safety of the facility.		

231. Hazards should be identified in terms of their severity and frequency of occurrence and characterised as having either a discrete frequency of occurrence (discrete hazards), or a continuous frequency-severity relation (non-discrete hazards). All hazards should be treated as initiating events in the fault analysis.

232. Discrete hazards are those that are realised at a single frequency (or set of discrete frequencies) with associated hazard severity/magnitude(s). Most internal hazards such as steam release are discrete hazards.

233. Non-discrete hazards are those that can occur across a continuous range of frequencies and are defined in terms of a hazard curve (a plot of hazard severity against the frequency of this severity being exceeded). Seismic hazard is an example of a non-discrete hazard.

234. The identification process should include reasonably foreseeable combinations of independently occurring hazards, causally-related hazards and consequential events resulting from a common initiating event (see Principle FA.2).

Engineering principles: external and internal hazards	Screening	EHA.19
Hazards whose associated faults make no significant contribution to overall risks from the facility should be excluded from the fault analysis.		

235. Screening criteria should be defined in terms of frequency of occurrence and potential consequences as follows.

Discrete hazards may be excluded that:

(a) have no significant identified consequential effect on the safety of the facility; or

(b) have a total initiating event frequency that is demonstrably below once in ten million years per annum.

Non-discrete hazards may be excluded where:

(a) their associated faults have no significant consequential effect on the safety of the facility; or

(b) their frequency of exceedance on their hazard curve is below once in ten million years.

Screening should retain all faults associated with both types of hazard that have the potential to make a significant contribution to the overall risks from the facility. See also paragraphs 631 and 649.

236. The potential for a hazard to affect safety should take account of the potentially widespread effects of external (and some internal) hazards (including concurrent and consequential hazards) which may challenge multiple safety functions and locations simultaneously. In addition, the hazard may affect multiple facilities, as well as the local and national infrastructure. Therefore the impact on accident management and emergency preparedness arrangements, such as site access and services, and also consequential hazards from adjacent nuclear and non-nuclear facilities, should be considered

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.		

237. Site-specific data should be collected and used to support and/or validate calculations of external hazard event severities and frequencies. Where neither facility-specific nor generic data is available, use of expert judgement may be acceptable, provided that the basis for the judgement is suitably justified.

238. Further guidance on applying valid data and models is provided in paragraphs 678 ff., and in particular Principles AV.3 and AV.7.

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 (see Principle EHA.19), a design basis event should be derived.		

Engineering principles: external and internal hazards	Frequency of initiating event	EHA.4
For natural external hazards, characterised by frequency of exceedance hazard curves and internal hazards, the design basis event for an internal or external hazard should be derived to have a predicted frequency of exceedance that accords with Fault Analysis Principle FA.5. The thresholds set in Principle FA.5 for design basis events are 1 in 10 000 years for external hazards and 1 in 100 000 years for man-made external hazards and all internal hazards (see also paragraph 629).		

Frequency of exceedance

239. For external hazards, the design basis event should be derived conservatively to take account of data and model uncertainties. The thresholds set in FA.5 for design basis events are 1 in 10 000 years for external hazards and 1 in 100 000 years for internal hazards (see also paragraph 629).

240. For non-discrete hazards, consideration may be given to arguments to derive design basis events from a higher frequency of exceedance if the facility (or the relevant parts of it) cannot give rise to significant unmitigated consequences.

241. Where the unmitigated consequences arising from an external hazard are low, it may be appropriate for a facility (or relevant parts of it) to be designed against hazard-induced loads applying normal industrial standards.

242. Some hazards may not be amenable to the derivation of a design basis event based on frequency. In such cases a surrogate maximum credible event, supported by scientific evidence, may be defined. The severity of the maximum credible event should be compatible with the principles of FA.5.

Engineering principles: external and internal hazards	Analysis	EHA.6
The effects of internal and external hazards that could affect the safety of the facility should be analysed. The analysis should take into account hazard combinations, simultaneous effects, common cause failures, defence in depth and consequential effects.		

Engineering principles: external and internal hazards	Design basis event operating states	EHA.5
Analysis of design basis events should assume the event occurs simultaneously with the facility's most adverse permitted operating state (see paragraph 631 c) and d)).		

243. The analysis should apply an appropriate combination of engineering, deterministic and probabilistic methods in order to:

- understand the behaviour of the facility in response to the hazard; and
- confirm high confidence in the adequacy of the design basis definition and the associated fault tolerance of the facility.

244. The analysis should include hazard analysis to:

(a) identify the potential impact of the hazard on the facility's structures, systems and components, and in particular its safety systems;

(b) determine the need for segregation, diversity and redundancy of plant and equipment and the location of barriers to limit this impact; and

(c) determine the safety functions (eg the withstand capability) to be provided by such barriers.

245. The analysis should take into account that:

(a) certain internal or external hazards may not be independent of one other and may occur simultaneously or in combinations that are reasonable to expect;

(b) the initiating hazard, or its effects may persist as the fault sequence progresses (see paragraph 631 a)).

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

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

(e) the most severe internal and external hazards have the potential to threaten more than one level of defence in depth (see Principle EKP.3) at once;

(f) internal hazards (eg fire) can arise as a consequence of faults internal or external to the site; and

(g) the severity of the consequences of internal and external hazards will often be affected by aspects such as facility layout, interactions between structures, systems and components, and building size and shape.

Engineering principles: external and internal hazards	Beyond design basis events	EHA.18
Fault sequences initiated by internal and external hazards beyond the design basis should be analysed applying an appropriate combination of engineering, deterministic and probabilistic assessments.		

246. The following items refer to discrete and non-discrete hazards unless specified. Analysis of beyond design basis events should:

(a) confirm the absence of 'cliff edge' effects just beyond the design basis (Principle EHA.7);

(b) identify the hazard level at which safety functions could be lost (ie determine the beyond design basis margin) (non-discrete hazards only);

(c) provide an input to probabilistic safety analysis of whether risks targets are met (see paragraph 713 ff.);

(d) ensure that safety is balanced so that no single type of hazard makes a disproportionate contribution to overall risk (see paragraph 749); and

(e) Provide an input to severe accident analysis (non-discrete hazards only) (see paragraphs 663 ff.).

Engineering principles: external and internal hazards	'Cliff-edge' effects	EHA.7
A small change in design basis fault or event assumptions should not lead to a disproportionate increase in radiological consequences.		

247. A cliff edge is where a small change in analysis assumptions, such as those relating to design basis hazard severity, facility response, or design basis analyses is predicted to lead to a disproportionate increase in radiological consequence.

248. The above principle should be applied both within the design basis and as part of severe accident analysis (see paragraphs 663 ff.). The analysis should identify the margins beyond the design basis to the point(s) where safety functions would no longer be achieved, as a function of increasing hazard severity. These margins should be used within the severe accident analysis to determine aspects such as the timescales available for remedial actions and the conditions which would result in a radiological release. The analysis should state the conditions under which the design basis cannot be met. This should be an input to the severe accident analysis process.

Engineering principles: external and internal hazards	Aircraft crash	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 should be determined.		

249. The calculation of crash frequencies 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).

250. Should the total predicted aircraft crash frequency be shown to be lower than that typically defined as a design basis event, but greater than that which can be automatically excluded (see paragraph 235), efforts should be made to understand and minimise the potential crash consequences on affected structures, systems and components.

251. The direct and indirect effects of aircraft crashes on structures, systems and components needed to achieve a stable, safe state should be analysed. These should include effects relating to mechanical resistance, vibrations and structural and component integrity.

252. The analysis should include fire and explosion hazards deriving from aircraft crashes including fires caused by aircraft fuel, fire ball and pool fire combinations and other consequential fires due to the aircraft crash. Buildings (or parts of buildings) containing nuclear fuel or housing structures, systems and components needed to achieve a stable, safe state should be designed to prevent aircraft fuel from entering them.

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

253. The evaluation 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;

(c) enable buildings, structures and plant in the facility to be designed to withstand safely the ground motions involved; and

(d) enable existing structures, systems and components to be seismically assessed.

254. An operating basis earthquake (OBE) should also be determined. No structure, system or component should be impaired by the repeated occurrence of ground motions at the OBE level. Where the appropriate response to an OBE is a facility or

plant shutdown, the facility or plant should not be restarted until inspections have shown that it is safe to do so.

255. In determining the effects of a seismic event on the facility, the effects of the event on other facilities or installations in the vicinity, and on the safety of any system or service at the facility, should also be taken into account. The effects of failure of non-nuclear safety related structures, systems and components (SSCs) should be taken into account if this could affect access for the control and/or repair of plant.

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

256. 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, the facility's systems and components, particularly instrumentation.

Engineering principles: external and internal hazards	Weather conditions	EHA.11
Facilities should be shown to withstand weather conditions that meet design basis event criteria. Weather conditions beyond the design basis that have the potential to lead to a severe accident should also be analysed.		

257. Types of weather conditions to be analysed should include (but not be limited to) abnormal wind loadings, wind-blown debris, precipitation, accumulated ice and snow deposits, lightning, extremes of high and low temperature, humidity and drought.

258. Design basis events should take account of reasonable combinations of extreme weather conditions that may be expected to occur, and of consequential hazards from adjacent nuclear and non-nuclear facilities arising from the extreme weather. Arrangements that give forewarning of developing weather conditions that could realistically give rise to a challenge to the effective functioning of safety related SSCs should be provided.

259. The reasonably foreseeable effects of climate change over the lifetime of the facility should be taken into account, particularly during Periodic Safety Reviews.

Engineering principles: external and internal hazards	Flooding	EHA.12
Facilities should be shown to withstand flooding conditions up to and including the design basis event. Severe accidents involving flooding should also be analysed.		

260. The design basis flood should take account, as appropriate, of the combined effects of wind, wave actions, duration of the flood and flow conditions. These should be assumed to occur simultaneously with the most adverse tidal cycle (see also Principle EHA.5). The effects of flooding on the ground conditions and the potential for any slope instability should be considered.

261. Facilities should be protected against a design basis flood by adopting a layout based on maintaining the ‘dry site concept’. In the dry site concept, all vulnerable structures, systems and components should be located above the level of the design basis flood, together with an appropriate margin in accordance with Principle EHA.7. This may be accomplished by locating the plant at a sufficiently high elevation, or by structural arrangements that raise the ground level (eg by use of fill material). In the latter case, the safety functions delivered by these structures should be assured through appropriate safety management arrangements including the ECS principles (paragraph 158ff).

262. Where it is not practicable to adopt the dry site concept, the design should include permanent external barriers such as levees, sea walls and bulkheads. Applying Principle EHA.7, the design parameters for these barriers may need to be more onerous than those derived from the design basis flooding event. The barriers should be subject to appropriate safety management arrangements (including periodic inspections, monitoring and maintenance (see Principle ECE.23)), even if their locations mean they are not under the direct responsibility of the licensee. In addition, levees, sea walls and bulkheads (etc) should be designed to ensure that water can leave the site when needed and that they do not act as a dam.

263. In line with Principle EKP.3 (defence in depth), consideration should be given to extreme hydrological phenomena. The design of all structures, systems and components needed to deliver the fundamental safety functions in any permitted operational states should be augmented by protection from water ingress and waterproofing as a redundant measure to provide a further barrier in the event of flooding of the site.

264. All structures, systems and components vulnerable to failure from water intrusion, submergence or consequential effects that cannot be placed above the design basis flood level should be protected by engineered features designed to prevent water intrusion and submergence and protect against consequential effects. All other structures, systems and components should be protected against the effects of a design basis flood. See also Principle ECE.9. Consideration should be given to the possibility that flood water may act as a moderator when fissile material is present.

265. The consequences of the design basis flood being exceeded should be taken into account in the design of the facility, with particular attention paid to overtopping of defences and cliff edge effects. Severe beyond design basis and severe accident analysis (see paragraph 651 ff.) should be used as part of the design process.

266. Arrangements that give forewarning of developing weather conditions that could realistically lead to flooding of the site should be provided. These should be designed to ensure there will be sufficient time to complete any necessary preparatory activities (eg the safe shutdown of the facility) and allow for the timely implementation of emergency procedures. The arrangements should employ real time monitoring so far as this is practicable, and draw from the hazards analysis in the safety case.

267. 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.

Engineering principles: external and internal hazards	Use, storage and generation of hazardous materials	EHA.13
The on-site use, storage or generation of hazardous materials should be minimised, controlled and located, taking due account of potential faults.		

268. Principle EKP.1 is relevant here and should lead to designs that seek to (for example) eliminate the hazard or use less hazardous substitutes.

269. The analysis should take due account of fires, missiles, toxic gases etc, either resulting from a fault or as part of an initiating event. The potential faults considered should include the inadvertent release of the hazardous material.

270. The potential for generation of hazardous materials (including toxic, corrosive and flammable materials) through normal processes or in fault conditions should be analysed.

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, quantified and analysed within the safety case.		

271. The safety case should include:

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

(b) the adequacy of protection from the effects of faults and accidents either within or external to the facility; and

(c) sources of harm such as means of transport, pipelines, power supplies and water supplies, located either inside or outside the site.

Engineering principles: external and internal hazards	Hazards due to water	EHA.15
The design of the facility should prevent water from adversely affecting structures, systems and components.		

272. 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. Where this is not reasonably practicable, the structures, systems and components should be adequately protected against the effects of water. (See also Principle EHA.12.)

Engineering principles: external and internal hazards	Appropriate materials in case of fires	EHA.17
Non-combustible or fire-retardant and heat-resistant materials should be used throughout the facility (see Principle EKP.1).		

Engineering principles: external and internal hazards	Fire detection and fighting	EHA.16
Fire detection and fire-fighting systems of a capacity and capability commensurate with the worst-case design basis scenarios should be provided.		

273. A fire hazard analysis should be carried out to:

(a) analyse the potential for fire initiation and growth and the possible consequences for the facility's structures, systems and components;

(b) determine the need for segregation of plant and equipment and the locations and required fire resistance of boundaries needed to limit the spread of fires; and

(c) determine the capacity and capability of the detection and fire-fighting systems.

274. 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 (see Principle EHA.15).

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 significant release of radioactivity should be prevented.		

275. In such situations:

(a) adequate redundancy and, where appropriate, diversity of the 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.		

276. The flow limiting devices should be as close to the main circuit as practicable. Where appropriate, 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 need 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.		

277. 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.

278. 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 necessitate 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 or toxic material from the facility to the environment is minimised. The potential to create an explosive atmosphere from the discharge should also be considered.		

279. The design should consider potential faults in the pressure discharge route which could prevent it delivering its safety functions. These might include blocking of or bypassing of filters, leakages and escapes, and the reliability of the system in fault or accident conditions.

Integrity of metal components and structures

280. *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. Guidance on assessing the safety of concrete structures and of non-metallic components and structures is provided in paragraphs 331 ff. and in paragraphs ENC paragraph 320 ff. respectively.*

281. *Structural integrity aspects of the safety case should be based on sound engineering practice and take account of the safety functions that need to be delivered. 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, are tested before coming into service to demonstrate the delivery of safety functions and are then monitored during service.

282. *The guidance caters for two types of situation commonly encountered in structural integrity assessments. Paragraph 286ff describes the approach that should be followed for highest reliability components or structures and where the safety case argues that gross failures can be discounted. The approach for other components and structures is described in paragraph 297ff, whilst paragraph 299 emphasises the importance of robust consequence arguments in situations where gross failure cannot be discounted. In either situation, the principles described in paragraph 301ff should also be applied.*

283. *Throughout the EMC principles 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).*

284. *The general lack of adequate reliability data for the disruptive failure of metal components and structures leads to assessments being based primarily on established engineering practice. As a result, although the radiological consequences of the failure of some components or structures may be significant (into the range where there are societal risks), 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 effects of the component or structure failure to be 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 that 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.*

285. Reliability estimates 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 1×10^{-5} per annum (pa) (see Principle FA.5);

(b) provide initiating event frequency input to fault analyses. Where the unmitigated consequences are large, consideration of initiating events with claimed frequencies rather less than 1×10^{-5} pa may be needed. As claimed failure frequencies for components and structures decrease (and certainly for claims notably less frequent than 1×10^{-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 will be made on a case by case basis; and

(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 these.

Highest reliability components and structures

286. *Discounting gross failure of a component or structure is an onerous approach to constructing an adequate safety case. Cases following this approach should provide*

an in-depth explanation of the measures over and above normal practice that support and justify the claim that gross failures can be discounted. If this cannot be justified, it may be possible to instead consider a case based on consequences (see paragraph 289).

287. *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 the gross failure of a reasonable sized pressure vessel. Therefore a claim that gross failure of a pressure vessel can be discounted is not plausible for failure rates much better than 1 x 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.*

288. A general aim for safety cases is that no single class of fault should dominate the overall facility risk. This should be borne in mind when considering the structural integrity safety case.

289. Where:

(a) the case cannot meet the level needed for a claim that the likelihood of an initiating 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 considered explicitly. This could involve a site-specific evaluation of short and long-term off-site consequences and would still need some estimate of the reliability of the components or structures in question. This broadening of the basis of the safety case would clearly need the involvement of specialisms in addition to structural integrity.

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

(a) a metal component or structure performs a principal role in ensuring nuclear safety; and

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

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

291. An example of the need to apply Principles EMC.1 to EMC.3 would be when considering the safety case for a steel reactor pressure vessel (RPV) containing a large core. The RPV will need 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 safety functions 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 a properly informed engineering judgement can be made that: (a) the metal component or structure is as defect-free as possible; and (b) the metal component or structure is tolerant of defects.		

292. In the first instance the safety case development process should identify situations that fall under Principle EMC.1. For non-redundant items (eg a 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 in the 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.		

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

294. A minor failure in a component or structure that performs a principal role in ensuring nuclear safety should not lead to significant radiological consequences.

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 identified in the safety case.		

295. To meet Principles EMC.1 and EMC.2, the 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, faults and accident conditions. This should include plant transients 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) confirmatory testing to demonstrate that the parent materials and welds have the appropriate material properties, especially strength and the necessary resistance to fracture;

(g) application of high standards of manufacture, including manufacturing inspection and examination;

(h) high standards of quality management throughout all stages of design, procurement, manufacture, installation and operation (see also paragraph 207 on excluding foreign material);

(i) pre-service and in-service examination to detect and characterise defects at a stage before they could develop to cause gross failure;

(j) defined limits of operation (operating rules), supported as necessary by safety measures (eg overpressure protection);

(k) in-service monitoring of facility operational parameters;

(l) in-service materials monitoring schemes;

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

(n) a process for review of and response to deviations;

(o) 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; and

(p) 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.

296. The strength and extent of the evidence provided here should be commensurate with its importance to the overall safety case.

Other components and structures

297. *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 168ff) and EMC.4 to EMC.34 below that expand on Principle EMC.3.*

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

299. *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.*

300. 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

301. *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.*

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

302. 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 components and structures important to safety are both free from significant defects and are tolerant of defects.		

303. The demonstration under Principle EMC.5 is expected to be less demanding than for the structures and components covered by the demanding situations under Principle EMC.1. The level of demonstration 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 full lifetime of the facility, there should be means to establish the existence of defects of concern.		

304. 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
The schedule of design loadings (including combinations of loadings) for components and structures, together with conservative estimates of their frequency of occurrence should be used as the basis for design against normal operation, fault and accident conditions. This should include plant transients and tests together with internal and external hazards.		

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

305. 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 (an aid to volumetric examination);

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

(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.		

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

306. *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.		

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 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	Third-party inspection	EMC.18
Manufacture and installation should be subject to appropriate third-party independent inspection to confirm that processes and procedures are being followed.		

Engineering principles: integrity of metal components and structures: manufacture and installation	Non-conformities	EMC.19
Where non-conformities with 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 apply the same standards as originally intended.		

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.		

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

Manufacturing, 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 capable of demonstrating with suitable reliability that the component or structure has been manufactured to an appropriate standard and will be fit for purpose at all times during future operations.		

308. This principle and the subsequent Principles EMC.28 to EMC.30 apply to the examination and testing during manufacturing, pre-service inspection and 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
Methods of 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	Qualification	EMC.30
Personnel, equipment and procedures should be qualified to an extent consistent with the overall safety case and the contribution of examination to structural integrity aspects of the safety case.		

309. The classification of the component or structure should be taken into account when determining the appropriate extent of the redundancy, diversity and qualification needed.

Operation

Engineering principles: integrity of metal components and structures: operation	Safe operating envelope	EMC.21
Throughout their operating life, components and structures should be operated and controlled within defined limits and conditions (operating rules) derived from the safety case.		

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 activity.		

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.		

310. In particular, for ferritic steel nuclear reactor pressure vessels (RPVs):

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

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

Note: For other conditions, the RPVs should also 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 relevant uncertainties and conditions are considered so that adequate margins on toughness are shown.

Monitoring

311. Monitoring aspects of ageing and degradation are dealt with in Principles EAD.2 to EAD.4.

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

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

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.		

312. These assessments 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.

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.		

313. 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 overall significance, not just the direct consequences 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.		

314. The stress analysis 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 their contribution to the safety case.		

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

316. 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 needed 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.		

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

318. Initiation fracture toughness should be the basis for analysis of normal loading conditions. For fracture analyses of extreme 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.

319. Where analysis is conducted for dynamic loading events (where the component or structure mass and stiffness are both needed to characterise the response to a loading, eg in a fault 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.

Integrity of non-metallic components and structures

320. This sub-section is concerned with the engineering assessment of the integrity of non-metallic components and structures. There are a range of components and structures, such as pressure vessels, storage tanks and pipework, which can be manufactured from a variety of non-metallic materials. In the nuclear context, non-metallic materials may be chosen in preference to metallic equivalents due to their corrosion or chemical resistance properties.

321. For the avoidance of doubt, non-metallic components and structures in this context do not include concrete structures, nor graphite reactor cores; these are addressed instead in paragraphs 331 ff. and 365 ff. respectively. Neither do they include non-metallic coatings applied to metal components, which are part of the assessment of the metal component.

322. Whilst there may be benefits in using non-metallic components and structures there may also be limitations on the structural reliability that can be claimed. For example:

- *nuclear design and construction codes may not exist for non-metallic components and structures;*
- *fitness for purpose assessment methodologies may not exist;*
- *the ability to detect defects or degradation in the component or structure may be more limited than in the equivalent metallic component or structure;*
- *many non-metallic materials have the potential to fail in a non-ductile manner which, combined with the limitations in detecting defects and degradation, may mean there is little forewarning of failure; and*
- *there may be material-specific degradation mechanisms that need to be taken into account such as low temperature creep and the potential for UV degradation.*

323. There may also be limitations on the internal or external hazards performance compared to their metallic equivalents. Principles EHA.1 to EHA.18 need therefore to be used to identify any such limitations.

324. Fire can be a particularly important hazard for non-metallic components or structures. For example, a fire could lead to premature failure of the component or structure itself; it could affect the performance of fire barriers where non-metallic components or structures pass though the barrier; or the component or structure may add to the fire loading if it is combustible.

325. The resistance of non-metallic components or structures to impact is also likely to be significantly less than for the metallic equivalent. Furthermore, impacts to some materials have the potential to weaken the component or structure without outward signs of damage.

326. The Principles EMC.1 to EMC.34 used to assess the integrity of metal components and structures are also relevant to non-metallic components and structures and may be applied with only a moderate amount of contextual interpretation. The principles in this section have been written to reflect aspects of the assessment of non-metallic components and structures in addition to these. In practice, however, EMC.1 to EMC.3 are unlikely to apply as it is very unlikely that a claim at the highest reliability levels could be justified for a non-metallic component or structure.

327. ECS.3 on classification and standards will also be relevant to these assessments, along with Principles EAD.1 to EAD.5 on ageing and degradation. Any limitations on the strength, stiffness, fracture toughness, operating temperature and operating life of non-metallic materials compared with their metallic equivalents will be addressed through application of these principles.

Engineering principles: integrity of non-metallic components and structures	Limitations of application	ENC.1
Where a non-metallic component or structure is chosen in preference to a metallic equivalent, the safety case should identify and then justify any limitations arising from this choice compared to using a metallic item.		

328. Examples of the limitations of non-metallic components or structures are provided in the preceding paragraphs. These may preclude the use of such items either entirely, or in certain locations. For example, if the additional threats from fire hazards cannot be appropriately mitigated then the corrosion resistance benefits of the material would be unlikely to justify its use.

329. The advantages and disadvantages of using a non-metallic component or structure in preference to a metallic one should be weighed so that the choice made is demonstrably in the interests of safety.

Engineering principles: integrity of non-metallic components and structures	Examination through life	ENC.2
The design of non-metallic components or structures should include the ability to examine the item through life for signs of degradation.		

330. Principles EMT.1 to EMT.8 and EMC.27 to EMC.30 provide guidance on in-service examination, inspection and testing in general and for structural integrity aspects in particular. The superior corrosion or chemical resistance of some non-metallic materials may, however, lead to claims that there is no need to provide for

examination (etc) since the material is not expected to degrade through life. Such claims should be subject to a robust demonstration in the safety case that unexpected degradation cannot occur; otherwise suitable provisions for examination (etc) should be made.

Civil engineering

331. *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, and river and coastal defences. Any specific aspects are stated in the appropriate principles. Where a structural component also forms part of containment, the principles in the Containment and ventilation sub-section (paragraph 519 ff.) will also be relevant. When assessing very high integrity metal civil structures, inspectors may similarly need to consider appropriate principles in the sub-section on Integrity of metal components and structures (paragraph 280 ff.).*

332. *Though structural reliability data is becoming more freely available for non-nuclear structures, this is often not directly applicable to the design and construction of nuclear structures. For instance, the data is often not based on comparable analysis methods or design, construction or materials standards. There are thus specific international codes for nuclear structures which describe how to achieve appropriate levels of reliability. These may be supported by good civil engineering practice, appropriate material specifications and good construction practice. The appropriateness of the limit states specified in these codes may need to be considered.*

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

333. The required resilience of civil engineering structures should be quantified and specified.

334. Margins should be such that civil engineering structures will continue to provide their residual safety function(s) following the application of beyond design basis loads by either having sufficient design margins, or by failing in a manner that suitably limits the radiological consequences.

335. Civil engineering structures to be considered should not be limited just to those located on the site, but also off-site structures needed to provide safety functions, eg they are needed to ensure adequate self-sufficiency in a severe accident.

336. The safety functional performance of civil engineering structures required for managing and controlling actions in response to an accident should be defined. These structures include control rooms and on-site and off-site emergency control centres. Consideration should be given to whether they can be affected by the same initiating events as the nuclear facility.

Engineering principles: civil engineering	Independent arguments	ECE.2
For structures requiring the highest levels of reliability, multiple independent and diverse arguments should be provided in the safety case.		

337. The multiple, independent and diverse arguments should provide a robust, multi-layered justification in which weaknesses in individual layers of the argument are offset by strengths in others. Such arguments should include 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 loading schedule covering normal operation, faults (including transients and internal and external hazards) and accidents;

(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) pre-service and in-service inspection to detect defects that have the potential for causing or developing into a failure mode;

(h) for structures for which the consequences of failure would be high, predictable, gradual and detectable failure modes for severe loadings; and

(i) the required resilience of the structures when subject to beyond design basis loadings during severe accidents.

(j) for new structures consideration should be given to the provision of cast-in corrosion monitoring, strain monitoring and similar devices. Coupons and/or dummy components exposed to similar environments (eg buried or exposed to marine salt-laden air) may also be considered to model and predict whole life performance of Civil Engineering SSCs. (See also Principle ECE.20.)

338. For structure types that are inherently less ductile, a sufficiently high margin may be provided by ensuring that failures are extremely unlikely to occur for credible initiating events.

339. For structures that are not of major safety significance, the list of factors in paragraph 337 remains relevant, though the stringency of their application should reflect the safety classification of the item.

Engineering principles: civil engineering	Defects	ECE.3
It should be demonstrated that structures important to safety are sufficiently free of defects so that their safety functions are not compromised, that identified defects can be tolerated, and that the existence of defects that could compromise safety functions can be established through their lifecycle.		

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.		

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

341. Natural site materials (soil and rock) may be used for engineering purposes such as backfill or sea defences. In such cases, the investigations should ensure the materials will be fit for purpose for the safety function required and duration needed.

Engineering principles: civil engineering: investigations	Geotechnical investigation	ECE.5
The design of foundations and sub-surface structures should utilise information derived from geotechnical site investigation.		

342. The information should include groundwater 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. Chemical analysis should be carried out to determine whether foundations may be subject to chemical attack. The descriptions and geotechnical properties of the soils and rocks in or on which a structure is founded or located should be investigated during construction.

343. Sufficient investigations and tests should be carried out to enable the behaviour of the foundations and sub-surface structures under extreme loading, and beyond design basis fault conditions, to be evaluated.

Design

Engineering principles: civil engineering: design	Loadings	ECE.6
Load development and a schedule of load combinations, together with their frequencies, should be used as the basis for structural design. Loadings during normal operating, testing, design basis fault and accident conditions should be included.		

344. To preclude cliff edge effects, margins to failure should extend beyond design basis fault (or hazard) loadings by an amount consistent with assumptions in the severe

accident analysis. Beyond design basis loading considerations should be included before the structural design is finalised. Special attention should be paid when assessing existing structures not designed in accordance with current standards or codes.

345. Where the safety function of a structure provides a principal role in ensuring nuclear safety (see paragraph 148ff), predicted failure modes should be gradual, ductile and, for slowly developing loads, detectable. The loadings assumed should take account of uncertainty in the underlying fault or hazard specification.

346. The data from the devices and measurements referred to in Principle ECE.20 and paragraph 359 should be used during periodic reviews of the safety case or in post-event analysis for civil structures.

Engineering principles: civil engineering: design	Foundations	ECE.7
The foundations and sub-surface structures should be designed to meet their safety functional requirements specified for normal operation and fault conditions with an absence of cliff edge effects beyond the design basis.		

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

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

348. If elements cannot be inspected, the safety case should demonstrate with 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 the facility should not jeopardise the safety of the facility.		

349. Consideration should be given to the overall resilience to flooding, applying appropriate safety classification to the structures, employing suitable redundancy and diversity and avoiding single barriers where possible. See also Principle EHA.12.

350. Where practicable, the design of sea defences should make provision for future modification in response to developments in climate change predictions and other uncertainties.

Engineering principles: civil engineering: design	Groundwater	ECE.10
The design should be such that the facility remains stable against possible changes in the groundwater conditions.		

351. The design should account for known and reasonably foreseeable groundwater conditions. Suitable margins should be incorporated and ensured by monitoring against identified limits and conditions (operating rules). Potential uncertainties due to climate change should be considered.

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

Engineering principles: civil engineering: design	Provision for construction	ECE.25
Items important to safety should be designed so that they can be manufactured, constructed, assembled, installed and erected in accordance with established processes that ensure the achievement of the design specifications and the required level of safety. The effects of construction hazards on any nearby safety related SSCs should be taken into account.		

352. In the provision for construction (and operation), due account should be taken of any relevant experience from the construction of similar facilities, including international experience. Where relevant good practice from other relevant industries is adopted, such practices should be shown to be appropriate to the specific nuclear application. (See also Principle ECE.17.)

Engineering principles: civil engineering: design	Provision for decommissioning	ECE.26
Special consideration should be given at the design stage to the incorporation of features to facilitate radioactive waste management and the future decommissioning and dismantling of the facility.		

Structural analysis and model testing

Engineering principles: civil engineering: structural analysis and model testing	Structural analysis and model testing	ECE.12
Structural analysis and/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 full range of loading for the lifetime of the facility.		

353. The analysis and/or model testing should use methods and data that have been appropriately validated and verified (see paragraph 678 ff.).

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

354. Uncertainties associated with assumed loadings, structural analysis methods, structural capacity and the properties of material potentially affected by degradation 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 and the data verified.		

355. The approach to validation and verification should consider whether the controlling physical equations have been correctly implemented into computer code, databases or spreadsheets or, in the case of hand calculations, correctly incorporated into the calculational procedures. The safety management arrangements should ensure that calculations are validated to an extent proportionate to their importance to the safety case. See also paragraph 678 ff.

356. Calculations of beyond design basis conditions often involve the prediction of extreme physical behaviour and the calculational methods used are consequently 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. See also paragraphs 669, 670 and 671.

Construction

Engineering principles: civil engineering: construction	Materials	ECE.16
The construction materials used should comply with the design methodologies employed, and be shown to be suitable for enabling the design to be constructed and then 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 a quality management system to minimise 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 and testing during construction to demonstrate that appropriate standards of workmanship etc have been achieved.		

Engineering principles: civil engineering: construction	Non-conformities	ECE.19
Where construction non-conformities or identified defects are judged to have a significant detrimental effect on integrity, remedial measures should be applied to ensure the original design intent is still achieved.		

357. Issues relating to the acceptability of the work or the need for remedial measures should be managed through a construction concession in accordance with safety and quality management procedures, and through a formal design change. The safety case should demonstrate that risks remain as low as reasonably practicable in the light of any construction problems.

358. Due account should be taken of the potential for an aggregation of concessions or design changes to undermine the original design intent.

In-service inspection, testing and monitoring

Engineering principles: civil engineering: in-service inspection and testing	Inspection, testing and monitoring	ECE.20
Provision should be made for inspection, testing and monitoring during normal operations aimed at demonstrating that the structure continues to meet its safety functional requirements. Due account should be taken of the periodicity of the activities.		

359. Where changes in parameters assumed in the safety case (such as the severity of seismic loading, groundwater levels, differential settlement or pre-stressing tendon loads) could affect the capability of a structure to meet its safety functional requirements, arrangements should be provided to monitor these. These arrangements should also provide for ageing phenomena (see Principles EAD.3 and EAD.4). The arrangements should identify action levels and include procedures for the collection, analysis and recording of relevant information.

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.		

360. Consideration should also be given to carrying out leak rate testing, eg when commissioning or as part of periodic inspections of containment buildings.

361. Other structural components, such as piles and rock anchors, should be proof tested proportionate to the safety consequences of their failure or in accordance with 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 for leak tightness prior to operation.		

362. Where appropriate, drainage systems should be provided and used to confirm continuing containment integrity, 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.		

363. These inspections 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. See also Principle EHA.12. These inspections may have to extend beyond the site boundary.

Engineering principles: civil engineering: in-service inspection and testing	Settlement	ECE.24
There should be arrangements to monitor civil engineering structures during and after construction to check the validity of predictions of performance made during the design and for feedback into design reviews.		

364. The arrangements should include monitoring for/of:

(a) settlement;

(b) deformations of the ground due to the structure;

(c) values of actions (ie applied loads);

(d) values of contact pressure between the ground and the structure;

(e) pore-water pressures; and

(f) forces and displacements (vertical or horizontal movements, rotations or distortions) in structural members.

Graphite reactor cores

365. *Due to differences in design and safety functions, graphite reactor cores may in some instances be defect tolerant, while in others, safety functions may exhibit low defect tolerance. Therefore the application of these principles needs to cater for a spectrum of safety performance.*

366. *Safety cases for reactor cores usually need to adopt a multi-legged approach, based on independent and diverse arguments. The rigour of application and robustness of the supporting data and information should be based upon the classification of the graphite components and structures. The multi-legged arguments, with the various elements of established engineering practice, should provide defence in depth.*

367. Novel approaches may be acceptable provided they are supported by appropriate research and development, are tested before coming into service to demonstrate the delivery of safety functions and are then monitored during service.

Engineering principles: graphite reactor cores	Safety cases	EGR.1
The safety case should demonstrate that either: (a) the graphite reactor core is free of defects that could impair its safety functions; or (b) the safety functions of the graphite reactor core are tolerant of those defects that might be present.		

368. The safety case should:

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

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

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

369. To meet Principle EGR.1, the safety case should include the following aspects, normally as part of a multi-legged argument:

(a) design;

(b) manufacture, construction and commissioning;

(c) component and core condition assessment (CCCA);

(d) defect tolerance assessment;

(e) analysis of radiological consequences of defectiveness;

(f) monitoring; and

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

370. Principles expanding on paragraph 369 are presented below; these should be applied having due regard for the importance of graphite aspects to the wider safety case.

371. Where known or reasonably foreseeable graphite defects might prejudice delivery of a safety function, the safety case should substantiate how the function will be delivered and identify the demands this places on graphite integrity. The substantiation should be proportionate to the function's safety category (see paragraph 160), but may result in a lower safety function category being assigned for the graphite component or structure. For example, a Category A safety function to control reactivity might lead to lower category safety functions being assigned for graphite components if there are multiple, independent and robust means to control the reactivity and these do not rely significantly on the integrity of the graphite to deliver their safety functions.

372. A defect in a graphite component is a deviation from the design specification. However, not all defects pose a threat to safety.

General

373. *Principles EMC.3 (paragraph 294f), EMC.4 (paragraph 301f), EMC.21 (paragraph 309 f.), EMC.32 to EMC.34 (paragraph 313ff) and Principles EDR.1 (paragraph 181f), EAD.1 to EAD.4 (paragraph 212 ff.), EKP.1 (paragraph 144f), and ECS.2 to ECS.5 (paragraph 163ff) are relevant to graphite reactor cores and should be considered in assessments.*

374. *A general assumption throughout is that analytical models will have used methods that have been verified and validated. This applies equally well to both component condition assessment and defect tolerance assessment. Principles AV.1 to AV.8 provide general principles for assessing the verification and validation of models and their data.*

Design

375. *Principles EMC.7 and EMC.8 (paragraph 304ff) are relevant to graphite reactor cores and should be considered.*

Engineering principles: graphite reactor cores: design	Demonstration of tolerance	EGR.2
The design should demonstrate tolerance of graphite reactor core safety functions to: (a) ageing processes; (b) the schedule of design loadings (including combinations of loadings); and (c) potential mechanisms of formation of, and defects caused by, design specification loadings.		

376. The schedule of design loadings should include normal operation, fault and accident conditions, including plant transients and tests, and internal and external hazards.

Engineering principles: graphite reactor cores: design	Monitoring	EGR.3
There should be appropriate monitoring systems to confirm the graphite structures are within their safe operating envelope (operating rules) and will remain so for the duration of the life of the facility.		

Engineering principles: graphite reactor cores: 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

377. *Principles EMC.13 to EMC.20 (paragraph 306ff) are relevant to graphite reactor cores and should be considered.*

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

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

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

Component and core condition assessment (CCCA)

379. *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 determine whether the cores will continue to perform their safety functions. The CCCA leg of a safety case should present the results of analyses to predict the condition of components and structures.*

Engineering principles: graphite reactor cores: component and core condition assessment	Materials properties	EGR.7
Analytical models should be developed to enable the prediction of graphite reactor core material properties, displacements, stresses, loads and condition.		

380. 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 effects 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.

381. For graphite reactor core components or structures that cannot be qualified directly under the most onerous conditions, additional analysis should carried out which utilises available test results and justifies the item's performance and reliability. Reference data should be taken from commissioning, model, rig or experimental tests for use in such analyses.

Engineering principles: graphite reactor cores: component and core 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 reactor cores: component and core condition assessment	Materials property 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.		

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

Defect tolerance assessment

Engineering principles: graphite reactor cores: defect tolerance assessment	Effect of defects	EGR.10
An assessment of the effects of defects in graphite reactor cores should be undertaken to establish the tolerance of their safety functions during normal operation, faults and accidents. The assessment should include plant transients and tests, together with internal and external hazards.		

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

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

Engineering principles: graphite reactor cores: defect tolerance assessment	Safe working life	EGR.11
The safe working life of graphite reactor cores should be evaluated.		

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

386. Graphite weight loss and reductions in graphite density affect the neutron moderation properties of the core. In particular, they make reactor core behaviour more sensitive during steam ingress faults and erode margins for shutdown and post-shutdown reactivity control. These effects should be analysed and taken into account in the safety case.

Engineering principles: graphite reactor cores: defect tolerance assessment	Operational limits	EGR.12
Operational limits (operating rules) should be established on the degree of graphite brick ageing, including the amounts of cracking, dimensional change and weight loss. To take account of uncertainties in measurement and analysis, there should be an adequate margin between these operational limits and the maximum tolerable amount of any calculated brick ageing.		

387. 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 reactor cores: 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

388. *Principles EMC.24 and EMC.26 (paragraph 311ff) are relevant to monitoring of the safety functions of graphite reactor cores and should be considered.*

Engineering principles: graphite reactor cores: monitoring	Monitoring systems	EGR.14
The design, manufacture, operation, maintenance, inspection and testing of monitoring systems should be commensurate with the duties and reliabilities claimed in the safety case.		

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

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

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

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

Examination, inspection, surveillance, sampling and testing

393. *Principles EMC.25 to EMC.30 (paragraph 311ff) and EMT.1 to EMT.8 (paragraph 201ff) are also relevant and should be considered.*

Engineering principles: graphite reactor cores: 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 confidence that degradation of graphite reactor cores will be detected well in advance of any defects affecting a safety function.		

394. 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 control and instrumentation

395. *Nuclear facilities use a variety of systems to achieve appropriate levels of 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 to maintain safe conditions;

(b) safety actuation systems, such as heat removal systems and reactor shutdown systems, that are brought in to assure the preservation of safe conditions at the facility; and

(c) systems providing essential services to items within the scope of a) or b), such as electrical power, pneumatic/hydraulic pressure, cooling or lubrication.

396. *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.*

397. *Further principles relevant to this section may be found in the general engineering sub-sections starting at paragraph 158 and the Essential services section (paragraph 436 ff.).*

Safety systems

Engineering principles: safety systems	Provision of 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 stable, safe state.		

398. Power reactors should be provided with safety systems to shut them down safely in normal operating and fault conditions and then maintain them in a 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	Safety system specification	ESS.2
The extent of safety system provisions, their functions, levels of protection necessary to achieve defence in depth and reliability requirements should be specified.		

399. The design basis (Principles FA.4 (paragraph 626 ff.) and FA.9 (paragraph 641 ff.)) and probabilistic safety (Principle FA.14 (paragraph 660 ff.)) 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 facility state in relation to safety and to enable the taking of any necessary safety actions during normal operational, fault, accident and severe accident conditions.		

400. 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 on the site (preferably a single location for a reactor) that will remain habitable during foreseeable facility or site emergencies.

Engineering principles: safety systems	Adequacy of initiating variables	ESS.4
The variables used to initiate a safety system action should be identified and shown to be suitable and sufficient for the system to achieve its safety function(s).		

401. The limiting values of these variables, up to which the safety system has been qualified, should be specified (operating rules). The safety system should be designed to respond so that these limiting values are not transgressed in any fault or accident condition where it provides a safety function.

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

402. For example, if the action is to initiate a coolant flow then the flow should be measured directly and not inferred from measurements 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 condition, the variable chosen should have a known relationship with the fault condition.		

403. Any mechanism that might give rise to the fault condition being misdiagnosed or remaining undetected should be analysed and appropriate corrective measures adopted.

Engineering principles: safety systems	Diversity in the detection of fault sequences	ESS.7
All Class 1 protection systems should employ diversity in their detection of and response to fault conditions, preferably by the use of different variables.		

Engineering principles: safety systems	Automatic initiation	ESS.8
For all fast acting faults (typically less than 30 minutes) safety systems should be initiated automatically and no human intervention should then be necessary to deliver the safety function(s).		

404. The design should be such that the operators or other facility personnel cannot negate a correct safety system action, but can initiate safety system functions and perform the necessary actions to deal with circumstances that might prejudice safety. See also EHF principles, and in particular Principles EHF.1 to EHF.5.

Engineering principles: safety systems	Time for human intervention	ESS.9
Where human intervention is needed to support a safety system following the start of a requirement for protective action, then the timescales over which the safety system will need to operate unaided should be demonstrated to be sufficient.		

405. In keeping with internationally accepted relevant good practice for power reactors, no human intervention should be necessary for approximately 30 minutes from the start of the safety system initiation.

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 and substantiated.		

406. The capability should exceed that necessary for the effective delivery of the safety functions in the prevailing operating environment (eg in fault or accident conditions) by a clear margin (see also Principle EQU.1). The selected margins should make due allowance not only for uncertainties in plant characteristics, but also for the effects of foreseeable degradation mechanisms (see Principle EAD.2).

Engineering principles: safety systems	Demonstration of adequacy	ESS.11
The adequacy of the system design to achieve its specified functions and reliabilities should be demonstrated for each safety system.		

407. A fault schedule (sometimes known as a safety schedule or a fault and protection schedule) should be provided to link faults, fault sequences and safety measures (see Principle FA.8). For each initiating fault or event, the schedule should identify the relevant initiating fault frequencies, the potential fault consequences, the safety systems and administrative safety measures that provide protection, any beneficial safety-related systems, the mitigated fault sequence frequency and the overall protection claim. The fault schedule should also identify any passive safety measures claimed to prevent faults or mitigate their consequences.

Engineering principles: safety systems	Prevention of service infringement	ESS.12
Adequate arrangements should be in place to prevent any infringement of the services supporting a safety system, its sub-systems or components.		

408. Infringement of a service includes the removal or degradation of support services such as power supplies, pneumatic/hydraulic pressure or instrument air, or adverse changes to the item’s operating environment.

409. Where prevention, or an acceptably low likelihood of infringement, cannot be demonstrated, features should be incorporated to ensure a failsafe outcome.

Engineering principles: safety systems	Confirmation to operating personnel	ESS.13
There should be direct means of confirming to operating personnel: (a) that a demand for safety system action has arisen; (b) that the safety systems have operated (actuated) fully and correctly; and (c) whether any limiting condition (operating rule) has been exceeded which takes the safety system beyond its substantiated capability (see Principle ESS.10).		

410. Such means should be clear and preferably sourced from the system carrying out the action (see also Principle EHF.7).

Engineering principles: safety systems	Self-resetting of safety systems	ESS.14
Safety system actions and associated alarms should not be self-resetting, irrespective of the subsequent status 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) can be altered, other than by specifically engineered and adequately secured maintenance/testing provisions used under strict administrative control.		

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

411. For this principle an external source of energy means external to the safety system (see also paragraphs 168, 413 and 436 ff.).

Engineering principles: safety systems	Faults originating from safety systems	ESS.17
Potential faults originating from within safety systems (eg due to spurious or mal-operation) should be identified and protection against them provided.		

412. This principle is aimed at ensuring that the facility remains safe following foreseeable safety system faults. The protection provided might, for instance, include designing the safety system so that it will enter a failsafe state upon detection of a fault. See also Principle ESS.22.

Engineering principles: safety systems	Failure independence	ESS.18
No design basis event should disable a safety system.		

413. 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 (see also paragraph 167).

Engineering principles: safety systems	Dedication to a single task	ESS.19
A safety system should be dedicated solely to the provision of its allocated safety functions.		

414. Where more than one safety function is to be delivered by a safety system, the whole system should be classified in accordance with the guidance in paragraph 166, with interfaces managed as per paragraph 167 (see also paragraph 172).

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

415. Where external connections to electrical, electronic or computer-based safety systems cannot be avoided, they should be restricted in function to unidirectional links, and should incorporate adequate isolation features so that faults cannot propagate and then jeopardise the functions of the safety system.

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

416. Where this cannot be achieved, eg because of the use of complex hardware, the reliability of the safety system should be demonstrated. The safety case 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; and

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

417. The nature of some safety systems means that faults cannot easily be detected (revealed) at the time of their occurrence, eg in the case of fluid or mechanical systems. In such cases, the safety case should specify the in-service or periodic testing needed to support the reliability claims of the equipment (see Principle EMT.6).

Engineering principles: safety systems	Avoidance of spurious actuation	ESS.22
Spurious actuation of safety systems should be avoided by means such as the provision of multiple independent divisions within the design architecture and majority voting.		

418. For a complex Class 1 safety system (eg one which is computer-based), every spurious actuation brought about by common cause failure of system components should be analysed as a design basis fault (see paragraphs 166 and 626 ff.). The fault analysis should assume that the common cause failure also disables all other safety functions provided by the system, but may assume that such disabling does not further exacerbate the fault.

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

419. The safety case should identify the permitted combinations of equipment unavailability for each permitted operating state (operating rules), applying design basis analysis (see paragraph 631) and probabilistic safety analysis (see paragraph 653). Reasons for equipment unavailability considered in the safety case should include:

(a) the need for testing and maintenance;

(b) catering for non-repairable equipment failures; and

(c) the potential for and likelihood of unrevealed failures (see paragraph 417).

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

420. Where such action cannot be avoided, the safety case should justify that there will be sufficient control of the hazard at all times (see Principle NT.2). Where a safety system comprises several redundant or diverse sub-systems, only one sub-system should be permitted to be out of service or vetoed at any one time.

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

Engineering principles: safety systems	Computer-based safety systems	ESS.27
Where the system reliability is significantly dependent upon the performance of computer software, compliance with appropriate standards and practices throughout the software development lifecycle should be established in order to provide assurance of the final design.		

421. The complexity of computer-based safety systems means they are usually not amenable to traditional methods of reliability assessment. This principle therefore provides for elements of a procedure to demonstrate the adequacy of such systems. The safety demonstration for hardware elements of these systems should include the items listed in paragraph 416.

422. The rigour of the standards and practices applied should be commensurate with the level of reliability required. The standards and practices should demonstrate 'production excellence' and, through the application of 'confidence-building' measures, provide proportionate confidence in the final design.

423. 'Production excellence' is a demonstration of excellence in all aspects of production from the initial specification through to the finally commissioned system. It should include 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 a modern standards quality management system; and

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

(i) prior to installation on site, the verification of all phases of the system production process and the validation of the integrated system against its specification by persons not involved in the specification and design activities;

(ii) following installation on site, a demonstration that the safety system, in conjunction with the plant, performs in accordance with its specification. This demonstration should be devised by persons not involved in the system's specification, design or manufacture; and

(iii) a programme of dynamic testing, applied to the complete system to demonstrate that the system is functioning as intended.

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

(a) complete, and preferably diverse, checking of the finally validated production software by a team that is independent of the system's suppliers, including:

(i) independent product checking that provides a searching analysis of the final system;

(ii) independent checking of the design and production processes, including the activities undertaken to confirm the realisation of the design intent; and

(b) independent assessment of the comprehensive testing programme covering the full scope of the test activities.

425. When demonstrating 'production excellence' and applying 'confidence-building' measures for computer-based safety systems:

- verification is the process of ensuring that a phase in the system lifecycle meets the requirements imposed on it by the previous phase; and
- validation is the process of testing and evaluation of the integrated computer system (hardware and software) to ensure compliance with functional, performance and interface requirements.

426. Statistical testing is highly recommended as an approach for demonstrating the numerical reliability of computer-based safety systems. Such testing may play a role in both 'production excellence' and 'confidence-building' aspects of the safety justification.

427. If weaknesses are identified in the production process, compensating measures should be applied to address these. The choice of compensating measures and their effectiveness should be justified in the safety case.

Control and instrumentation of safety-related systems

428. *Safety-related systems are distinct from safety systems (see previous section) in that, while they often have a significant influence on safety, they do not provide the primary means of protection for fault sequences. In a control and instrumentation context, safety-related systems include facility control systems, indicating and recording instrumentation, alarm systems and communications 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 secondary control or monitoring locations.		

429. Principle EHF.7 on user interfaces is also relevant to this principle.

430. The systems should provide for control, monitoring and data recording in normal operations, fault conditions and severe accidents. The extent of these provisions should be consistent with the fault analysis and justified in the safety case. See also paragraph 778.

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 it to deliver its safety functions.		

Engineering principles: control and instrumentation of safety-related systems	Provision of controls	ESR.3
Adequate and reliable controls should be provided to maintain all safety-related plant parameters within their specified ranges (operating rules).		

Engineering principles: control and instrumentation of safety-related systems	Minimum operational equipment	ESR.4
The minimum control and instrumentation in each of the facility's permitted operating modes should be specified (operating rules) and its adequacy substantiated.		

Engineering principles: control and instrumentation of safety-related systems	Standards for equipment in safety-related systems	ESR.5
Where computers, programmable or non-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.		

431. For modern complex control systems, the avoidance of spurious operation cannot be guaranteed. Therefore major, spuriously initiated failures of control systems should be analysed as initiating faults in the fault analysis (see Principles FA.2 and ESR.10).

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 safety functions being performed.		

432. In the case of monitoring, warning and communication functions, these supplies should be uninterruptible and independent of other safety-related systems.

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 on and, where necessary, off the site. The systems should provide robust means of communication during normal operations, fault conditions and severe accidents.		

433. The safety functions to be delivered by these systems should be analysed and justified in the safety case and be consistent with the site's emergency preparedness and accident response arrangements (see Principle AM.1).

434. The communication systems should be designed to not have any adverse effect on safety systems, or other safety-related systems.

Engineering principles: control and instrumentation of safety-related systems	Monitoring of radioactive material	ESR.8
Instrumentation should be provided to detect the leak or escape of radioactive material from its designated location and then to monitor its location and quantity.		

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, reliable 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 safety systems or take any safety system beyond its capability limits.		

435. An analysis should be provided that identifies the foreseeable ways in which control system faults, including multiple spurious faults or failures on demand, could generate a demand on a safety system (see also Principles ESS.4, ESS.10 and ESS.11).

Essential services

436. *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 an uninterruptible 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 this service until normal supplies can be restored.*

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 in fault and accident conditions.		

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

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

437. The source should provide the service for a sufficient period of time to allow the facility to be brought to a stable, safe state and then maintained in that state until such time as the normal supply is restored. See also paragraph 782.

438. Where the source, or elements of the source, are located on the site, its safety classification should be assigned in accordance with paragraph 168 (ie be based in the first instance on the classification of the systems or equipment it supports).

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

439. It should be shown that the safety functions of all the facilities will be delivered in all permitted operating modes (including during maintenance) and for fault and accident conditions (see also paragraph 134).

Engineering principles: essential services	Cross-connections to other services	EES.5
The ability of the essential services to meet the demands of the safety function(s) they support should not be undermined by making cross-connections to services provided for safety functions of a lower category (see paragraph 160).		

440. Where such cross-connections are necessary, provision should be made to isolate the essential service from these other services (see also paragraph 135).

Engineering principles: essential services	Reliability of back-up sources	EES.6
Back-up sources of essential services should be designed so that their reliability will not be prejudiced by adverse conditions in the services to which they provide a back-up, eg from common cause failures.		

Engineering principles: essential services	Protection devices	EES.7
The protection devices provided for essential service components or systems should be consistent with the safe operation of the facility and limited to those justified as necessary in the safety case.		

441. The overall provision of protection devices and their potential effects on the facility and its safety systems should be analysed and justified.

Engineering principles: essential services	Simultaneous 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.		

442. The safety case should analyse such loss of service events and demonstrate the continuing safety of the facility. Elements of the demonstration should include, where appropriate:

(a) justifying how further back-ups will be brought into service to meet the safety demand;

(b) showing there would be sufficient time available to restore the service before unacceptable consequences could arise;

(c) demonstrating the likelihood and consequences of the event mean that it is not reasonably practicable to add further back-up provisions to the design; and

(d) where the potential consequences merit this, employing severe accident analysis to show that the site's emergency arrangements would be sufficient to manage the event (see paragraphs 663 ff. and paragraph 768 ff.).

Human factors

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

Engineering principles: human factors	Integration within design, assessment and management	EHF.1
A systematic approach to integrating human factors within the design, assessment and management of systems and processes should be applied throughout the facility's lifecycle.		

444. Whilst human factors integration is expected throughout all design phases, for new designs, the majority of the human factors analysis should be undertaken during the Pre-Construction Safety Report (PCSR) stage in order to influence the design and inform the safety analysis. As the design progresses, human factors analysis should start to focus on verification of the human factors claims in the safety case.

Engineering principles: human factors	Allocation of safety actions	EHF.2
When designing systems, dependence on human action to maintain and recover a stable, safe state should be minimised. The allocation of safety actions between humans and engineered structures, systems or components should be substantiated.		

445. This allocation should consider the monitoring of automatic functions and the potential need to assume manual control in the event of the failure of an automatic system.

446. Where administrative safety measures are identified to deliver safety functions (see Principle EKP.5) the guidance in paragraphs 155 and 156 should be followed. Principles ESS.8 and ESS.9 on safety system initiation are also relevant here.

Engineering principles: human factors	Identification of actions impacting safety	EHF.3
A systematic approach should be taken to identify human actions that can impact safety for all permitted operating modes and all fault and accident conditions identified in the safety case, including severe accidents.		

447. This principle includes identifying all the safety actions of personnel responsible for monitoring and controlling the facility and of personnel carrying out maintenance, testing and calibration activities. It also includes consideration of the impact on safety arising from engineers, analysts, managers, directors and other personnel who may not interact directly with plant or equipment.

Engineering principles: human factors	Identification of administrative controls	EHF.4
Administrative controls needed to keep the facility within its operating rules for normal operation or return the facility back to normal operations should be systematically identified.		

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

Engineering principles: human factors	Task analysis	EHF.5
Proportionate analysis should be carried out of all tasks important to safety and used to justify the effective delivery of the safety functions to which they contribute.		

449. This analysis should be applied to all actions and controls identified under Principles EHF.3 and EHF.4 so that the safety case demonstrates high confidence in the feasibility of completing these tasks within requisite timescales. In so doing, the analysis should inform the way tasks are designed and supported to achieve reliable and effective task performance.

450. The analysis should evaluate the demands these tasks place upon personnel in terms of perception, decision making and action. It should also take into account the physical and psychological factors that could impact on human performance.

451. The analysis should be sufficiently detailed to provide a basis for developing user interfaces, procedures and job aids, as well as helping define operator roles and responsibilities, staffing levels, personnel competence and training needs, communication networks and workspace design. Further principles related to these topics are provided below.

452. The workload of personnel required to undertake these actions and controls should be analysed and demonstrated to be reasonably achievable. Where practicable, this demonstration should form part of the inactive commissioning of the facility. The workload of personnel and its impact on the effective completion of tasks important to safety should be reviewed in periodic safety reviews and as part of emergency demonstration exercises.

Engineering principles: human factors	Workspace design	EHF.6
Workspaces in which operations (including maintenance activities) are conducted should be designed to support reliable task performance. The design should take account of the physical and psychological characteristics of the intended users and the impact of environmental factors.		

Engineering principles: human factors	User interfaces	EHF.7
Suitable and sufficient user interfaces should be provided at appropriate locations to provide effective monitoring and control of the facility in normal operations, faults and accident conditions.		

453. Appropriate locations include central control rooms, local plant control stations, locations where maintenance and/or testing is carried out and locations identified for monitoring or control within the facility's emergency preparedness and response arrangements (eg site emergency control centres (see paragraph 783)).

454. User interfaces, which may be analogue or digital, include controls, indications, alarms, recording instruments, overview displays, mimics, communication equipment, computer-based procedures, computerised operator support systems, intelligent decision aids and reconfigurable displays and controls.

Plant equipment such as valves, emergency supply connection points and similar plant and equipment are also considered to be user interfaces.

455. User interfaces should be designed to ensure compatibility with the psychological and physical characteristics of the intended users and to facilitate reliable human performance. Interfaces and equipment should be clearly labelled.

456. User interfaces should:

(a) provide sufficient, unambiguous information for the operator to maintain situational awareness in all operating modes and in fault and accident

conditions (eg the behaviour and status of the automated plant control systems);

(b) provide a conspicuous early warning of any changes in parameters affecting safety;

(c) provide a means of signalling safety system challenges and of confirming that the safety system has initiated and achieved its safety functions;

(d) support effective diagnosis of plant deviations;

(e) enable the operator to determine and execute appropriate actions including those needed to overcome failures of automated safety systems or to reset a safety system after its operation; and

(f) support communication between personnel located in the same or different operating locations, including locations external to the facility or site.

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

457. 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 training programme evaluation. The process should be applied to all whose actions could impact on safety, whether they are an employee or a contractor, including personnel who may not interact directly with plant or equipment (see paragraph 447). Close 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.		

458. Procedures should be accurate and designed and presented so that they:

(a) meet the needs of all intended users; and

(b) facilitate the safe and effective completion of tasks important to safety.

459. Procedures should be controlled, subject to approval and reviewed and revised periodically to ensure their continuing adequacy and effectiveness.

460. Procedures relating to fault and accident conditions should be designed recognising the potential physical and psychological state of the operators and the possibility of degraded plant conditions, particularly for severe accidents.

461. The design of procedures should provide for reliable navigation within the document and support transition between procedures of the same and different types, eg between alarm response procedures and emergency operating procedures.

Engineering principles: human factors	Staffing levels	EHF.11
There should be sufficient competent personnel available to operate the facility in all operational states.		

462. Task analysis completed under Principle EHF.5 should provide the basis for establishing required staffing levels, both for normal operation, fault and accident conditions. Further guidance on staffing levels in accident conditions is provided in paragraph 786.

Engineering principles: human factors	Fitness for duty	EHF.12
A management process should be in place to ensure the fitness for duty of personnel to perform all safety actions identified in the safety case.		

463. Safety actions should be identified as per Principle EHF.3. Management controls should then be established to control fatigue arising from shift patterns and hours worked.

464. Management controls should also be established to identify and manage the effects of wider factors impacting fitness for duty, including occupational stress, and drug and alcohol use.

Engineering principles: human factors	Human reliability	EHF.10
Human reliability analysis should identify and analyse all human actions and administrative controls that are necessary for safety.		

465. The analysis should be conducted as part of design basis analysis (DBA), probabilistic safety analysis (PSA) and severe accident analysis (SAA) aspects of the safety case (see Fault analysis, paragraph 605 ff.). Proportionate analysis should be undertaken to support the claims and arguments made in regard to these actions and administrative controls.

466. The human reliability analysis should include: pre-fault human actions during maintenance, calibration or testing activities where error could result in the non-availability of equipment or systems important to safety; actions that contribute to initiating events; post-fault human actions; and long-term recovery actions in severe accidents.

467. The selection and application of probabilistic data for human errors should:

(a) be derived from operational experience data and/or through the application of recognised human reliability assessment techniques. The approach adopted should be justified in terms of its relevance to the task and context;

(b) be underpinned by task analysis (see Principle EHF.5), taking into account the range of factors that might influence the performance of operators; and

(c) be on a best-estimate basis, properly justified and make due allowance for uncertainties.

468. Contingent operator actions and dependent human errors committed by single or multiple operators should be modelled explicitly in the human reliability analysis and accounted for quantitatively. The analysis should also account for indirect dependence and avoid unrealistically low single or combined human error probabilities being propagated through the fault analysis.

Control of nuclear matter

469. *The term 'nuclear matter' should be interpreted as defined in the glossary. The principles in this sub-section apply to all types of nuclear matter unless the wording makes it clear that limited application is intended, or unless the total amount of nuclear matter concerned is sufficiently small or is in such a chemical or physical form as to make application of the principles disproportionate. However, when nuclear matter has been designated as radioactive waste, the principles in the section on Radioactive waste management (paragraph 788 ff.) also apply. Many of the more specific principles in other sub-sections are also relevant, eg Containment and ventilation (paragraph 519 ff.).*

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

470. 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 on the site.		

Note: Licence Condition 4, which addresses restrictions on nuclear matter on the site, is relevant here.

471. Such arrangements should include as appropriate:

(a) handling provisions;

(b) the use of flasks, containers and other packages;

(c) treatment and processing facilities;

(d) designated storage facilities and areas, of appropriate capacity, including spare and buffer capacity where necessary;

(e) disposal facilities; and

(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.		

472. 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.

473. 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.

474. Temporary re-routing of nuclear matter (eg for sampling purposes) should only be undertaken where necessary and suitably justified. Once the need for temporary re-routing has passed, the facility should be restored promptly to its normal configuration and any nuclear matter that was removed returned to a suitable and designated location.

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.		

475. Nuclear matter should be identified and recorded in an inventory that is kept up to date. The inventory should be consistent with the licensee's arrangements for Licence Conditions 25 and 32 and should include details of:

(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) all nuclear matter stored or accumulated on the site;

(f) appropriate characterisation information (such as that considered in Principle ENM.5 below); and

(g) details of location, containers and packaging.

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

477. 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 leakages and escapes.

478. Containers or packages used for the transport or movement of nuclear matter on site, or within a facility, should be appropriately designated and marked or labelled as such.

479. The unauthorised access to, or removal of, nuclear matter should be prevented.

480. 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 also applies.

481. Records should be maintained in a secure and accessible form, for the appropriate period of time and in accordance with the licensee's arrangements for Licence Conditions 6, 25 and 32.

Engineering principles: control of nuclear matter	Characterisation and segregation	ENM.5
Nuclear matter should be characterised and segregated whenever practicable to facilitate its safe management.		

482. 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.

483. Sufficient representative information should be obtained from characterisation of nuclear matter to support ongoing and future materials management activities.

484. Provision should be made for identifying, assessing and dealing with nuclear matter that does not meet existing process specifications.

485. Nuclear matter should be segregated from incompatible materials where mixing or contact could adversely affect subsequent steps in its management.

486. Where it is proposed to mix different types of nuclear matter, such mixing should be justified in the safety case.

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 whenever practicable and in accordance with good engineering practice.		

487. Principle RW.5, which is concerned with the passive safe storage of radioactive waste, should also be applied to nuclear matter, but 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.		

488. The design of facilities and their 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 474); and

(c) take account of the anticipated storage duration and any changes in the characteristics of the nuclear matter, its containment or its storage environment 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.		

489. Engineering and operational controls should provide the main lines of protection against leaks and escapes of radioactive, corrosive or toxic substances and any unintended 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 an accumulation or diversion of nuclear matter, eg due to leaks or blockages.

490. Procedures should be established to implement, verify, approve, monitor, audit and systematically review the accountancy systems and evaluate their effectiveness.

491. The extent and frequency of the accountancy analysis should be defined and justified in the safety case, taking into account the requirements of international safeguards processes.

492. 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.

493. Display systems should be configured to provide an overview of the condition of the process including, where appropriate, mass and volumetric balance summaries.

494. Operators should perform volumetric, mass balance and radioactive concentration checks whenever unusual level or flow imbalances are observed.

Chemical (Process) Engineering

495. Chemical Engineering (commonly known as Process Engineering) links the underpinning science of processes to the engineering that delivers the required plant functionality. Whilst it is primarily focused on fuel cycle facilities there are principles

which can also be applied to ancillary processes on power reactors and to mechanical processing facilities.

496. The nature of fuel cycle facilities is different to power reactors in that the radioactive material is often deliberately placed in a mobile form in order to allow separation and physical changes. As a consequence, one of the major drivers will be to control the energy within the process in order to minimise potential challenges to containment. Another major difference between a fuel cycle facility and a power reactor is that there can often be a greater choice of processes to deliver safe and effective outcomes. This means there will be greater focus on the extent to which the optioneering (eg in the safety case) achieves the underpinning intent of the engineering key principles (EKP).

497. Chemical Engineering is also concerned with designing facilities to achieve appropriate levels of throughput. Whilst clearly an economic matter, throughput can also be a significant safety issue at radioactive waste processing facilities and at facilities being decommissioned, particularly where there are degradation mechanisms for the radioactive contents, the process equipment or the facility structure.

498. Further relevant guidance may be found in the Chemistry principles (paragraphs 508ff) and on the HSE Hazardous Installations Directorate Control of Major Accident Hazards (COMAH) Guidance website.

Engineering principles: Chemical Engineering	Design and operation	EPE.1
The design and operation of nuclear chemical processes and facilities should be fault tolerant and ensure safety functions are delivered with suitable capability and sufficient reliability and robustness.		

499. The process design should be developed in tandem with the safety case to ensure they are mutually consistent. In line with the inherent safety key principles (see Principle EKP.1), operations should aim to be as close to being inherently safe as possible, for example:

(a) Sources of energy within the process should be minimised. For instance, use of reactive chemicals should be minimised; inventories should be the minimum consistent with safe and reliable operation; and processes that function at or below ambient temperatures and pressures, or maximise the time spent under these conditions, should be preferred.

(b) Processes should be tolerant of the widest range of feedstock (in terms of physical, chemical and radiochemical properties) and throughputs justified by the safety case. This should include consideration of bounding levels of decay heat from radioactive decay and the capabilities of the cooling systems, including under fault conditions.

(c) Design documents such as flow sheets should be based on normal expected operating conditions, but also include the most restrictive conditions justified in the safety case, including during fault conditions and foreseen subsequent faults.

(d) Chemical reactions should be controllable and either be endothermic, or have reaction properties that change relatively slowly in terms of equipment

response times. The thermodynamics and kinetics should be analysed for all normal operation and fault conditions identified in the safety case. Side reactions, interactions with adventitious materials and the potential for cliff edge effects should also be considered in the analysis.

(e) The design should tolerate the effects of process degradation or malfunction, eg side reactions, accumulation of by-products, degradation products, and accumulation of solids.

(f) Circumstances leading to significant deviations from the original design intent should be identified and suitably analysed to evaluate their effect on safety. The design intent may need to be revised to account for these.

Engineering principles: Chemical Engineering	Process stability	EPE.2
Nuclear chemical processes should be designed and operated so as to maintain suitable and sufficient stability.		

500. Systematic techniques such as Hazard and Operability studies (HAZOP) should be used to improve operability as well as for fault identification.

501. Safe, stable, reliable and predictable operation should be promoted by:

(a) process choices made according to the degree of confidence in their safety and effectiveness;

(b) design and operation of individual processes that are fully integrated with other processes in the facility, applying suitable interstage buffering. Interstage buffering should be limited to levels sufficient to allow for reasonable downtimes between stages as storage has its own associated risks. Similar considerations should also apply between different facilities on multi-facility sites;

(c) minimising the need within the design for manual interventions into the process or workarounds;

(d) a design which is tolerant of differing plant availabilities. This may also involve interstage buffering (see above);

(e) simplifying plant and equipment design with due regard to the required functionality, eg minimising penetrations, avoiding dead legs, minimising the number of instruments in contact with radioactive materials, and minimising the need for inspection, maintenance and testing;

(f) appropriate consideration of facility start up, shutdown, restart and maintenance; and

(g) minimising or controlling process drift.

Engineering principles: Chemical Engineering	Experimental processes	EPE.3
Where an experimental chemical process is proposed, the safety case should establish an appropriate degree of confidence in the safety of the process and that it will deliver as intended.		

502. Where experiments are used to underpin a new process, these need to be pertinent to the design of the final facility and demonstrate that the underpinning design intent will be maintained over all reasonably foreseeable conditions. Thus the proposals should include the following:

(a) The experiment should show sufficient similarity to the intended design, eg kinetic, thermodynamic, dynamic and geometric similarity. Where this is not possible, then the critical parameters should be modelled in greater detail.

(b) The experiments should simulate all reasonably foreseeable transients with an appropriate degree of realism.

(c) Where it is not possible to conduct full-scale active experiments then an acceptable demonstration may involve full-scale inactive work and/or small-scale active work.

(d) The experiments should provide an input into the definition of the parameters needed to ensure safe and effective operation.

(e) The experiment should simulate possible faults (malfunctions) including those above under Principle EPE.1.

(f) Where experiments show process uncertainties such as instability, the design should make allowance for these or an alternative design should be selected.

503. Experiments on production facilities should be closely controlled (Licence Condition 22). Where these are carried out, there should be no production pressures and the facility should be suitably instrumented to ensure all safety critical aspects are appropriately monitored. All the facility's existing safety measures should continue to deliver their safety functions under the experimental conditions and the need for additional safety measures should be considered explicitly.

Engineering principles: Chemical Engineering	Severe accident data	EPE.4
Process behaviour under severe accident conditions should be analysed.		

504. Although severe accident analysis has traditionally been focused on power reactors, the hazards posed by some fuel cycle facilities mean that these meet the SAPs criteria defining a severe accident (paragraph 664) and so should also be subject to severe accident analysis and then assessed as per Principles FA.15, FA.16 and FA.25. These principles require a good understanding of how the chemical processes and operations would behave under extreme conditions.

505. Process behaviours that could be pertinent to severe accident analysis include cliff edge effects such as column flooding, transition to multi-phase flow or complete loss of utilities and support services. Where the transient is fast, then adiabatic or similar

limiting assumptions should be made. Otherwise, the analysis should adopt a best estimate approach.

506. Where experiments are used to underpin the design, critical parameters such as kinetic, thermodynamic, dynamic and geometric similarity used to model normal operation should be re-examined as their behaviour may change under severe accident conditions.

Engineering principles: Chemical Engineering	Process design and commissioning	EPE.5
The process design and commissioning should provide inputs to operational safety parameters defining limits and conditions necessary in the interests of safety (operating rules).		

507. Limits or conditions necessary for the safe operation of the facility from a chemical engineering perspective should be identified in the safety case. These may include:

(a) the feedstock specification used for the process design specification;

(b) operational limits derived from the design, eg temperatures, pressures and chemical compositions; and

(c) time-dependent conditions or limits based on transient modelling, relevant operational experience or commissioning, eg for the degradation of feedstock, reagents or process materials, the build up of undesirable by-products or energetic reactions.

Chemistry

508. The safety assessment principles described in this sub-section are concerned with how chemistry can affect nuclear safety, radiological protection or radioactive waste management. In the principles that follow, the term 'chemistry' should be interpreted to mean chemical or radiochemical parameters or effects.

509. Chemistry can affect materials, systems and processes and their associated hazards in a variety of ways. For example, it can have an influence on reactivity, radioactivity, radioactive waste and radiation doses to the public and workers, it can influence the performance of structures, systems and components, for example the integrity of vessels and fuel cladding, and it can lead to the generation of undesirable products, such as combustible gases. Adequate control of chemistry therefore needs planning in design, consideration in safety cases, and may demand rigorous controls over certain operations. The effects of chemistry may be important throughout the full lifecycle of the facility, although the effects and their importance will likely vary over time.

510. This section is not intended to be used standalone; chemistry will be important to safety in a range of topical areas and other safety assessment principles will apply. These principles should therefore be read in conjunction with those relating to material degradation (EAD.1 ff.), nuclear matter (paragraph 469 ff.), reactor core (paragraph 539 ff.), heat transport systems (paragraph 558 ff.), radioactive waste management (paragraph 788), and in particular the principles therein relating to characterisation), fault analysis (paragraph 605 ff.), Chemical (Process) Engineering (paragraph 495ff) and internal hazards (paragraph 228ff).

Engineering principles: chemistry	Safety cases	ECH.1
Safety cases should, by applying a systematic process, address all chemistry effects important to safety.		

511. The safety case should identify and analyse how chemistry can impact safety during normal operations and in fault and accident conditions, and demonstrate how the chemistry will be controlled. A systematic approach should be adopted that identifies the limits and conditions (operating rules) that need to be applied in the interests of safety (see Principle SC.6). The derivation of such chemistry-based limits and conditions should account for implicit assumptions made in regard to the performance of chemical processes affecting safety.

512. The analysis should distinguish between chemistry affecting safety and that applied for other reasons, such as asset protection or commercial benefit. It should include a thorough and structured review of all relevant chemical reactions involving the facility's materials and their environment, and the safety consequences of these. The breadth and depth of the analysis should be in proportion to the complexity of the system and its risk and hazard potential.

513. The analysis should include:

(a) reactions between chemicals and other materials within the process, plant or facility, including, for example, corrosion and the production of radionuclides or combustible gases;

(b) the rates, extent, energy released or absorbed, and the timings of chemical reactions;

(c) the products from reactions and how these evolve, including heat generation and phase changes, transport and accumulation; and

(d) the effects of adventitious impurities that might accelerate or alter the reactions.

514. Where generic chemistry is applied, the safety case should demonstrate its relevance to the facility or operations being analysed.

Engineering principles: chemistry	Resolution of conflicting chemical effects	ECH.2
Where the effects of different chemistry parameters conflict with one another, the safety case should demonstrate that an appropriate balance for safety has been achieved.		

515. Changing a particular chemistry parameter to improve safety in one respect may cause a detrimental effect in another. In these cases the safety case should identify the positive and negative impacts of the chosen solution and demonstrate how this reduces risks to as low as reasonably practicable.

Engineering principles: chemistry	Control of chemistry	ECH.3
Suitable and sufficient systems, processes and procedures should be provided to maintain chemistry parameters within the limits and conditions identified in the safety case.		

516. These limits and conditions (operating rules) should cater for:

(a) controls over the quality of feedstock chemicals;

(b) management of the quantities of chemicals held;

(c) optimisation of the frequency and means of chemical additions;

(d) processes to minimise adventitious impurities, exclude foreign materials and maintain material compatibility; and

(e) the provision of processing equipment suitable for the concentrations and quantities expected.

517. Consideration should be given to the safe and effective addition and/or removal of chemicals to/from the system. The safety, effectiveness and reliability of the system to control the chemistry should be demonstrated in all normal operational, fault or accident conditions where the system provides such a safety function. The system design should incorporate appropriate levels of redundancy, diversity and segregation (see Principle EDR.2).

Engineering principles: chemistry	Monitoring, sampling and analysis	ECH.4
Suitable and sufficient systems, processes and procedures should be provided for monitoring, sampling and analysis so that all chemistry parameters important to safety are properly controlled.		

518. Guidance on assessing the characterisation of nuclear matter and radioactive waste may also be relevant here (see Principles ENM.5 and RW.4). The chemistry monitoring, sampling and analysis should:

(a) verify the effectiveness of chemistry control in systems and that structures, systems and components are being operated within specified limits (operating rules). Consideration should be given to providing alarms to assist the chemistry monitoring regime;

(b) be performed according to a clearly defined scope and periodicity;

(c) be applied under appropriate conditions defined to ensure representative sampling is undertaken;

(d) adopt an appropriate balance between on-plant measurements and laboratory analysis; and

(e) utilise appropriate processes and procedures.

Containment and Ventilation

519. *Containment and ventilation systems should confine the radioactive material within the facility and prevent its leakage or 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.*

520. *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.*

521. *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 managed safely.*

522. *Containment and associated nuclear ventilation systems will normally form part of systems important to safety and so the general principles applicable to engineering (paragraph 140 ff.), safety systems (paragraph 398 ff.) and essential services (paragraph 436 ff.) will be relevant. Ventilation systems may, however, be required on parts of a facility that would not be considered as containment, in the sense that these are areas to which access is freely available. Such systems need not necessarily be classed as important to safety.*

523. *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. 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 (EHA.13 ff.).*

Engineering principles: containment and ventilation: containment design	Prevention of leakage	ECV.1
Radioactive material 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
Containment and associated systems should be designed to minimise radioactive releases to the environment in normal operation, fault and accident conditions.		

524. The safety functions of containment and associated systems should be clearly defined for all normal operations, fault and accident conditions identified in the safety case, including for internal and external hazards.

Engineering principles: containment and ventilation: containment design	Means of confinement	ECV.3
The primary means of confining radioactive materials should be through the provision of passive sealed containment systems and intrinsic safety features, in preference to the use of active dynamic systems and components.		

525. Where appropriate, the safety case should:

(a) define the containment boundary and identify means of isolating the boundary;

(b) establish a set of limits and conditions (operating rules) for the containment systems and for individual structures and components within each system;

(c) define the requirements for the performance of the containment during severe accidents, including its structural integrity and stability;

(d) include provision for making the facility safe following any fault or accident involving the release of radioactive material within or from containment, including equipment to allow decontamination and post-event re-entry to be 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 radioactive material escaping via routes installed for other purposes;

(f) justify that, where fire dampers are provided, their position and operation will not compromise either the containment function or the safety functions of the ventilation system;

(g) avoid the use of ducts that need to be sealed by isolating valves under fault conditions. Where isolating valves and devices are provided, their performance should be consistent with the required containment duties and should not prejudice adequate containment performance;

(h) provide for discharge routes, including pressure relief systems, with treatment system(s) to minimise radioactive discharges to acceptable levels. There should be appropriate treatment or containment of radioactive wastes generated by such systems. Should the pressure relief system operate, the performance of the containment should not be degraded;

(i) justify the continuing safe functioning of the containment and its discharge routes in faults or accidents involving combustible, explosive and/or toxic gases;

(j) allow for the safe removal and reinstatement of shielding;

(k) define the performance requirements of the containment system during maintenance activities;

(l) demonstrate that a loss of electrical supplies, air supplies or other services does not lead to a loss of containment, nor the delivery of other safety functions;

(m) justify the adequacy of control methods and timescales for re-establishing contained conditions where access to the containment is temporarily open (eg during maintenance work); and

(n) incorporate measures to minimise the likelihood of unplanned criticality if a significant amount of fissile material could be present.

Engineering principles: containment and ventilation: containment design	Provision of further 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 radioactive material, should be provided with further containment barrier(s) that have sufficient capacity to deal safely with the leakage resulting from any design basis fault.		

526. 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.		

527. Where access is necessary the containment should be designed to perform its safety function(s) at all times.

528. There should be no need for access to the containment to ensure the safety of the facility in either the short or long term following an accident.

529. 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 failures and still provide confinement by minimising the migration of airborne activity; and

(c) ensure that a major failure in one glovebox or its systems does not compromise the containment performance of associated gloveboxes.

Engineering principles: containment and ventilation: containment monitoring	Monitoring devices	ECV.6
Suitable and sufficient monitoring devices with alarms should be provided to detect and assess changes in the materials and substances held within the containment.		

530. The devices and alarms should monitor the physical and environmental conditions important to safety. These devices and alarms should ensure the timely detection, and aid assessment, of unplanned or uncontrolled changes in materials and substances held within the containment. Examples of these may include changes to the quantity, composition, characteristics of volume, radioactivity, fissile content, temperature, and pressure of materials and substances, as well as the presence of explosive mixtures, including gases and vapours that could challenge the containment boundary. Where appropriate the capability to sample the materials and substances should also be provided. Further guidance on assessing the control of nuclear matter is provided in paragraphs 469 ff.

Engineering principles: containment and ventilation: containment monitoring	Leakage monitoring	ECV.7
Appropriate sampling and monitoring systems should be provided outside the containment to detect, locate, quantify and monitor for leakages or escapes of radioactive material from the containment boundaries.		

531. The sampling and monitoring should include environmental surveys in the vicinity of the facility.

532. Provision should be made for testing the leakage monitoring systems at suitable intervals to confirm continuing system performance. Such testing may include, for example, monitoring depressions, airflows, inerting gas concentrations, filter performance or valve response times (see also Principle EMT.6).

Engineering principles: containment and ventilation: import and export of nuclear material	Minimisation of provisions for import or export of materials or equipment	ECV.8
Where provisions are required for the import or export of materials or equipment into or from containment, the number of such provisions should be minimised.		

Engineering principles: containment and ventilation: import and export of nuclear material	Containment and ventilation system design	ECV.9
The design should ensure that controls on fissile content, radiation levels, and overall containment and ventilation standards are suitable and sufficient.		

533. Where appropriate, the following should be provided:

(a) remote handling devices and means to facilitate their operation, decontamination and repair; and

(b) additional containment, local ventilation, and shielding.

Engineering principles: containment and ventilation: ventilation design	Ventilation system safety functions	ECV.10
The safety functions of the ventilation system should be clearly identified and the safety philosophy for the system in normal, fault and accident conditions should be defined.		

534. The safety philosophy should identify the relative priorities of aspects such as the direct protection of people; the control and minimisation of discharges; fire protection; and process protection.

535. Where a ventilation system is needed, 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.

536. Where appropriate, the ventilation design and the associated safety justification should include the following:

(a) provision of a suitable working environment for personnel and structures, systems and components, 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, vapours etc from external sources where this ingress could prejudice the safety of operators or operations due to its chemical, radioactive or toxic 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 material as appropriate;

(i) minimising the risk arising from the chemical, radioactive and toxic properties of process materials and from explosive mixtures, including gases and vapours, that may be generated;

(j) segregation and isolation to protect against identified faults 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 the 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(s) and appropriate selection of materials and equipment for the required design life;

(p) setting the total airflow through the system from inlet to discharge to minimise the requirement for disposal of filters, while still retaining a safe atmosphere, airflow velocities, pressure differences and other features of the design; and

(q) provision of inerting atmospheres where appropriate, for example in gloveboxes, either as part of normal operations, or temporarily as part of a fire suppression system.

537. 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 also be made to enable filters to be changed, in accordance with a defined replacement regime, while maintaining the effectiveness of the ventilation system.

538. 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 design requirements. This should include provision of appropriate alarm/control systems on key plant parameters.

Reactor core

539. *The principles 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 365 ff.). The principles relate to the need 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.		

540. This principle covers normal operation, including 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; and

(c) confinement of radioactive material.

541. 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 radioactive materials are challenged. These should be chosen so that safety systems (or administrative safety measures) will provide robust and reliable protection against any such release.

542. 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.

543. 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.		

544. Where a shutdown system is also used for the control of reactivity, a suitable and sufficient shutdown margin should be maintained at all times. The margin should be chosen to maintain sub-criticality in the most reactive conditions permitted by the safety case and should include appropriate allowances for uncertainties.

545. 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 permitted range.		

546. An increase in reactivity or reduction in coolant flow, caused by 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.

547. 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; and

(b) failure of the primary coolant circuit.

Note: Where these mechanisms cannot be prevented by design, protective measures should be available to maintain the facility in a safe condition.

548. The structural integrity limits for the core structure and its components (including the fuel) should be determined to ensure that their geometry will be suitably maintained.

549. 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.

550. The 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.

551. There should be suitable and sufficient design margins to ensure that any reactivity changes do not lead to unacceptable consequences. Limits (operating rules) should be set for the maximum degree of positive reactivity.

552. 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.

553. 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.

554. Core components should be mutually compatible and compatible with the remainder of the plant.

555. The incorrect location of any core components should be physically inhibited.

Engineering principles: reactor core	Monitoring of parameters important to safety	ERC.4
The core should be designed so that parameters and conditions important to safety can be monitored in all operational and design basis fault conditions and appropriate recovery actions taken in the event of adverse conditions being detected.		

556. Fuel assemblies should be designed to permit suitable and sufficient inspection of their structure and components before loading into the core. Provision should be made for in-service monitoring and post-irradiation inspection to confirm fuel behaviour and performance.

557. The design should allow fuel to be removed from the reactor, despite any in-service damage such as bowing, swelling or from other damage occurring in normal operation and design basis fault conditions.

Heat transport systems

558. *These principles relate to the systems required to transport heat within nuclear facilities, both in normal operation and fault conditions. They are intended to cover the full range of facilities where heat transfer is important to safety, for example 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 be considered.*

Engineering principles: heat transport systems	Design	EHT.1
Heat transport systems should be designed so that heat can be removed or added as required.		

559. 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 limits (operating rules) derived for normal operational and design basis fault conditions.		

560. The various sources of heat to be added or removed from any system and its component parts under normal and fault conditions should be quantified, and the uncertainties estimated in each case.

561. Inherent cooling processes such as natural circulation can be taken into account in assessing the effectiveness of the heat transport system, provided they are shown to be effective in the conditions for which they are claimed.

562. In the case of liquid heat transport systems, there should be a margin to the failure of the intended heat transfer regime under predicted normal operational and fault conditions. The minimum value of this margin should be stated and justified with reference to the uncertainties in the data and in the calculation methods employed.

Engineering principles: heat transport systems	Heat sinks	EHT.3
A suitable and sufficient heat sink should be provided.		

563. Provision should be made for removal of heat to an adequate heat sink both in normal operations and during faults and accidents. The safety case should consider the potential non-availability of external resources and also site-related environmental parameters such as variations in air and water temperatures, available levels and flow rates of water etc.

Engineering principles: heat transport systems	Failure of heat transport system	EHT.4
Provisions should be made in the design to prevent failures of the heat transport system that could adversely affect the heat transfer process, and to maintain the facility in a safe condition following such failures.		

564. Provision should be made to:

(a) minimise the effects of faults within the facility that may propagate through the heat removal or ventilation systems. Personnel and structures, systems and components 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 coolant. Provision should be made for the detection of significant losses 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 leakages of the coolant and keep it within specified limits (operating rules). Isolation devices should be provided to limit any loss of radioactive fluid. Bottom penetrations and lines that are prone to siphoning faults should be minimised in spent fuel ponds; and

(c) provide, where appropriate, 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.

565. The properties of any heat transport fluid, including its composition and impurity levels, should be specified so 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 (operating rules) are maintained.

566. Where mutually incompatible heat transport fluids are used within the facility, provision should be made to prevent their mixing and, where appropriate, to protect personnel and structures, systems and components from harm 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.		

567. Components subject to neutron irradiation should be fabricated from materials that minimise the effects of neutron activation.

568. Provision for removing and storing the radioactive coolant to allow inspection and repair work should be made where appropriate.

569. The design, construction and operation of the facility and the choice of heat transfer fluid should minimise the amount of radioactive material in the fluid. Provision should be made to monitor, control and remove any significant build-up of radioactive material from the heat transport fluid and associated containment.

Criticality safety

570. *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 a significant amount of fissile material may be present, there should be safety measures to protect against unplanned criticality.		

571. The hierarchy of controls set out in the Key engineering principles sub-section (paragraph 145 ff.) is appropriate for criticality safety, and gives preference to minimising the amount of fissile material present, consistent with the process requirements. 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 provided, such as fixed neutron absorbers. Reliance on neutron absorbers requires assurance of their continued presence and effectiveness.

572. Further safety measures may need to be provided, for example to:

(a) control the mass and isotopic composition of the fissile material present;

(b) control the concentration of fissile material in solutions; and

(c) control the amount of neutron moderating and reflecting material associated with the fissile material.

573. The design and operation of plant and equipment dealing with fissile material should facilitate the termination of a criticality incident.

Engineering principle: criticality safety	Double contingency approach	ECR.2
Criticality safety cases should employ the double contingency approach.		

574. The double contingency approach involves a demonstration 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.

575. 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 therefore 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

576. *Most of the Euratom Basic Safety Standards (BSS) Directive (96/29/Euratom) is implemented in Great Britain by the Ionising Radiations Regulations 1999 (IRR99) which are made under the Health and Safety at Work etc Act 1974 (HSW Act). Northern Ireland publishes separate regulations.*

577. *The main aim of the Regulations and the supporting Approved Code of Practice (ACoP) and Guidance (Ref. 12) is to establish a framework for ensuring that exposure to ionising radiation arising from work activities is kept as low as reasonably practicable and does not exceed specified dose limits.*

578. *BSS Directive Articles on intervention for emergency preparedness and response are implemented by the Radiation (Emergency Preparedness and Public Information) Regulations 2001 (REPPIR) which are also made under the HSW Act.*

579. *At the time of writing, a revised Euratom BSS Directive had recently been published; changes will be implemented in national legislation in due course.*

580. *By ensuring that their radiation protection programmes are compliant with this national legislation (IRR99 and REPPIR), operators meet the Euratom BSS and are consistent with the International BSS.*

581. *Providing adequate protection for members of the public and for workers against exposure to ionising radiation and radioactive contamination is required both in normal operations and fault and accident conditions. All facilities must be operated, inspected, maintained and decommissioned in compliance with regulations relating to the safe use of ionising radiations. Adequate protection is that level which ensures compliance with the reasonable practicability requirements of all relevant legislation, taking the latest modern standards into account.*

582. *The principles and guidance in this section apply to all activities we regulate, including 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 IRR99, but with additional details relevant to safety case assessments, along with relevant good practice for licensed sites. For the most part, however, they omit aspects already covered suitably in IRR99.*

583. *Under the BSS, radiation protection is based on the principles of justification of practices and interventions, optimisation of protection and individual dose limitation. Justification of practices is not regulated by ONR and so is not considered in the SAPs.*

Radiation protection	Hierarchy of control measures	RP.7
The dutyholder should establish a hierarchy of control measures to optimise protection in accordance with IRR99.		

584. Guidance from IRR99 is provided below:

"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."

585. The dutyholder should have a strategy to restrict radiation exposure. This should include, but not be 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 case. 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 facility, should be kept ALARP.

586. Personnel exposures in normal operation and in fault and accident conditions (planned and emergency exposure situations) should be optimised taking into account the:

- resources available for protection;
- distribution of individual and collective exposures among different groups of workers, and between workers and members of the public;
- probability and magnitude of potential exposures; and
- potential impact of protection actions on other (non-radiological) risks to workers or members of the public.

Radiation protection	Normal operation (Planned Exposure Situations)	RP.1
Adequate protection against exposure to radiation and radioactive substances should be provided in those parts of the facility to which access is permitted during normal operation.		

Radiation protection	Fault and accident conditions (Emergency Exposure Situations)	RP.2
Adequate protection against exposure to radiation and radioactive contamination should be provided in those parts of the facility that will need to be accessed during faults or as part of accident management. This should include prevention or mitigation of accident consequences.		

587. In line with guidance in the ACoP, the safety case should give preference 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 needed to achieve or maintain a stable, safe state.

588. There should be appropriate provisions for the measurement of radiation doses to individuals in both normal operations and in fault or accident conditions (planned and emergency exposure situations). Personal dosemeters should be provided to assess effective dose to the whole body and, where appropriate, measure equivalent dose to extremities and the lens of the eye.

589. Exposures should be estimated in advance for normal operations (planned exposure situations) and then monitored and assessed during the work activity using personal dosemeters or suitably located devices.

590. In planning for a radiation emergency, and noting the provision in REPPIR that IRR99 dose limits are dis-applied during such an emergency, the operator shall identify emergency exposure dose levels and must notify these to ONR (which may subsequently direct the substitution of alternative dose levels), and make appropriate arrangements for their application during such an emergency.

591. Appropriate stocks of personal protective equipment (PPE), monitoring equipment, dosemeters etc that are needed for emergency response should be provided, appropriately maintained and securely stored at appropriate locations such as to ensure that they will remain viable and accessible during any emergency conditions (see also Severe accident analysis (paragraph 663 ff.) and Accident management and emergency preparedness (paragraph 768 ff.).

592. Effective systems should be provided 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.

593. Instrumentation should be provided to give prompt, reliable and accurate indication of airborne activity and direct radiation, particularly in operating areas. These should be fitted with alarms to indicate any significant changes in levels necessitating prompt action. The design of this equipment should take into account the required reliability levels and the environmental conditions in which it will need to provide safety functions (see paragraphs 178 ff.). Consideration should also be given to the provision of remote indication of radiological conditions following accident situations (see paragraph 778).

594. Adequate warning systems (though not necessarily a Criticality Incident Detection (CID) system) should be provided wherever fissile material is present, unless the safety case 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 warning systems. Where suitably justified in the safety case, criticality warning systems may form part of a safety system, ie be linked directly to the safety measures designed to achieve the safe termination of a criticality incident (eg they may directly 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 material.		

595. The further division of designated areas should be based upon the levels of radiation, contamination and airborne activity, measured and/or expected as a result of planned work activities within normal operations.

596. Each area should have appropriate controls on access and egress (including evacuation), occupancy and defined arrangements for the use of personal protective equipment.

597. Where doses forming a significant fraction of any statutory dose limit could be incurred in a matter of minutes during normal operations, access should be controlled

by physical means such as interlocks, alarms, or locked doors to prevent unauthorised entry. The viability of prompt escape from such places should be justified in the safety case (see paragraphs 443 ff.). Where physical control measures are not reasonably practicable, an equivalent standard of access control should be ensured by suitably justified administrative arrangements.

Radiation protection	Contaminated areas	RP.4
Effective means for protecting persons entering and working in contaminated areas should be provided.		

598. These should provide for monitoring and controlling any spread of airborne activity and contamination within and beyond each area.

599. Levels of contamination should be kept ALARP, taking into account the nature of the activities being undertaken.

Radiation protection	Decontamination	RP.5
Suitable and sufficient arrangements for decontaminating people, the facility, its plant and equipment should be provided.		

600. These should include provision for monitoring of anything removed from, or any person leaving, contaminated or potentially contaminated locations. The decontamination should be performed locally unless it is demonstrated that a centralised facility is more appropriate in the circumstances.

601. Manipulation of items with high surface radiation dose rates or levels of contamination should be carried out so as to minimise exposures. This may include using remote handling devices and enclosures to prevent 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 normal operation and fault conditions where it provides this safety function.		

602. In particular, the safety case should take into account:

(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 (eg through locations where the shielding is less effective);

(c) the potential for unplanned or uncontrolled movement or loss of shielding (particularly when the shielding is provided by a liquid medium, eg in spent fuel ponds (see also paragraph 604));

(d) the installation behind shielding of equipment or components involving regular handling or to which regular access is needed;

(e) worker extremity exposures during handling and manipulation of radioactive sources;

(f) worker exposure to the lens of the eye; and

(g) the potential for unplanned or uncontrolled removal from behind shielding of any source.

603. Shielding should be used as an integral part of a wider dose optimisation strategy (for example, considering time of exposure and distance from direct radiation sources) designed to keep exposures ALARP. Where temporary shielding is erected, the predicted dose saved by its use must exceed the dose predicted to be received during its installation.

604. Special care should be taken where liquid is used as a shielding material. In such instances the design should include means to prevent unintentional loss of the liquid, detect such losses and initiate an alarm. A recovery plan for loss of the liquid shielding events should be prepared and rehearsed.

FAULT ANALYSIS

605. *The assessment of risks arising from nuclear facilities needs to consider those arising both from normal operation and from fault and accident conditions. This section addresses fault and accident conditions.*

606. *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.*

607. *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 (operating rules), 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 rules. However, DBA alone may not be sufficient to demonstrate adequate safety of the facility.*

608. *Firstly, additional analysis may be needed to understand the overall risk presented by the facility and to allow comparisons to be made against the SAPs Numerical targets (paragraph 695 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).*

609. *Secondly, it will not always be reasonably practicable to incorporate the robust, conservatively designed preventative and protective safety measures expected for design basis faults when the initiating event is highly unlikely or difficult to predict. However, planning for how events with more severe consequences than allowed for in the design basis would be managed, and providing the plant, equipment and procedures that would be needed to control or mitigate their consequences is often reasonable. Plant states which could merit such planning include those arising following:*

    (a) high consequence events of very low frequency for which the design safety measures may be ineffective; and

    (b) design basis events where, conservatively, the safety provisions are assumed to fail.

610. *The principle of defence in depth (EKP.3) means that these types of 'beyond design basis' plant states where the potential consequences are severe should be considered in the safety case. Severe accident analysis (SAA) is therefore used to complement engineering judgement, DBA and PSA to help understand such accidents and determine safety measures to mitigate their consequences and/or protect against further escalation. SAA differs from the DBA in that it is usually (though not exclusively) performed on a best-estimate basis) and its starting point is the degraded plant state following an event, rather than the event itself. Its main aims are to help plan for potential severe accidents and to assist with identifying what*

further plant, equipment and human actions are required beyond what has been identified through DBA and PSA are reasonably practicable.

611. *In line with wider international guidance, the SAA should form part of a demonstration that potential severe accident states have been 'practically eliminated'. To demonstrate practical elimination, the safety case should show either that it is physically impossible for the accident state to occur or that design provisions mean that the state can be considered to be extremely unlikely with a high degree of confidence. Each instance where practical elimination is claimed should be assessed separately, taking into account relevant uncertainties, particularly those due to limited knowledge of extreme physical phenomena (eg the behaviour of molten reactor cores). Moreover, an accident state should not be considered to have been practically eliminated simply on the basis of meeting probabilistic criteria. Instead, any claims made on SSCs in relation to practical elimination need to be substantiated appropriately.*

612. *The fault analysis principles have been written to apply to criticality safety. 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 principles that need to be applied when identifying these measures are no different to those needed for other applications of fault analysis.*

613. *Fault analysis of nuclear facilities often involves consideration of fault sequences and accident conditions for which there is limited or no experience. This may result in 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 ONR'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, professional judgement on whether the assumptions or estimates are supported by appropriate evidence will be a key element of the assessment.*

614. *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 SAA respectively.*

General

Fault analysis: general	Design basis analysis, PSA and severe accident analysis	FA.1
Fault analysis should be carried out comprising suitable and sufficient design basis analysis, PSA and severe accident analysis to demonstrate that risks are ALARP.		

615. The nature and extent of the fault analysis undertaken will depend on the circumstances. It should be very rare for safety submissions in support of permissioning decisions not to include DBA, even if this is just to demonstrate that there are no qualifying design basis faults. Safety cases for power reactors, or where there is significant complexity, or where the Numerical Targets may be challenged should include PSA. Where the hazards are high (see paragraph 664), the safety case should include SAA.

616. Figure 1 (page 210) illustrates the inter-relationship between the three types of fault analysis, DBA, PSA and SAA, and how, in combination, they address the range of potential initiating events with nuclear safety significance off the site.

617. Where the fault analysis is in support of a design under development, the analysis should be against a well-defined reference point in the design process. Where facility-specific or site-specific details have yet to be finalised, all the assumptions made in lieu of these should be stated explicitly and then used to support the later design and construction activities.

Fault analysis: general	Identification of initiating 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.		

618. 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 above which individual doses 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.		

619. The scope, content, level of detail and rigour of the analysis should be proportionate to the complexity of the facility and the hazard potential.

620. There should be a clear relation between the fault sequences used in the DBA, accident states and scenarios used in the SAA, and the fault sequence development of the PSA.

621. Transient analysis or other analyses should be carried out as appropriate to provide adequate understanding of the behaviour of the facility under fault conditions.

622. 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 729, 735 and 751.)

623. The calculated doses should include those arising from the potential release of radioactive material, direct radiation and criticality incidents. The calculations should, where relevant, take into account local (site) aspects relevant to the dispersion of released radioactivity and its potential effects on people (see Principle ST.3).

624. Radiological analysis of severe accidents should be carried out to determine whether the consequences specified in the societal risk target (Numerical Target 9) could be reached.

625. Following the end of operations, a new fault analysis is likely to be needed to cover the decommissioning phase.

Design basis analysis

626. *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.		

627. If possible, DBA should be carried out as part of the engineering design. Where this is not possible (eg for reviews of existing facilities), the analysis should be developed in line with the engineering and human factors analysis to demonstrate that safety functions are met with suitable levels of confidence. In either case, it is important that the analysis fully reflects the engineering and iterates with it to engender improvements, taking the Key Engineering Principles (EKP.1 ff.) into account.

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.		

628. 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 1×10^{-5} pa;

(b) failures of structures, systems or components for which appropriate specific arguments for preventing the initiating fault have been made (see, for example, Principle EMC.3);

(c) natural hazards that conservatively have a predicted frequency of being exceeded of less than 1 in 10 000 years; and

(d) those faults leading to unmitigated consequences which do not exceed the BSL for the respective initiating fault frequency in Numerical Target 4 (paragraph 727 f.).

Note: These criteria have been set to help to identify those fault sequences where application of DBA is likely to be proportionate to the hazard. Where the criteria lead to initiating faults being excluded from the DBA, the safety case should still demonstrate that the resultant risks are as low as reasonably practicable, but by applying other approaches (eg application of relevant good engineering practice, PSA and other forms of deterministic analysis).

629. Initiating fault frequencies should be determined on a best-estimate basis with the exception of natural hazards where a conservative approach should be adopted, eg to reflect uncertainties in the underlying data used when defining the most extreme events.

Fault analysis: design basis analysis	Fault sequences	FA.6
For each initiating fault within the design basis, the relevant design basis fault sequences should be identified.		

630. Correct performance of safety-related and non-safety equipment should not be assumed where this would alleviate the consequences. Where failures or unintended operation of equipment not qualified for specific accident conditions could exacerbate the consequences, or otherwise make the fault more severe, this should be assumed within the DBA.

631. 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 (see Principle EDR.4);

(c) the worst normally permitted configuration of equipment outages for maintenance, test or repair; and

(d) the most onerous initial operating state within the inherent capacity of the facility permitted by the operating rules (see paragraph 643).

Sequences with very low expected frequencies need not be included in the DBA. Judgement should be exercised in this regard, but for high hazard facilities, a fault sequence frequency of 1×10^{-7} pa would be a typical cut-off when applying design basis techniques.

632. 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.

633. Operator actions can be claimed as part of safety measures only if sufficient time is available, adequate information for fault diagnosis is presented and, for existing facilities, appropriate written procedures exist and compliance with them is assured,

and suitable training has been provided. Appropriate analysis should be carried out on any claimed actions (see Principle EHF.5).

634. 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.		

635. The fault sequence analysis should demonstrate, so far as is reasonably practicable, that the correct performance of the claimed passive and active safety systems ensures that:

(a) none of the physical barriers to prevent the escape or relocation of a significant quantity of radioactive material 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.

636. Relocation means the material is no longer in its designated place of residence or confinement.

637. Where the criteria a) to c) in paragraph 635 cannot be fully met within the design, FA.7 nevertheless seeks minimal consequences. This is reflected in Numerical Target 4 which defines the Basic Safety Objectives for the mitigated consequences of design basis fault sequences.

638. In addition to the inclusion of conservative assumptions, it should be demonstrated that a small change in a DBA parameter will not lead to a disproportionate increase in radiological consequences, ie there should be no cliff edge effect. The severity and frequency of the initiating event should be amongst the parameters considered. The aim is to be conservative without being overly pessimistic.

639. DBA consequence assessments should also be used, where appropriate, to inform accident management strategies and emergency plans. This should be done, however, recognising the conservative nature of such assessments.

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.		

640. The analysis should demonstrate that:

(a) all design basis initiating faults are addressed;

(b) appropriate 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.

This demonstration should be summarised on a Fault Schedule (see paragraph 407).

641. The safety measures should be shown to be capable of bringing the facility to a stable, safe state following any design basis fault. Consideration should therefore be given to the mission times required of SSCs when defining the performance requirements for delivering their safety functions. This should include consideration of the time it would take to introduce alternative equipment to take over the long-term provision of safety functions.

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.		

642. DBA procedures should be consistent with and linked explicitly to its safety function categorisation and SSC classification methodologies (see paragraphs 158 ff.) so that safety measures claimed in the DBA are designed and operated (etc) to appropriately high standards.

643. DBA should provide the main basis for:

(a) performance requirements and safety settings (eg actuator trip settings) for safety systems and safety-related equipment;

(b) conditions governing permitted plant configurations and the availability of safety systems and safety-related equipment; and

(c) the safe operating envelope for the facility.

These aspects should be defined through explicit limits and conditions (operating rules) derived within the DBA, or from the results of the DBA. The DBA should also inform the preparation of the operating instructions for implementing these limits and conditions at the facility.

Probabilistic safety analysis

644. *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.*

645. *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 fuel 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.		

646. 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 Numerical Targets 5 to 9 and should help to demonstrate that the risks are, and remain, ALARP.

647. Where the off site accident consequences are potentially significant, such as for an operating power reactor, the PSA should be at least to level 2 (ie provide information on the frequencies and characteristics of different fission product releases to the environment) and include analysis of all external events (including 'beyond design basis' events) that could realistically lead to a significant off-site release (see paragraph 618).

Fault analysis: PSA	Validity	FA.11
PSA should reflect the current design and operation of the facility or site.		

648. PSA should be directly related to existing facility and site information, data and documentation. Assumptions used in the absence of such information should be justified and careful consideration taken of their impact on the analysis. The PSA should be updated regularly, which for power reactors should mean adopting a 'living PSA'. Where the PSA is in support of a design under development, the guidance set out in paragraph 617 should be followed.

Fault analysis: PSA	Scope and extent	FA.12
PSA should cover all significant sources of radioactivity, all permitted operating states and all relevant initiating faults.		

649. Faults with low initiating frequencies need be included only in so far as the PSA results might reasonably affect the design or operation of the facility. Screening criteria used to exclude low frequency faults should be justified.

650. The identification of initiating faults should consider the potential for combinations of hazards. At multi-facility sites, the analysis should also consider the potential for specific initiating faults giving rise to simultaneous impacts on several facilities or for faults in one facility to impact another facility.

Fault analysis: PSA	Adequate representation	FA.13
The PSA model should provide an adequate representation of the facility and/or site.		

651. 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.

652. The sequences defining the success criteria used in the PSA should be modelled either individually or as part of a bounding sequence until a stable, safe state (for example on reactors, a cold shutdown state) is reached. The 'mission time' (ie the duration over which the PSA is applied) for PSA should be justified accordingly. Where repair and/or recovery actions are needed to achieve a stable, safe state, these should be modelled.

653. The PSA should account for contributions to the risk including, but not necessarily restricted to:

(a) random individual component failures;

(b) components which fail 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 (see Principle EHF.3);

(g) human errors during the course of fault sequences, including those required for repair or recovery actions (see Principle EHF.5); and

(h) potential dependencies between separate human activities (either by the same or by different operators).

654. 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.

655. Best-estimate methods and data should be used as far as possible within the PSA and in particular for determining initiating event frequencies and in the supporting transient, accident progression, source term and radiological analyses. Where this is not practicable, conservative assumptions should be made and the sensitivity of the results to these assumptions should be established. Notwithstanding Principle FA.5, an adequately justified best estimate frequency should be used for naturally occurring hazards.

656. 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 is 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.

657. 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 all key influencing factors.

658. Assumptions made regarding the behaviour of the facility or its operators should be justified, and the sensitivity to those assumptions should be analysed.

659. Due regard should be given to the uncertainties in input probability and frequency values used, and their impact on the results.

660. 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.		

661. Appropriate use of PSA should be made in activities such as:

(a) designing the facility;

(b) supporting modifications to design or operation;

(c) supporting the demonstration that risks are tolerable and ALARP;

(d) informing the selection of safety function categories or the safety class of structures, systems and components (see paragraphs 161 and 165);

(e) setting operating rules;

(f) informing arrangements for examination, maintenance inspection and testing (eg the frequencies of these activities);

(g) plant configuration control (including maintenance planning), which for power reactors is normally through the use of risk monitors;

(h) event analysis and investigating significant incidents and events;

(i) developing and changing operating procedures and associated training programmes for managing faults and accidents (including severe accidents);

(j) helping to determine initiating event frequencies for DBA; and

(k) providing an input to SAA and to analyses performed under REPPIR.

662. PSA models and data should be suitable for their intended application, and sensitivity and uncertainty analyses undertaken as appropriate. In cases where the PSA is not full scope, due account should be taken of the potential impact of aspects not covered.

Severe accident analysis

663. *Rigorous application of DBA and PSA should ensure that the predicted risks from fault sequences leading to significant radiological consequences are very low. Nevertheless, it is important that operators of facilities with very large hazard potentials consider possibilities such as:*

- *the DBA or PSA may be incorrect or incomplete;*
- *the true severity of an initiating event may exceed that considered in the analysis; or*
- *a safety measure could be circumvented or fails in some unpredicted way.*

In considering these matters, further beyond design basis improvements may then be identified as reasonably practicable for either preventing severe accidents, or mitigating their consequences, eg by preventing further escalation. The insights gained from SAA are also important for planning for the possibility of severe accidents and are used to inform the response activities that would be needed were such an accident to occur.

664. *Undertaking SAA is not proportionate for all types of facilities, as not all present hazards of sufficient magnitude to warrant this. However, SAA is beneficial for facilities presenting the highest hazards, such as operating reactors, spent fuel storage facilities and facilities storing significant quantities of nuclear matter. In these principles, severe accidents are defined as those fault sequences that could lead either to consequences exceeding the highest off-site radiological doses given in the BSLs of Numerical Target 4 (i.e. 100 mSv, conservatively assessed) or to an unintended relocation of a substantial quantity 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 9.*

665. *SAA looks typically at states and scenarios which the DBA and PSA have justified as being highly unlikely, and then considers questions such as 'what more can reasonably be done?' or 'what would need to be done in such an event?'. Solutions to these questions will vary according to the type and age of facility under analysis. For example, for the most modern power reactors, where SAA is used to plan for how to contain and cool molten fuel in the aftermath of a major event, solutions such as in-vessel retention and ex-vessel core catchers have been proposed. At older facilities not designed with the insights of SAA, the analysis has helped to identify improvements such as better emergency power supply arrangements capable of catering for situations where grid supplies might be lost for extended periods.*

Fault analysis: severe accident analysis	Scope of severe accident analysis	FA.15
Fault states, scenarios and sequences beyond the design basis that have the potential to lead to a severe accident should be analysed.		

666. The SAA should, through a systematic approach, analyse beyond design basis states and scenarios arising from the circumstances listed in paragraph 609. In line with the principle of practical elimination (see paragraph 611), states and scenarios should not be dismissed from the analysis on frequency grounds alone. Indeed, SAA is not normally concerned with the sequences leading to the severe accident (these being the province of DBA and PSA), but instead should be focused on how the accident state or scenario will be controlled and/or mitigated.

667. For each state or scenario, the SAA should:

(a) determine the magnitude and characteristics of the predicted source term and its potential radiological consequences, including societal effects; and

(b) demonstrate that there is no sudden escalation of consequences just beyond the design basis (see Principle EHA.7 – cliff edge effects).

668. The analysis should include consideration of failures that could occur in the physical barriers containing radioactive material, or in the shielding against direct radiation.

669. 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. Where a best estimate approach is not followed, the extent to which the analysis could nevertheless be used to inform emergency response activities (eg in regard to the expected timings of escalations in the accident sequence) should be considered.

670. In addressing paragraph 632 b) and Principle EHA.7, the SAA should include a best-estimate margins analysis as described in paragraph 248.

671. The SAA should be based on an adequate understanding of the severe accident phenomena and accident progression. 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
Severe accident analysis should be used in the consideration of further risk-reducing measures.		

672. The severe accident analysis should provide information to:

(a) assist in the identification of any further reasonably practicable preventative or mitigating measures beyond those derived from engineering analysis, DBA and PSA;

(b) form a suitable basis for accident management strategies and procedures (see Principle AM.1);

(c) support the preparation of emergency plans for the protection of people (see Principle AM.1); and

(d) support the PSA of the facility's design and operation.

673. Measures identified under a) above need not necessarily involve the application of conservative engineering practices used in the DBA, but could instead be based upon realistic or best estimate assumptions, methods and analytical criteria. Such approaches have advantages in a severe accident context in that they can result in the provision, for instance, of simple and flexible measures that can be stored remote to the site and deployed to the uncertain and degraded environment following a major event. The SAA should consider the nature of the safety functions to be provided by the additional measures, the conditions and circumstances under which

they will need to operate (see paragraph 175) and the ease with which they could be deployed. Some safety functions will need to be fulfilled in situ and in circumstances where the design basis provisions will by definition have already failed. This will likely dictate the use of robust designs. The appropriateness of the engineering standards adopted should be justified on a case-by-case basis.

674. In order to address b) and c), the severe accident analysis should be consistent with the site's (or facility's) accident management and emergency preparedness arrangements. In particular, consistent assumptions should be applied in regard to each of the aspects listed in paragraphs 771 ff., for example the procedures in place, the instrumentation, plant, equipment and supplies available, the personnel who could be deployed and the timescales assumed (eg time when self-reliant, see paragraph 778 and 786).

Fault analysis: severe accident analysis	Relationship to DBA and PSA	FA.25
The severe accident analysis should be performed in a manner complementary to the DBA and PSA, so that each type of analysis informs the others in a mutually consistent manner within the facility's safety case.		

675. DBA and PSA should be used to identify areas which require additional attention from SAA. DBA has the potential to identify the bounding magnitude of the potential consequences and measures which would need to fail for there to be a severe accident.

676. PSA should not be constrained by the assumptions and Numerical Target 4 (etc) criteria defining DBA fault sequences. As a result it should consider the consequences of initiating events not considered within the design basis and fault sequences where design basis measures have failed. For facilities capable of suffering a severe accident, the PSA should be conducted to at least level 2 (see paragraph 647).

677. Unlike DBA and PSA, the SAA should not focus particularly on the detail of the fault sequences leading to a severe accident. These aspects of the fault analysis should be addressed within the DBA and PSA. Instead, the SAA should start by identifying potential severe accident states and scenarios which could impact the facility by virtue of its inherent hazard potential and then analyse these, and in particular how they might develop or escalate, to inform the applications listed in paragraph 672. The results of the SAA should be included within the PSA and used to confirm the validity of the DBA, eg by confirming the absence of cliff edge effects just beyond the design basis.

Assurance of validity of data and models

678. *This section contains principles governing the methods and data used in safety case analyses. They should be applied in the assessment of transient, radiological and other analyses forming part of fault analysis and also in other areas of the safety case underpinned by analysis and/or data, eg engineering substantiation.*

Fault analysis: assurance of validity of data and models	Theoretical models	AV.1
Theoretical models should adequately represent the facility and site.		

Fault analysis: assurance of validity of data and models	Calculation methods	AV.2
Calculation methods used for the analyses should adequately represent the physical and chemical processes taking place.		

679. Where possible, the analytical models should be validated by comparison with actual experience, appropriate experiments or tests.

680. Models 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.

681. Care should be exercised in the interpretation of experiments to take account of uncertainties in replicating the range of anticipated plant conditions. The limits of applicability of analytical models should be identified.

682. Where validation against experiments or tests is not possible, a comparison with other, different, calculation methods may be acceptable.

683. Where possible, independent checks using diverse methods or analytical models should be carried out to supplement the original analysis.

684. Radiological analyses 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	AV.3
The data used in the analysis of aspects of plant performance with safety significance should be shown to be valid for the circumstances by reference to established physical data, experiment or other appropriate means.		

685. Where uncertainty in the data exists, an appropriate safety margin should be provided.

686. 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	AV.4
Computer models and datasets used in support of the safety analysis should be developed, maintained and applied in accordance with quality management procedures.		

687. These procedures should identify measures and controls to provide confidence that calculations are undertaken without error, to a level commensurate with the importance to safety of the analysis being performed.

688. The procedures should, where appropriate, address code and dataset verification, version control, testing, documentation, user qualification requirements and training, peer review and endorsement.

689. The procedures should specify independent verification of computer codes and datasets to confirm consistency with the supporting documentation.

690. The process of inputting data into a model should be independently verified.

Fault analysis: assurance of validity of data and models	Documentation	AV.5
Documentation should be provided to facilitate review of the adequacy of the analytical models and data.		

691. 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	AV.6
Studies should be carried out to determine the sensitivity of the analysis (and the conclusions drawn from it) to the assumptions made, the data used and the methods of calculation.		

692. Where the predictions of the analysis are sensitive to the modelling assumptions, they should be supported by additional analysis using independent methods and, where relevant, computer codes.

Fault analysis: assurance of validity of data and models	Data collection	AV.7
Data should be collected throughout the operating life of the facility to check or update the safety analysis.		

693. This should include, but not be limited 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	AV.8
The safety analysis should be updated where necessary, and reviewed periodically.		

694. 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 analysis or modelling techniques.

NUMERICAL TARGETS

695. *This section describes the numerical targets that inspectors should use as an aid to judgement when considering whether radiological hazards are being adequately controlled and risks reduced to ALARP. The targets quantify ONR's risk policy, and have been set to assist us in making proportionate regulatory decisions and targeting our resources to where the risks and hazards are greatest. More specifically, the targets are guides to inspectors to indicate where additional safety measures may need to be considered and, in the case of permissioning decisions, to help judge whether risks are tolerable.*

696. *The structure of the targets is based on the TOR framework, which was extended in R2P2. In assessing the safety of nuclear facilities, inspectors should examine the safety case to judge the extent to which the targets are achieved, noting that some are also legal limits. Some of the targets are in the form of dose levels; others are expressed as frequencies or risks. Each is set in terms of a Basic Safety Level (BSL) and a Basic Safety Objective (BSO); these have been used to translate the TOR (R2P2) risk policy framework as described in Annex 2. The BSO marks the start of the broadly acceptable level in R2P2.*

697. *Separate targets are defined for normal operations, design basis fault sequences, individual risks, accident frequencies and societal risk. Although most targets are not mandatory, two of the BSLs are legal dose limits in IRR99; these are highlighted below as BSL(LL).*

Basic safety levels

698. *It is ONR's policy that a new facility or activity should at least meet the BSLs. However, even if the BSLs are met, the risks may not be ALARP; in such cases the designer/dutyholder must reduce the risks further. Deciding when the level of risk is ALARP needs to be justified by the designer/dutyholder on a case-by-case basis, applying the legal test of gross disproportion. A graded approach should be used so that the higher the risk (or hazard), the greater the degree of disproportion applied, and the more robust the argument needed to justify not implementing additional safety measures.*

699. *Existing facilities may have been designed and constructed to earlier safety standards, or safety-related structures, systems and components may have deteriorated with the passage of time. Safety cases for such facilities may, in the first instance, demonstrate that the facility exceeds one or more of the BSLs. If the BSL is a legal limit, measures must be taken by the dutyholder to restore compliance and appropriate enforcement action should be considered by inspectors. For other BSLs, ONR's policy is that the level of gross disproportion in ALARP considerations should be very high and so inspectors should assume that it is highly likely that additional improvements to safety will prove reasonably practicable. Inspectors should therefore press dutyholders to demonstrate that a robust optioneering process has been undertaken, including considering the development of new options through research, to control the radiological hazard. Continuing to operate while failing to meet a BSL should only be acceptable if the dutyholder can demonstrate that there are no options that are reasonably practicable to reduce risks further in the short term. Moreover, if operation is to continue, then inspectors should seek a clear longer-term plan to manage and reduce the risks within a period that is as short as is reasonably practicable. Where a BSL is exceeded, consideration should be given to regulatory action to shut down the facility or prohibit or curtail the activity.*

700. *When applying the BSLs, it must be remembered that the TOR2 framework does not in itself provide inspectors with a basis for recommending particular actions, as it has no legal status. The framework does nevertheless help to identify when serious consideration should be given to formal enforcement as a means of achieving compliance with legal requirements, ie reducing risks to ALARP, in accordance with ONR's Enforcement Policy Statement.*

Basic safety objectives

701. The BSOs form benchmarks that reflect modern safety standards and expectations. The BSOs also recognise that there is a level beyond which further consideration of the safety case would not be a reasonable use of ONR resources, compared with the benefit of applying these resources to areas of higher risk. Inspectors therefore need not seek further improvements from the designer/dutyholder but can confine themselves to assessing the validity of the arguments 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 must do so by law.

Numerical targets and legal limits	Applying the targets	NT.3
When comparing the estimates submitted with the targets, inspectors should take account of the assumptions and limitations of the analysis used.		

702. Uncertainties in the submitted safety analyses, and claims of accuracy and precision in numerical estimates should be assessed, eg through sensitivity analyses.

703. In addition, the inspector should compare the assumptions used by designers/dutyholders in determining their estimates against the assumptions built into the target (see Annex 2).

704. When assessing safety cases against the targets, 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 and so meet a target. This is no more than common sense: revising an estimate by a small amount to move it from one side of a target to the other does not make an unsafe situation safe, or a safe one unsafe. Additionally, as with any calculation, the risk estimates are subject to a degree of uncertainty. The numerical targets should thus be applied as approximate guidelines, taking a pessimistic view of the estimated risks in cases where a target is only just met.

705. ALARP demonstrations are sometimes supported by cost benefit analysis (CBA). CBA compares the benefits of implementing further measures to improve safety, taking account of an appropriate gross disproportion factor, with the costs of implementing those safety measures. Where CBA is used to support the ALARP argument, it should follow HSE's general ALARP guidance. In particular, CBA should not form the whole argument justifying an ALARP decision, nor be used to undermine existing standards or relevant good practice.

The targets and TOR/R2P2

706. The levels for individual risk of death in R2P2 cover risks to workers and to members of the public from activities on the site. These are:

- *The 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

- *The 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

707. *Radiation risks arise from normal operational doses and from faults and accidents. These contributions are treated separately in the targets below.*

708. *TOR discussed the effects on society of a major accident and suggested, based on the findings of the 1990 Barnes report on Hinkley Point C (Ref. 13), that an event leading to one hundred to several hundred immediate and eventual deaths ought not be more frequent than one in a hundred thousand years, allowing for the influence of weather conditions. The TOR approach was used in deriving the societal risk target (Target 9).*

709. *More detail on the rationale behind the numerical targets is provided in Annex 2.*

Numerical targets and legal limits	Assessment against targets	NT.1
Safety cases should be assessed against the SAPs numerical targets for normal operational, design basis fault and radiological accident risks to people on and off the site.		

710. Inspectors should not expect or require a detailed calculation to be provided in the safety case for each and every target. However, the safety case should include sufficient information to be able to judge whether the target is likely to be achieved and to justify that the overall risks are ALARP.

711. Safety cases may include intermediate targets for some potential accident sequences; for example, many countries have a target for reactors based on core damage scenarios. Where such targets are proposed, they should be taken into account by inspectors, though it is essential that the overarching Principles EKP.1 to EKP.5 are not compromised through such approaches.

Dose targets and legal limits for normal operation

712. *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 or ingestion of radioactive material, or through the food chain as a result of discharges and disposals of radioactive waste.*

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 (IRR99). Normal operational doses should also be reduced ALARP.*	

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	

713. 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.

714. The analysis of the predicted doses from normal operation to 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.

715. 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 IRR99. Persons under 16 years old should be prevented from working with ionising radiations (International Labour Organisation (ILO) Convention 115 (1960) Article 7.2).

716. 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 (IRR99).*	

717. 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 IRR99 Guidance advises constraining the dose to members of the public from each source to less than 0.3 mSv pa. ONR'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.

718. ONR 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 civil nuclear sites are regulated by the Environment Agency (EA) in England, by the Scottish Environment Protection Agency (SEPA) in Scotland and by Natural Resources Wales (NRW) in Wales, by means of permits or authorisations granted under the Environmental Permitting Regulations (EPR10, in England and Wales) or Radioactive Substances Act RSA93 (in Scotland).

719. 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 the relevant regulatory bodies.

720. The predicted doses likely to be received by people outside the site from normal operations 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

721. *The Fault analysis section (paragraph 605 ff.) describes three forms of analysis used in safety cases for fault and accident conditions: design basis analysis (DBA); probabilistic safety analysis (PSA); and severe accident analysis (SAA). The numerical targets in this section have been selected to assist when judging the results of these analyses.*

722. *DBA is focused on the key safety measures for those initiating faults that are most significant in terms of frequency and unmitigated potential consequences. Target 4 (below) has a dual role in this context:*

    1. *It is used within Principle FA.5 as part of the determination of whether a particular initiating fault should be analysed using DBA. This is done by comparing the conservative unmitigated consequences of the fault against the BSL for the relevant initiating event frequency.*

    2. *It is then used to help judge whether the effectiveness of the safety measures that the DBA has claimed provide protection against the fault sequence. Paragraph 635 sets out qualitative success criteria that these safety measures should achieve (see also paragraphs 630 ff.). The BSOs of Target 4 quantify clauses (b) and (c) of paragraph 635 in terms of mitigated*

radiological doses. They have been set at a level comparable with the BSOs for normal operational doses in Targets 1 and 3, reflecting the intent of DBA to identify safety measures that protect against faults rather than mitigate their consequences (see also paragraph 635). Where the safety measures only provide mitigation, the BSOs and BSLs provide targets for the acceptability of the mitigated consequences as set out in paragraphs 637 ff.

723. *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 paragraphs 630 ff. (for DBA), and including initiating faults as set out in Principle FA.12. 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 653 ff. 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 655). The PSA results can then 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 assessing the overall adequacy of the safety measures and other plant features contributing to safety, and to assist in identifying areas where further risk reduction may be reasonably practicable. The overall risk impact from all facilities on the site should also be assessed against Targets 5 and 7.*

724. *The third form of fault 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 preparedness and other measures that may be taken to control severe plant conditions (see Levels 4 and 5 in Principle EKP.3). 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. These are addressed in the highest dose band of Target 8 and also by Target 9 for societal risk.*

725. Targets 4, 6 and 8 are written in terms of bands (staircases) of increasing dose consequence. Recognising fault analysis is not an exact science; where the estimated consequences of a fault or accident lie just outside a given band (either in terms of frequency or dose) greater account should be taken of the degree of conservatism and uncertainties. This is consistent with Principle NT.3.

Dose targets for design basis fault sequences

726. The numerical targets for DBA represent criteria for assessing the safety of the facility's design and operations for faults that could have significant consequences. They are based on initiating fault frequencies and so take no account of the reliability of the claimed safety measures. Instead, they place the focus on the effectiveness of the safety measures in addressing the fault's consequences (effective dose). The BSOs are set at levels where the consequences will be broadly acceptable, given the likelihood of the initiating fault. Consequences at these low levels will normally only be achievable through installation of appropriately engineered safety measures rather than mitigating systems (see paragraph 151). The DBA should demonstrate that adequate robust safety measures are in place, including the presence of at least one intact barrier at sequence termination.

727. For 'frequent' faults (ie those with an initiating fault frequency exceeding 1×10^{-3} pa) the BSLs are set at the legal limits for normal operational exposures, though they are not legal limits in this case. For less frequent faults, higher fault consequences are likely to be consistent with the requirement to reduce risks to ALARP (other

numerical targets notwithstanding) leading to the stepped relationship shown schematically in Figure 1 (page 210).

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 between 1 x 10^{-4} and 1 x 10^{-5} pa BSO: 0.1 mSv **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 between 1 x 10^{-4} and 1 x 10^{-5} pa BSO: 0.01 mSv	

728. As noted in paragraph 722, the BSLs in Target 4 are also used as screening criteria to assist when identifying which faults should qualify for DBA.

729. The effective doses calculated for comparison with Target 4 should be evaluated conservatively. In addition to the general aspects set out in paragraphs 619 ff., 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 accidents a more realistic occupancy may be assumed after a suitable interval;

(b) the conditions under which the accident is analysed have 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

730. *Risk targets 6 and 8 for accidents apply to individual nuclear facilities rather than whole sites: Target 6 sets out frequency-based BSLs and BSOs for a person on the site from a single accident. Target 8 is for any person off the site and provides BSLs and BSOs that represent the total frequency of all the accidents in each dose band. PSA results may be compared with these targets to assist judgements on:*

(a) the overall adequacy of the safety measures and other plant features (e.g. safety-related systems) contributing to safety; and

(b) identifying areas in which further risk reduction may be reasonably practicable.

731. Targets 5 and 7 are set in terms of the overall (summated) risk impact to individuals from all the facilities on a site. The values used for these targets have been taken from R2P2.

732. *Since most of the risk to people on UK nuclear sites is associated with normal operations, the BSL for accidents in Target 5 is set lower than recommended in R2P2, at 1 x 10^{-4} pa rather than at 1 x 10^{-3} pa. The BSO value is, however, set in line with R2P2, at 1 x 10^{-6} pa. These risk levels are substantially lower than the risk levels associated with Target 1 for employees working with ionising radiation. Dutyholders and/or designers may therefore propose alternative targets applying a different trade-off between normal operational risk and accident risk. Such alternative targets are acceptable provided they are suitably justified.*

733. *Estimation of individual risk on site (Target 5) often requires assumptions regarding occupancy, shift-working etc and so the numerical result by itself does not clearly emphasise the importance of seeking prevention and protection rather than mitigation. It is important therefore that any occupancy (etc) assumptions are properly reflected in formal control measures and are clearly set out in the analysis so that the calculated risks take proper account of their potential failure. Target 6 is helpful in this respect as it sets reasonable expectations for the frequency of single accidents as a function of dose where a worker is assumed to be present. Setting the target in these terms means that occupancy effects are removed from the calculations; the target thus forces a focus on prevention and protection in line with Principle EKP.5.*

734. Care also needs to be taken when assessing safety cases where the estimated risk assumes short-term exposure. Provided sufficient controls and/or alarms are in place, inspectors can take these into account, though the analysis will also need to consider their potential failure.

Individual risk of death from accidents – any person on the site	**Target 5**
The targets for the individual risk of death to a person on the site, from accidents at the site resulting in exposure to ionising radiation, are: BSL: 1 x 10^{-4} pa BSO: 1 x 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 x 10^{-1}	1 x 10^{-3}
20–200	1 x 10^{-2}	1 x 10^{-4}
200–2000	1 x 10^{-3}	1 x 10^{-5}
> 2000	1 x 10^{-4}	1 x 10^{-6}

735. Ideally, best estimate methods should be used to calculate frequencies used for Targets 5 and 6 and for the predicted dose to the most exposed person on the site. Where this is not practicable, reasonably conservative assumptions may be made. The effects of any mitigating action may also be taken into account if a satisfactory case has been made for them.

736. When applying Target 5, the risk of death for each fault sequence should be determined using appropriate dose-risk conversion factors and may take account of occupancy factors. Care will, however, be needed to ensure that the appropriate combinations of doses and probabilities are selected which avoid underestimating the risk.

737. There should be checks to ensure that the Target 5 BSL is not exceeded, particularly if there are contributing dose bands in Target 6 where the predicted frequencies approach its BSLs. In determining the risk to the most exposed person on site, due account should be taken of risk contributions from all facilities on the site.

738. Alternative methods and data, including different dose and frequency bands, may be used to determine worker risks. Where this is done, the case should nevertheless be assessed as described above.

739. Targets 5 and 6 are not intended to include the risks associated with personnel returning to perform recovery actions after an accident once a stable, safe state has been reached.

Assessment of individual risk to people off the site from accidents

740. *The basis of the off-site risk target, Target 7, is that the individual risk to people off the site from the summation of all potential accidents on the site needs to be understood and properly controlled. This target is supported by Target 8, which is facility-based, in the form of a dose-frequency staircase derived from Target 7. The facility-based target is usually the principal target applied for accident risk assessments on the grounds that most safety cases do not lead to significant change in the overall risk from the site. However, should there be a significant increase in the risks from single facilities or a major new risk added to the site, then summated site risk will need to be re-analysed and compared with Target 7.*

741. *The individual risk levels in R2P2 include the risks arising from normal operational doses. Although the legal limit of 1 mSv (Target 3 BSL) equates to a risk of death of approximately 5 x 10^{-5} pa, in general the normal operational doses received are significantly lower. Therefore normal operational risks are not a significant factor when setting individual risk targets for accidents. Moreover, it is very unlikely that the predicted risks from normal operation and accidents will both be near the BSL for any particular individual. As such, the BSL and BSO for Target 7 have been set in line with R2P2.*

742. *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 a particular dose given that the accident has occurred, allowing for wind and weather conditions and the effect of countermeasures. The location assumed for the hypothetical person will also be a critical feature of the analysis.*

743. *The dose-frequency staircase 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 751). These suggest that the dose bands are generally a suitable surrogate for a range of other possible alternative measures of risk, including risk of death. It is also possible for a safety case to demonstrate broad compliance with Target 7 by making use of Target 8 results.

744. *A single facility which just meets all the BSLs in Target 8, 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 1990 Barnes Report for Hinkley Point C and an order of magnitude less than the BSL for Target 7 (which is set in terms of summed site risk and so includes contributions to the risk from the individual facilities on the site).*

745. *A similar estimate can be made for a facility that just meets the BSO frequencies in Target 8, giving an individual risk of the order of 1 x 10^{-7} pa. This is an order of magnitude below the individual site risk BSO of 1 x 10^{-6} pa in Target 7.*

746. *As with the other risk-based numerical targets, Targets 7 and 8 have been set to enable assessment of safety case risks and frequencies evaluated on a best estimate basis.*

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 accidents at the site resulting in exposure to ionising radiation, are: BSL: 1 x 10^{-4} pa BSO: 1 x 10^{-6} pa	

747. As noted in paragraph 706, in comparing Target 7 with Target 5, it should be recalled that workers on the site are also exposed to risks from normal operational doses; these are a more significant fraction for persons on site than persons off site. Taking this factor into account brings these two targets into alignment with one another.

748. The individual risk from a site that contains multiple facilities should be determined from an appropriate combination of the individual contributions. In practice, safety cases often adopt a risk quota approach, facility by facility. In such cases, the quota sums should be compared with the BSOs and BSLs in this target.

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	1×10^{-2}
1–10	1×10^{-1}	1×10^{-3}
10–100	1×10^{-2}	1×10^{-4}
100–1000	1×10^{-3}	1×10^{-5}
>1000	1×10^{-4}	1×10^{-6}

749. The risks from the facility 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 targets for each dose band.

750. Where estimated doses are above about 1000 mSv, the risk of prompt death should also be considered and the analysis extended to enable assessment against the societal risk levels in Target 9.

751. Radiological analysis to evaluate the effective dose for Target 8 should be carried out for a hypothetical person located at the distance of the nearest habitation (ie any place with significant daily occupancy), 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. For Target 7, the analysis should identify the hypothetical person at most risk overall. This will normally be one of the hypothetical persons selected for one of the facilities on the site. They may, however, not be the one closest to the site given variations in individual facility risk and prevailing wind directions. For both Targets 7 and 8, the estimated effective dose should be calculated as the expected value over the possible weather conditions, and for Target 7 the frequency element can also take account of wind direction probabilities.

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 (for power reactors) 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 (for power reactors) 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 (for power reactors) likely to be implemented to several kilometres from the site;
- evacuation of nearby population likely to be implemented.

Societal risk

752. *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.*

753. *The SAA is important in determining the overall impact of the site in terms of the risks of major accidents with significant off-site consequences. The nature of such accidents means that long-term, large-distance stochastic effects will be important, though the magnitude of these depends strongly on the weather. Such accidents may have significant regional or national consequences and so are considered to pose a societal risk. Societal risks from severe accidents are addressed by Target 9.*

754. *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, likely to be mainly from very low doses to very large populations (ie stochastic deaths). The target does not in itself cover*

directly all the factors related to societal concerns (eg environmental damage and clean-up costs) but is intended instead to be a surrogate to reflect these aspects. In addition, dutyholders' ALARP demonstrations must also include all applicable societal effects directly attributable to the accident.

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 accidents at the site resulting in exposure to ionising radiation, are: BSL: 1×10^{-5} pa BSO: 1×10^{-7} pa	

755. The safety case should identify accidents with source terms that could cause 100 or more deaths. The total risk should be calculated taking account of the frequency distribution of these accident source terms, applying probabilistic weather condition assumptions. In estimating the risks, fatalities both on and off the site should be included.

756. It is expected that a significant proportion of the fatalities resulting from a severe accident will involve stochastic deaths, which are typically estimated using collective dose calculations. Based on studies carried out by Public Health England (formerly 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 Target 9.

757. 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.

758. The ability to implement off-site countermeasures should be based on current UK and relevant international advice and, where claimed, should be justified in the safety case. Similarly, assumptions that on-site effects will be limited by the implementation of accident management and emergency preparedness arrangements should be properly justified.

Dealing with time at risk situations

759. *Most of the risk targets set out above are given as frequencies based on annual averages. Circumstances will arise, however, where a higher risk will exist for shorter periods of time that make the use of annualised frequency targets inappropriate. A decision nevertheless has to be made as to whether additional safety measures are needed to reduce these higher risks to ALARP. Clean-up and decommissioning activities may also entail periods of elevated risk where arguments related to the timescale of the activity may be important.*

760. *There are three main situations where a safety case may argue for the acceptability of increased risk for relatively short periods in order to justify not improving safety to a level that would otherwise be reasonably practicable in continuous, long-term operation:*

(a) Through life – Where a short-term increased risk is needed for continued normal operation of the facility. Examples here include undertaking certain maintenance activities; temporary disconnection of safety measures to allow

completion of essential tasks or other intermittent activities that are required to sustain operation.

(b) Residual facility life – Where an ageing facility may now have eroded safety margins, for example due to ageing effects, or its risks may appear high when compared to modern standards. These higher risks may be argued to be acceptable because the short residual operating life of the facility means that significant investment is not reasonably practicable.

(c) End of life legacy – Where clean-out or decommissioning of a facility causes short periods of increased risk compared to those prior to these activities commencing. Dutyholders may argue this is unavoidable if remediation of the facility is to be completed and that the risks are acceptable when balanced against the risk reductions to be gained in the longer term.

761. *The guidance in this section has been written to apply to all three situations described above.*

Numerical targets and legal limits	Time at risk	NT.2
There should be sufficient control of radiological hazards at all times.		

762. Any period in which the risk is elevated (eg due to any of the reasons a) to c) listed in paragraph 760) must be subject to a specific demonstration that risks are controlled to ALARP. The period of elevated risk should be as short as reasonably practicable. The short duration of the increased risk should not be used as the sole argument for justifying risks are ALARP.

763. The safety case should not rely solely on numerical risk estimates or on averaging risk over a longer period of time. Instead, sufficient protection based on good engineering and administrative controls should be available and prominent in the safety case. The extent of the protection should be commensurate with the prevailing level of risk, taking due account of the hierarchy of safety measures described in paragraph 155 (Principle EKP.5) and considering all levels of defence in depth (Principle EKP.3).

764. Any reasonably practicable step that can be taken to eliminate, reduce or mitigate increased risks should be taken even though the time of higher risk may be short.

765. Means of reversing the situation or otherwise recovering control should be available in the event that a significant deviation from the basis of safety or operational intent occurs. Reasonably practicable contingency measures should also be identified to manage safety should such a reversal or recovery not be possible, including temporarily enhanced accident management arrangements.

766. During operations which impose a planned, short-term, elevated risk, appropriate 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 of the safety case. Increased surveillance may form part of the overall argument justifying a short-term period of increased risk.

767. Short-term high risks that would exceed a BSL if they had instead been evaluated as a long term continuous risk 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 in order to reach a safer state in the long term (eg during the recovery phase following an event or in end of life legacy situations highlighted in paragraph 760).

ACCIDENT MANAGEMENT AND EMERGENCY PREPAREDNESS

768. *The objective of accident management and emergency preparedness is to take all reasonably practicable measures to prepare for possible accidents at nuclear facilities, and to mitigate their consequences should they occur. Accident management and emergency preparedness comprise Levels 4 and 5 of the Defence in Depth hierarchy in Principle EKP.3. In summary proper application of the hierarchy should ensure, with high confidence, that all faults and accidents taken into account in the design of the facility will have only minor radiological consequences that are below prescribed limits. The accident management and emergency preparedness arrangements should also be designed to cater for severe accidents beyond the design basis of the facility (see paragraph 663 ff.) and ensure that the consequences of these will be mitigated to the extent that is reasonably practicable.*

769. *Fundamental Principle FP.7 states that arrangements must be made for emergency preparedness and response in the case of nuclear and radiological incidents. For licensees these arrangements are regulated through various licence conditions, including Licence Condition 11. In addition, REPPIR places duties on relevant operators of nuclear facilities and on local authorities in regard to emergency preparedness.*

770. *REPPIR and its supporting guidance establish a framework for the protection of workers and the public through emergency preparedness for radiation emergencies. The regulations place specific duties on both operators and local authorities. These duties include, among other things, the need for hazard identification and risk evaluation (HIRE), a Report of assessment (RoA), and the development and testing of dutyholders' off-site emergency plans. ONR uses RoA and HIRE reports to help define the REPPIR Off-site Emergency Planning Area. Local authority emergency planners are then required to develop detailed off-site emergency plans covering this area. It is good practice for local authority emergency planners to also consider the extendibility of countermeasures beyond the REPPIR Off-site Emergency Planning Area. This framework is intended to provide an integrated approach so, for instance, the dutyholder's emergency plan should be developed in liaison with the emergency services.*

Accident management and emergency preparedness	Planning and preparedness	AM.1
Strategies and plans should be in place to prepare for and manage accidents at the facility and/or site.		

771. Accident management strategies should be developed to manage the escalation of accidents and to restore control. The dutyholder's safety case, related fault analysis and HIRE analysis should be used to form a suitable basis for developing these strategies. Where the hazard potential is significant (see paragraph 664), the HIRE should be informed by severe accident analysis. The strategies should aim primarily to prevent the breach of barriers to release or, where this cannot be achieved, to mitigate accident consequences. Their ultimate aim should be to return the facility and/or site to a stable, safe state.

772. Where the site emergency plan relies on the use of shared or mobile equipment stored elsewhere, in order to be effective, the plan should secure the availability of the necessary equipment at the appropriate timescales.

773. On multi-facility sites, the scope of the strategies and plans should include accidents affecting multiple facilities. Similarly, where neighbouring sites could be affected by a common incident, this should be reflected in the strategies and plans. Further guidance on multi-facility and neighbouring sites is provided in Principle ST.6.

774. The strategies and plans should include the management of long-lasting events in which external assistance to the site may be limited or absent due to severe infrastructure disruption in and around the site. In addition, they should be capable of extension should a more severe accident occur than planned for.

775. The strategies and plans should identify all the procedural support requirements that will be needed during an accident. The procedures should define all the roles and responsibilities needed for an effective accident response. Effective storage arrangements should be in place to ensure the timely availability of these procedures in accident conditions.

776. The procedural support requirements should include emergency operating procedures and accident management guidelines. The accident management guidelines should be based on the facility's severe accident analysis and be written to facilitate timely and well-informed decision making during accidents. The emergency operating procedures should be written recognising the potential practical difficulties (eg degraded state, radiation levels, poor lighting, access issues and communication system failures) that could reasonably be encountered by operators working in accident conditions.

777. The emergency operating procedures and accident management guidelines should be tested during emergency exercises to confirm their accuracy and effectiveness and should also form part of operator training. At operating power reactors, testing of the emergency operating procedures and, where practicable, the accident management guidelines should include the use of full-scope plant simulators.

778. The strategies should include the provision of appropriately robust, suitable and sufficient instrumentation for monitoring the facility and site in accident conditions (see Principle ESR.1). The design and location of in-situ instrumentation should be informed by severe accident analysis. The instrumentation should:

(a) support implementation of the emergency operating procedures and accident management guidelines;

(b) facilitate decision making;

(c) indicate the facility/plant status;

(d) support the estimation of quantities, and the location of released radioactive material; and

(e) record important parameters.

779. The plant, equipment and supplies needed for the accident management strategy should be identified and then tested, maintained and inspected in accordance with their safety significance (see Principles EMT.1, EMT.2 and ECS.3). Where additional plant, equipment or supplies beyond those needed for the design basis would facilitate accident management, this should be provided wherever reasonably practicable.

780. The plant and equipment identified for accident management should be of appropriate robustness, although it may be of a different type and of lower robustness than that provided for normal operations and design basis faults. However, where such plant or equipment is located within the facility that is subject to the accident conditions, it should be sufficiently robust to survive those conditions and accessible during those accident conditions. The robustness requirements of all plant and equipment needed for accident management should be informed by severe accident analysis as described in paragraph 673.

781. The emergency preparedness arrangements should provide appropriate secure storage for all plant, equipment and supplies needed for accident management. This will necessitate either robust stores capable of surviving the initiating event, or stores located remotely from the facility (either on or off the site). The suitability of the storage arrangements and the viability of plans to deliver materials and equipment to the site (eg in situations where the local infrastructure is severely disrupted) should be assessed in the safety case.

782. In addition to the arrangements made by the local authority in the off-site plan, provision should be made for off-site logistical and technical support, for example for the delivery of materials and supplies that might be needed when responding to a severe accident and for strategic (regional or national) stores of plant, equipment and other supplies. Suitably conservative timescales for how long the site might need to be self-sufficient should be identified and justified. These should be used to set detailed requirements for the materials and supplies to be held on, or local to the site. Further guidance on essential services is provided in paragraphs 436 ff., and in particular in Principle EES.3

783. An on-site emergency control room should be provided from which an emergency response can be suitably and safely directed. This should be located such that the likelihood of its non availability due to the emergency itself is minimised. At operating reactor sites, this should be separate from both the control room and the supplementary control site. In the case of multi-facility sites, where one or more such centres may be provided, appropriate command and control arrangements to ensure a co-ordinated response shall be put in place. A strategic centre should be located on or off site, to support responding agencies, to receive information and briefings, and to support the response with local government etc.

784. Facilities should also be provided for managing the deployment and return of emergency response teams, including briefing and rest/recuperation areas. Where reasonably practicable, such facilities should be of a robust design and suitably protected from radiation and other hazards potentially present in accident scenarios. These facilities should be designed to operate independently, without any need for off-site support.

785. The accident management strategy should identify the number of operators and other site staff needed to address different types of accidents, the skills they need and how they would be deployed to and within the site or facility in accident conditions. Deployment plans should cater for long-lasting accidents, including those where there is severe local infrastructure disruption. On multi-facility sites the plans should describe how resources will be shared across the site.

786. Provision should be made for training personnel (including from the local emergency services) in the accident management procedures and implementing the accident management strategies. The training should include periodic exercising of the site's emergency arrangements, including multi-facility exercises where relevant. The

exercises should be chosen so that in total they test the full scope of the site's arrangements and activities within the plans, eg the deployment of mobile equipment such as pumps and generators.

787. Further guidance relevant to on-site accident management can be found throughout these principles (eg on severe accident analysis, see paragraph 663 ff.). Detailed guidance on off-site arrangements for nuclear emergency planning is maintained on the UK Government's Nuclear Emergency Planning Liaison Group (NEPLG[5]) website (Ref 14).

[5] The NEPLG is to be renamed the Nuclear Emergency Planning and Response Guidance Working Group in the near future

RADIOACTIVE WASTE MANAGEMENT

788. *The management of radioactive waste is a function potentially spanning all the stages of the lifecycle of a facility. In addition to the principles provided in this section, most of the rest of the SAPs will be relevant.*

789. *This section recognises that the minimisation and control of waste should be taken into account at all stages of the facility's lifecycle, starting at the planning and design stage and then 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. The principles need to be applied in a proportionate manner.*

790. *Some radioactive waste is also nuclear matter, and therefore the principles in the sub-section Control of nuclear matter (paragraph 469 ff.) will apply. Conversely, the principles in this section may also be relevant to the management of 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 the radioactive waste management principles to nuclear matter and vice versa should be considered on a case-by-case basis taking account of the specific circumstances.*

Strategies for radioactive waste

791. *A strategy is an essential prerequisite for the safe and timely management of radioactive waste on a site and to meet Government policy. The strategy links together relevant factors, defines timescales (eg for achieving passive safety) and demonstrates how the site's waste management will be integrated with other relevant strategies. The timescale for the achievement of passive safety is an important aspect of strategy.*

792. *Relevant factors within the strategy will include the identification and availability of waste storage facilities and potential disposal routes, how to manage multiple waste streams in parallel, the quantities of waste involved, the magnitude of the radiological (and other associated) hazards, the potential for those hazards to be realised, the expected dose uptake and the costs.*

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.		

793. 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;

(c) demonstrate how the hazards posed by historic wastes are reduced systematically and progressively (see Principle RW.6);

(d) include a description of the dutyholder's policy and objectives for the management of radioactive waste;

(e) ensure that the generation of radioactive waste is prevented or minimised (see Principle RW.2);

(f) cover the site's current and future radioactive waste inventory, including waste arising from proposed new facilities;

(g) encompass the anticipated timescales for the management of radioactive wastes, from production to disposal (where appropriate), including intermediate management steps;

(h) consider a full range of options during its development. The optioneering process should take account of all relevant factors, which may include those listed in Principle RW.6 concerned with timing;

(i) describe, or refer to, the different options that were considered during its development and the safety case justifying the chosen option(s);

(j) contain, or refer to, the plan for managing each waste stream on the site from its generation to the final management step, including nuclear matter that may be categorised as waste in the future;

(k) identify the optimum waste management route;

(l) take account of off-site and on-site interdependencies, eg between waste processing facilities;

(m) ensure that radioactive waste is managed in a manner that minimises the need for future processing;

(n) ensure that the generation of radioactive waste of a type or form incompatible with currently available storage or disposal technology is prevented or minimised;

(o) ensure that waste that cannot be managed using current techniques, or techniques under current development, is not created;

(p) take account of biological, chemical and other hazards that may influence the management of radioactive waste;

(q) ensure that the adequacy of the storage capacity needed is reviewed at appropriate intervals, eg to take account of current and future wastes generated, the safe operating lifetimes of existing stores and planned additional stores;

(r) be compatible with facility safety cases, including, where relevant, facilities at other sites;

(s) include an outline of the safety management system and the general approach to ensuring that radioactive waste is managed safely now and in the future;

(t) describe the significant assumptions, uncertainties and project risks associated with the strategy, and how these will be managed;

(u) be compatible with the requirements of permits or authorisations granted by the environmental regulators; and

(v) be kept up to date and reviewed at appropriate intervals.

Waste minimisation

794. *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 are two of the foremost principles of good waste management. This is embodied in international standards and Government policy and so needs to be considered and applied during the planning, design, construction, manufacture, commissioning, operational and decommissioning stages of a facility's lifecycle.*

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.		

795. Licence Condition 32 requires the rate of production of radioactive waste be minimised so far as is reasonably practicable. The safety case should therefore describe:

(a) the specific design provisions;

(b) operating practices; and

(c) approaches to decommissioning that will ensure waste minimisation and include a demonstration that the rate of production of radioactive waste has been minimised.

796. 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's lifetime.

797. Factors to be considered in assessment against this principle should include:

(a) the facility layout and service infrastructure;

(b) secondary waste generation;

(c) recycling and re-use of materials; and

(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, the benefits (or otherwise) of waste segregation, doses to operators, other wastes generated and resultant discharges.

798. Trends in radioactive waste generation should be monitored and the effectiveness of the waste minimisation measures employed demonstrated. This should be undertaken in a holistic manner, taking into account plant operations and all forms of radioactive waste. Reviews should be undertaken to seek further opportunities for radioactive waste reduction.

Radioactive waste management	Accumulation of radioactive waste	RW.3
The total quantity of radioactive waste accumulated on site at any time should be minimised so far as is reasonably practicable.		

Note: Achieving this principle is mandatory under Licence Condition 32. The principle applies throughout the lifecycles of the facilities on the site.

799. The safety case should demonstrate that the accumulation of radioactive waste has been duly minimised. In addition, volume reduction should be considered during all stages of a facility's lifecycle.

800. Where disposal is the most appropriate option, full use should be made of appropriate, duly authorised disposal routes. This includes routes that are both authorised and covered by exemption provisions under the Environmental Permitting Regulations (EPR10, in England and Wales) or the Radioactive Substances Act (RSA93, in Scotland).

Characterisation and segregation

801. *The development and application of good characterisation and segregation practices for radioactive wastes provide a sound foundation for their safe and effective management from generation through to disposal. However, for some existing wastes, the extent to which characterisation and segregation can be applied may be limited. Where this is the case (eg due to past poor practice), the safety case should justify how these wastes will be managed safely, highlighting relevant uncertainties and how these will be accommodated, adopting a precautionary approach.*

Radioactive waste management	Characterisation and segregation	RW.4
Radioactive waste should be characterised and segregated to facilitate its subsequent safe and effective management.		

802. Suitable and sufficient design features, locations, equipment and arrangements should be provided to support characterisation, segregation and other waste management activities.

803. An inventory identifying all the radioactive waste at the site should be established, kept up to date and reviewed periodically.

804. The waste should be characterised at appropriate stages in terms of its physical, chemical, radiological and biological properties. The extent of the characterisation should be sufficient to enable properly informed decisions to be made in regard to its subsequent management and, in particular, decisions about its suitability for disposal. The safety case should take account of characterisation uncertainties.

805. Where fissile material is present in the waste, it may be appropriate to characterise waste streams according to their intrinsic neutron absorption properties. Assessments of permissible quantities of fissile material in these waste streams should take into account uncertainties in the level and distribution of fissile material, neutron absorbers and moderators within the waste.

806. Provision should be made for identifying, assessing and managing radioactive waste that does not meet existing process specifications or disposal criteria.

807. Decisions to mix waste streams need not be precluded if it can be properly justified and provide a net benefit in favour of safety or environmental factors including the later safe management of the waste through to disposal. Where radioactive waste is to be mixed with other wastes or materials, their mutual compatibility should be established in the safety case. Mixing of incompatible wastes should be prevented. Dilution of wastes solely to reduce their category should be avoided.

Storage of radioactive waste and passive safety

808. *The following principle addresses characteristics of the waste form and its storage facility, as both contribute to achieving passive safety. It is recognised that it will not be possible to meet this principle fully for all radioactive wastes without undertaking further retrievals and waste processing.*

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.		

809. The safety case should identify the operational limits and conditions (operating rules) needed for safe storage. These may include limits and conditions relating to:

(a) environmental conditions, including temperature, humidity, and contaminants;

(b) heat generation (from individual items or from the whole store);

(c) gas generation from packages (eg resulting in pressurisation, flammable mixtures, deformation);

(d) radiological or criticality hazards (eg taking account of on-site storage and long-term management, which may include disposal); and

(e) the monitoring, examination, inspection, maintenance and testing arrangements for the facility and its stored wastes.

810. The safety case should:

(a) align with the site's radioactive waste strategy (see Principle RW.1);

(b) demonstrate that radioactive waste is managed in accordance with relevant good practice and good engineering principles;

(c) justify the continued safe storage of the waste for the entire planned storage period;

(d) address all wastes stored in a facility, including waste for which further processing is planned, and waste already in a passively safe condition;

(e) justify the adequacy of the facility's structures, systems and components (including waste packages) and administrative safety measures in normal, fault and accident conditions; and

(f) explain the monitoring, examination, inspection, and testing arrangements for the facility and its stored wastes.

811. 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 condition.

812. Good engineering practice for storing radioactive waste includes the following elements:

(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 period of storage, or disposal.

(c) The waste should be immobile or immobilised.

(d) The need for active safety systems 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, maintenance, inspection and any refurbishment of the facility should take account of the entire planned storage period, including allowance for potential ageing and degradation (see Principle EAD.1 and subsequent principles).

(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 faults or accidents.

(k) Appropriate provisions should be made for dealing with any radioactive waste or its packaging that shows signs of unacceptable degradation.

813. The design of waste packages should aim to ensure that future management steps can be carried out, and that they are compatible with handling, retrieval, transport and storage requirements.

814. Each waste package should be uniquely identifiable through a marking system that is suitable for the entire planned storage period.

815. Acceptance criteria (which may include operating rules) should be established for admitting waste to the storage facility. These should take account of relevant factors and may include criteria for:

(a) storage, handling, and retrieval; and

(b) the overall management strategy, including disposal where appropriate.

816. The arrangements for implementing the acceptance criteria (eg examination, testing and auditing of packages and records) should cater for the safe management of any incoming radioactive waste that fails to meet the criteria.

817. Appropriate and sufficient capacity should be provided for the temporary storage of radioactive waste. This should include allowance for waste resulting from incidents. Planning should be in place for the provision of any further storage needs identified in the site's accident management strategies (see paragraph 771).

818. Where fissile material is present in the waste, the safety case should demonstrate sub-criticality margins appropriate for long-term storage, taking account of all uncertainties (see also paragraph 570 ff.).

Passive safety timescales

819. *The rationale for deciding when radioactive waste is processed into a passive safe state needs to be transparent and based on an appropriate balance of relevant factors.*

Radioactive waste management	Passive safety timescales	RW.6
Radiological hazards should be reduced systematically and progressively. The waste should be processed into a passive safe state as soon as is reasonably practicable.		

820. Factors that influence timing should include:

(a) worker and public risks, including from normal operations and accidents;

(b) environmental impact;

(c) security;

(d) the availability of disposal routes, the disposability of the waste (package), and the potential need for reworking;

(e) technical and logistical practicability;

(f) current and future wastes expected to be generated;

(g) interaction and dependencies between facilities and strategies (see Principle RW.1);

(h) possible burdens on future generations;

(i) maintenance of corporate memory and records;

(j) cost;

(k) the need to adopt a precautionary approach;

(l) ongoing or proposed research and development;

(m) the magnitude of the hazard;

(n) the current state and rate of deterioration of the waste, associated containers and packages, and existing storage facilities;

(o) removal of dependence on active safety systems, maintenance, monitoring and human intervention to ensure safety (see paragraph 812); and

(p) radionuclide decay or in-growth.

821. Where it is proposed to defer the processing of radioactive waste into a passive, safe state, the reasons for the deferral should be substantiated.

Records for management of radioactive waste

822. *In addition to the need for records to help to manage radioactive waste in the present, future generations will need to be provided with suitable information to manage, and eventually dispose of, the waste safely. Dutyholders will therefore need to make and maintain adequate records of the waste inventories and how it has been managed.*

Radioactive waste management	Making and keeping records	RW.7
Information that might be needed for the current and future safe management of radioactive waste should be recorded and preserved.		

823. The information recorded should include:

(a) details of the ownership of radioactive waste;

(b) relevant characteristics of the waste, which should include the radionuclide inventory, the amount of waste, its radioactive waste category, its physical, biological and chemical form, associated uncertainties in the estimates of the characteristics and, for waste containing fissile material, criticality-relevant information;

(c) the origin of the waste;

(d) its location on site, or within the storage facility;

(e) findings from research and development;

(f) details of the development of conditioning recipes and the specification of packaging criteria;

(g) details of packages;

(h) the operational history of processes and stores;

(i) records of non-compliance with specifications or acceptance criteria;

(j) records of waste disposals;

(k) the safety case(s) relevant to the waste and its storage;

(l) records of incidents;

(m) details of regulatory interactions; and

(n) any further records needed to support future permits under the Environmental Permitting Regulations (EPR10, in England and Wales) or authorisations granted under the Radioactive Substances Act (RSA93, in Scotland).

824. Licence Condition 32 requires records to be kept of radioactive wastes accumulated on licensed sites. These records should be maintained in a secure and accessible form for as long as the information could be of value. Records should be kept so that sufficient information will be readily identifiable to service both current and future needs for each individual waste package. Timescales for decommissioning, waste management and disposal will mean record keeping in excess of 100 years in many cases.

DECOMMISSIONING

825. *Licence Condition 35 requires licensees to make and implement adequate arrangements for decommissioning facilities on a nuclear licensed site. Although decommissioning is the last stage in the overall lifecycle of a facility, it needs to be taken into account at all stages in the lifecycle, starting at the planning and design stage*.

826. *These principles have therefore been written to apply to all stages in a facility's lifecycle. However, it is important that they are applied proportionately (see paragraph 27ff) across all the lifecycle stages.*

827. *As decommissioning proceeds the radiological hazards posed by a facility will eventually reduce, particularly once the bulk of the radioactive material is removed. There may, however, be a short-term increase in risk as a result of specific activities, such as those needed to retrieve radioactive material. Principle NT.2 (and paragraphs 759 ff.) provides general guidance on controlling such short-term risks and so will also be relevant here.*

Design and operation

Decommissioning	Design and operation	DC.1
Facilities should be designed and operated so that they can be safely decommissioned.		

828. Decommissioning and waste retrieval should be taken into account during the planning, design, construction and operational stages of a new facility or modifications of an existing facility, including:

(a) design measures to minimise activation and contamination etc;

(b) physical and procedural controls to prevent the spread of contamination;

(c) control of activation;

(d) design features to facilitate decommissioning and to reduce future 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; and

(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.		

829. The strategy should describe the significant assumptions and project risks associated with its achievement, and how these will be managed. The initial strategy should be produced during the planning stage of a new site or facility.

830. The overall strategy should:

(a) be consistent with Government policies and strategies, including 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, its associated risks and hazards, and anticipated decommissioning timescales;

(c) state the dutyholder's decommissioning policy and objectives; and

(d) encompass the full extent of the decommissioning liabilities on the site, including existing and planned facilities.

831. Interdependencies between facilities or between plants within facilities should be identified and taken into account. This should include interactions between any decommissioning and continuing facility operations.

832. The strategy should be integrated with other relevant strategies. Depending on the site, these might include strategies for:

(a) radioactive material, including nuclear matter (see Principle ENM.1) and radioactive wastes (see Principle RW.1);

(b) wider radioactive waste management and decommissioning, such as those set by the Nuclear Decommissioning Authority (NDA) and the Ministry of Defence (MOD);

(c) control and remediation of radioactively contaminated land (see Principle RL.1); and

(d) services, utilities and transport.

833. The strategy should describe the planned end state for the site.

834. 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 planned end-state.

835. The strategy should describe or refer to:

(a) the decommissioning options and the timescales considered;

(b) the reasons for selecting the chosen option(s); and

(c) the methodology for determining the relative priorities of decommissioning projects.

836. The strategy should take account of relevant factors, and show how these have been accommodated. These are likely to include the factors affecting the timing of decommissioning listed in paragraph 841. Other factors that should be taken into account include the magnitude of the remaining hazard, the duration of the work, the overall status of the facility, the availability of a 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 hazard.

837. If it is proposed to defer the decommissioning of a facility, the strategy should demonstrate that options for implementing earlier decommissioning will remain available and will not become technically foreclosed.

838. The strategy should be reviewed at appropriate intervals and kept up to date.

839. The management of decommissioning wastes should be covered by the radioactive waste management strategy (see Principle RW.1).

Timing of decommissioning

840. *The timing of decommissioning is an important aspect of decommissioning strategies and of significant interest to many stakeholders. Many factors can, however, influence this timing, not all of which will necessarily be within the control of the dutyholder (eg the availability of funding on sites owned by the NDA). Equally, prompt or early decommissioning may not be a viable option for technical or logistical reasons. The rationale for the timing of decommissioning therefore needs to be transparent and properly justified, taking all relevant factors into account.*

Decommissioning	Timing of decommissioning	DC.3
The safety case should justify the continuing safety of the facility for the period prior to its decommissioning. Where adequate levels of safety cannot be demonstrated, prompt decommissioning should be carried out and, where necessary, prompt remedial and operational measures should be implemented to reduce the risk.		

841. Decommissioning should be carried out as soon as is reasonably practicable, taking all relevant factors into account. Decommissioning should occur promptly where this is reasonably practicable. The timing of the decommissioning should be rigorously justified. Relevant factors which may apply in the period prior to decommissioning, during decommissioning, or both, will include:

(a) worker and public health and safety, including compliance with the Numerical targets (see paragraph 695ff);

(b) environmental impact;

(c) security;

(d) technical practicability;

(e) radionuclide decay or in-growth;

(f) ageing of facilities (see Principle EAD.2) and the potential for safety to degrade;

(g) the costs of different options, including care and maintenance and infrastructure costs;

(h) the volumes and categories of decommissioning wastes and the availability of interim storage facilities and 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 decommissioning and how this might affect achieving the facility or site's proposed end-state (see paragraph 878 ff.):

(j) interactions with and dependencies on other facilities or services;

(k) compatibility with site and national strategies (see Principles DC.2 and RW.1);

(l) the continuing maintenance of an appropriate safety management organisational structure, corporate memory and records;

(m) the continuing maintenance of site infrastructure;

(n) the availability of suitably qualified and experienced personnel;

(o) systematic and progressive hazard reduction (see Principle RW.6);

(p) uncertainties, including from climate change;

(q) the need to adopt a precautionary approach;

(r) possible burdens on future generations; and

(s) the potential for re-use.

842. Should decommissioning need to be deferred, then this should be explicitly justified in the safety case and strategy as appropriate. The safety case should limit the period of proposed deferment and demonstrate that the risks posed will be acceptable and properly controlled throughout. It should also justify how future safe decommissioning and the management of the resultant radioactive wastes will not be prejudiced by the deferment. The safety case should include all the activities needed to maintain the facility in a safe condition or to aid the eventual decommissioning.

Planning for decommissioning

843. Account needs to be taken, throughout the lifecycle of a facility, of its future decommissioning and to manage its wastes. This requires a strategy (see Principle DC.2) and a plan.

Decommissioning	Planning for decommissioning	DC.4
A decommissioning plan should be prepared for each facility that sets out how the facility will be safely decommissioned.		

844. The plan, including its supporting decommissioning programme, should form part of the demonstration that the facility can be safely decommissioned (see also Principle DC.9 on Decommissioning safety cases). If a plan is not already in place, one should be produced without undue delay. The plan and programme should be reviewed, developed and maintained up to date throughout the lifecycle of the facility.

845. The decommissioning plan should:

(a) define the planned decommissioning end-state for the facility and any interim states required to achieve it; and

(b) be supported by appropriate evidence to demonstrate that decommissioning can be undertaken safely and that the planned end-state (and any interim state) can be achieved.

846. The plan should be updated before the end of routine operations. This should include the results of a detailed characterisation survey performed to determine the extent and type of radioactive contamination, activation, waste and other materials in the facility. In the case of an unplanned early shutdown, the plan should be reviewed and, where necessary, updated without undue delay.

847. The type of information and level of detail contained in the plan should be commensurate with the type and status of the facility, its associated radiological hazard, its decommissioning timescales and the practicability of obtaining the information.

848. The plan should:

(a) optimise the use of existing facilities and plant during decommissioning;

(b) be used to ensure that these facilities and plant will be available when needed;

(c) address any changes to existing structures, systems or components needed for the decommissioning; and

(d) cater for any replacement or new facilities, plant, structures, systems or components that are needed; and

(e) be consistent with the planned end-state for the site.

849. The plan should identify and address the type and quantity of wastes to be managed (including solid, liquid and gaseous wastes) and the timescales over which the wastes will arise, and should be consistent with the waste management strategy (see Principle RW.1). The plan should provide information on the proposed treatment, packaging, storage and disposal of wastes.

850. Information and knowledge about the facility should be generated and maintained throughout its life so that this will be available to inform later detailed planning and during decommissioning (see Principle MS.2). In particular, this should include information relating to the design, modifications, operating history of the facility (including the impact of past operations and incidents) and operator knowledge.

851. If it is proposed to defer decommissioning, the plan should be developed sufficiently and relevant information preserved, so that the subsequent decommissioning can be undertaken safely.

Passive safety

852. *The following principle has been included for cases where decommissioning of a facility will be completed following a period of care and maintenance. Guidance on assessing the passive safe storage of radioactive waste is provided in paragraphs 808 ff.*

Decommissioning	Passive safety	DC.5
Facilities should be made passively safe before entering a care and maintenance phase.		

853. Bulk process materials including fissile material, process liquors and operational wastes should normally be removed from the facility.

854. The facility should undergo post-operational clean out. This should include:

(a) the removal of any residual radioactive material;

(b) the immobilisation of any potentially mobile radioactive material that cannot be removed, taking account of waste management compatibility and future decontamination; and

(c) the removal of any readily removable contaminated or activated items.

855. The facility, or parts of the facility, should be decontaminated where appropriate, eg to reduce risks or to produce waste of a lower waste category.

856. Before starting a care and maintenance phase, an operating regime should be established to cater for any ongoing maintenance, examination, inspection and testing at the facility. The regime should be designed:

(a) to minimise the need for active safety systems;

(b) to minimise monitoring needed in the interests of safety; and

(c) so that there is no need for prompt intervention to maintain the facility in a safe condition.

857. Access to the facility should be controlled and entry points provided for response to incidents. Provision should be made to prevent access by flora and fauna etc.

858. The storage of any remaining radioactive material within the facility should follow the paragraphs supporting Principle RW.5.

Records for decommissioning

859. *Licence Condition 6 requires licensees to make and preserve adequate records to demonstrate compliance with licence conditions. This requirement includes records associated with decommissioning. It may be necessary for decommissioning operations to involve two or more separate phases, spanning a number of decades. The records required for decommissioning operations, in both the short and long term, need therefore to be generated and retained over appropriate timescales, and in a manner and form that allows them to be utilised when needed.*

Decommissioning	Records for decommissioning	DC.6
Documents and records that may be required for decommissioning purposes should be identified, prepared, updated, retained and owned so that they will be available when needed.		

860. The process of making and preserving these documents and records should start at the planning and design stage and continue throughout the whole lifecycle of the facility. Particular attention should be given to records relating to:

(a) the as-built facility design and subsequent modification;

(b) its operational history (including information from operator knowledge, see paragraph 850);

(c) incidents, accidents and unusual occurrences;

(d) radiological surveys;

(e) radioactive material (eg quantities, locations, condition and ownership) with specific focus on the inventory at the end of routine operations (see also Principle RW.7);

(f) the safety case;

(g) regulatory interactions;

(h) the physical condition of the facility, including examination, inspection, maintenance and testing records; and

(i) the decommissioning history, including decommissioning reports and records, ie documentation which shows how the objectives of the decommissioning plan, including the planned end-state for the facility, were achieved.

861. 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.

Decommissioning organisation

862. *Decommissioning can be a time of considerable change for an organisation and its personnel, particularly during the transition from routine operations. 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 Principles MS.2 and EHF.8 and their supporting guidance.*

Decommissioning	Decommissioning organisation	DC.7
Organisational arrangements should be established and maintained to ensure safe and effective decommissioning of facilities.		

863. 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 (see also paragraph 63).

864. Suitable and sufficient capability to function as an intelligent customer should be demonstrated for work carried out by contractors (see paragraph 66).

865. The 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 (see Principle EHF.8).

Management system

866. *The following principle has been provided because the facility's (or site's) management arrangements will likely need to be modified during the course of the decommissioning to reflect the progressively changing state of the facility (or site).*

Decommissioning	Management system	DC.8
The management system should be reviewed periodically and modified as necessary prior to and during decommissioning.		

867. General guidance for assessing the adequacy of management systems in respect of safety is provided in paragraphs 60 and 61. During decommissioning, the facility's (or site's) management system should be modified to reflect changes to facilities and their associated risks and hazards. Any modifications should be substantiated before implementation.

868. Particular aspects for consideration should include the management of:

(a) safety function categorisation of structures, systems and components and administrative controls (see Principle ECS.1);

(b) examination, inspection, maintenance and testing arrangements;

(c) on-site and off-site emergency plans;

(d) on-site and off-site monitoring programmes;

(e) radioactive and other hazardous waste management arrangements; and

(f) the number of staff and contractors working at the facility and the nature of their work.

Decommissioning safety case

869. *General guidance for assessing safety cases is provided in the section on The regulatory assessment of safety cases (paragraph 79 ff.). This has been supplemented in the following section to highlight particular aspects important to decommissioning. These include the need to keep the safety case up to date during the decommissioning with the changing state of the facility and its radiological hazards and risks; and because conventional (non-radiological) risks can often affect how decommissioning activities are undertaken.*

Decommissioning	Decommissioning safety case	DC.9
A safety case should be provided to demonstrate the safety of the decommissioning plan and its associated decommissioning activities and then kept up to date as the work progresses.		

870. Guidance for assessing decommissioning plans is provided in DC.4. An outline decommissioning safety case should be prepared in conjunction with the updated decommissioning plan prior to the end of routine operations (see paragraph 846) and then suitably developed before the decommissioning commences.

871. Where decisions on managing radiological risks are affected by conventional risks (eg from cutting, dismantling and demolition), the safety case should justify how overall risks are reduced so far as is reasonably practicable. In such cases, decommissioning activities may need to balance radiological and conventional risks (see paragraph 18).

872. The effect of decommissioning activities on adjacent plant and safety-related services should be taken into account in the safety case.

873. Decommissioning activities may need to increase risks temporarily (for example, remedial work, equipment installation or radioactive waste retrievals) in order to achieve a reduction in the longer-term risk. The safety case should justify such increases in terms of the overall risk reduction to be achieved by the decommissioning. Principle NT.2 provides general guidance on assessing short-term risks and how these should be managed.

874. Where the prevailing risks are high (eg the risk prior to decommissioning is approaching or exceeds a basic safety level, see paragraph 698 ff.), the safety case should justify explicitly why the decommissioning cannot be completed more quickly and/or sooner. The activities proposed in such cases should reflect the prevailing risk levels.

875. The depth and rigour of the decommissioning safety case should be proportionate to the associated radiological risks and hazards. Particular focus should be given to demonstrating the safety of any new or unusual activities or circumstances arising during decommissioning.

876. The safety case should be updated at appropriate points during the decommissioning to reflect changes made to the facility and the risks and hazards it poses.

877. Where information about the state of a facility or its contents is incomplete to an extent that producing an adequate safety case in advance of decommissioning activities is impossible, a managed process should be adopted that allows the necessary information to emerge in a controlled manner. In such cases, the safety case should be staged to enable the decommissioning to progress safely.

LAND QUALITY MANAGEMENT

878. *The principles in this section are concerned with the safe management of radioactively contaminated land on nuclear licensed sites. ONR treats radioactively contaminated land and emplaced radioactive material as accumulations of nuclear matter, unless they are, or arise from, authorised disposals. The principles apply both to the ongoing control and remediation of contaminated land and to activities undertaken in preparation for achieving the site's final end-state. They need to be applied in a proportionate manner.*

879. *The environmental regulators are responsible for the regulation of disposals on, and from, licensed sites in accordance with the Environmental Permitting Regulations (EPR10, in England and Wales) or the Radioactive Substances Act (RSA93, in Scotland), and for the regulation of other environmental legislation. The principles therefore need to be applied in a manner that is in accordance with the relevant Memoranda of Understanding (see Annex 1).*

Strategies for radioactively contaminated land

Land quality management	Strategies for radioactively contaminated land	RL.1
A strategy should be produced for the control and remediation of any radioactively contaminated land on the site.		

880. The strategy, which should be integrated with other related strategies (eg for radioactive waste (Principle RW.1) and decommissioning (Principle DC.2)), should cater for all known and suspected instances of radioactive contamination on the site.

881. The type of information and level of detail within the strategy should be commensurate with the extent, nature and hazard potential of the radioactive contamination.

882. The strategy should:

(a) be consistent with Government policy, including the Government's overall policy aims on sustainable development;

(b) include arrangements for identifying any restrictions necessary to protect people and the environment;

(c) include a process for considering options for the management of the radioactively contaminated land;

(d) be supported by a plan that sets out how the strategy will be delivered (Principle RL.6); and

(e) be subject to appropriate stakeholder engagement.

883. The strategy should describe, or refer to, the options and timescales that were considered during its development and substantiate those chosen. The optioneering process should take account of the factors that might have a bearing on the management of radioactively contaminated land, for example:

(a) worker and public safety, including individuals and groups who may currently be exposed, those who may be exposed as a result of control and remediation actions, and those potentially exposed in the future;

(b) avoiding or reducing any environmental impact now or in the future (including the potential for contamination to spread);

(c) waste minimisation (see Principle RW.2);

(d) the results and reliability of survey, investigation, monitoring, surveillance and characterisation work (see Principles RL.4 and RL.5);

(e) continuing radioactive contamination from known sources;

(f) the availability of waste processing and disposal routes, including technical practicability aspects;

(g) costs;

(h) future requirements for surveys, investigation, monitoring, surveillance and characterisation (see Principles RL.4 and RL.5);

(i) interaction and dependencies with other facilities and other areas of radioactive contamination on the site;

(j) the effectiveness of control and remediation measures;

(k) possible burdens on future generations;

(l) the maintenance of corporate memory and records;

(m) the need to adopt a precautionary approach;

(n) plans for the future use of the site (or parts of the site);

(o) the biological, chemical and other hazards relating to the radioactively contaminated land;

(p) incidents, accidents and unusual occurrences at the site and the management actions taken to address these, eg the clean-up of any spills or other known contamination events;

(q) the natural radioactive decay of specific radionuclides to safe levels, or levels resulting in a lower category of waste for disposal; and

(r) how to achieve the final end-state.

884. The strategy should describe the licensee's policy and objectives for the management of radioactively contaminated land from the present through to the final end-state. In order of preference, the strategy should aim to:

(a) remove where appropriate radioactive material for appropriate management;

(b) establish measures to achieve in-situ stabilisation; or

(c) prevent (or where this is not practicable, minimise) the migration of contamination on site. This will minimise both future waste volumes and the potential for contamination to spread off site.

885. The strategy should define and substantiate the proposed end-state(s) and any interim state(s) for contaminated land on the site, and set out the anticipated timescales to achieve these.

886. The strategy should describe the means by which the radioactively contaminated land will be controlled and remediated to achieve the end-states. This may involve remedial work at various times, or leaving the land in situ where justified. Any proposed restrictions related to the end-states should be described.

887. The strategy should describe the significant assumptions and project risks associated with its achievement, and how these will be managed.

888. The strategy should be reviewed and kept up to date.

Actions to identify radioactively contaminated land

889. *This principle relates to the need for licensees to understand the extent and nature of radioactive contamination on and around the licensed site.*

Land quality management	Identifying radioactively contaminated land	RL.2
Steps should be undertaken to identify any areas of radioactively contaminated land on or adjacent to the site.		

890. A programme of surveys, investigation, monitoring, surveillance and analysis should be in place to establish the nature and extent of radioactively contaminated land.

891. The programme should be proportionate, taking account of the current and previous uses of the site (or areas of the site) and any previous incidents, leaks, or accidents that are known or suspected.

Discovery of contaminated land and management of leaks and escapes

Land quality management	Discovery of contaminated land and management of leaks and escapes	RL.3
Arrangements should be in place to ensure that leaks and escapes giving rise to radioactive land contamination are promptly identified and controlled.		

892. The arrangements should ensure that:

(a) the source of the radioactive contamination is established;

(b) any ongoing leakage or escape is terminated or minimised, and measures are taken to avoid any recurrence;

(c) the escaped radioactive material and/or contamination is recovered, where appropriate;

(d) an appropriate management strategy is developed and implemented for remaining radioactive contamination;

(e) any radioactive material or contamination does not disperse and generation of radioactive waste is minimised;

(f) restrictions to protect people and the environment are implemented;

(g) the leakage or escape is notified, recorded, investigated and reported in accordance with the requirements of Licence Condition 34; and

(h) the relevant environmental regulator is informed.

Characterisation of radioactively contaminated land

893. *General guidance for assessing the characterisation of radioactive waste is provided under Principle RW.4. In addition, the following principle also applies here.*

Land quality management	Characterisation of radioactively contaminated land	RL.4
Radioactively contaminated land should be characterised to facilitate its safe and effective control and remediation.		

894. Characterisation of radioactively contaminated land should seek to obtain the information needed for its future management. Examples include:

(a) the source of the contamination;

(b) the location of contamination;

(c) volumes;

(d) radionuclide 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, groundwater flows, geological structure and rock fractures;

(i) whether the contamination is recent or 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; and

(l) other potential effects including commercial impacts.

895. The characterisation should include the taking and analysis of soil, rock etc and groundwater 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

Land quality management	Survey, investigation, monitoring and surveillance	RL.5
Radiological surveys, investigation, monitoring and surveillance of radioactively contaminated land should be carried out such that its characterisation is kept up to date.		

896. The objectives of these activities should be defined, and may include:

(a) confirmation of the extent and nature of the contamination;

(b) establishing rates of migration;

(c) evaluation of the effectiveness of management measures;

(d) confirmation of continued compliance with the safety case; and

(e) ensuring consistency with the site's radioactive waste management strategy (see Principle RW.1).

897. The arrangements for, and frequency of, surveys, investigation, monitoring and surveillance should take account of:

(a) the extent, nature and hazard potential of the radioactive contamination;

(b) uncertainties in the characteristics of the contaminated land;

(c) the extent to which the properties of the contaminated land may be changing;

(d) the proximity to the site boundary; and

(e) dose uptake to those undertaking the work.

898. These arrangements should be subject to review and modified to reflect changes in circumstance.

Plan for control and remediation

Land quality management	Plan for control and remediation	RL.6
A plan should be prepared and implemented for the safe control and remediation of radioactively contaminated land and should be subject to appropriate stakeholder engagement.		

899. The plan should implement the site's strategy (see Principle RL.1) for achieving the proposed end state of the site, or area of the site and any interim states required to achieve it.

900. The type of information and level of detail contained within the plan should be commensurate with the extent, nature and hazard potential of the contamination, and

the time remaining before implementation. Plans prepared well ahead of implementation (eg in the early lifecycle stages of the facility) should be subject to regular review so that they are kept up to date and become increasingly detailed as the time for their implementation approaches.

901. The plan should identify the areas of contaminated land to be managed and the type and quantity of radioactive material or items present. This information should be substantiated by safety and environmental analyses of surveys (etc) used to characterise the land (see Principles RL.4 and RL.5).

902. The plan should identify the proposed means for controlling or remediating the contaminated land to achieve the proposed end-state, for example:

(a) in-situ monitoring;

(b) excavation;

(c) in-situ or ex-situ treatment for removal of contamination;

(d) in-situ stabilisation;

(e) surface caps or covers;

(f) natural or artificial containment barriers;

(g) existing hydrogeological controls;

(h) engineered hydraulic controls;

(i) groundwater treatment;

(j) control of personal access;

(k) control of local flora and fauna; and

(l) other restrictions necessary to protect people and the environment.

903. The plan should identify the type and quantity of radioactive waste arising and how this will be managed. These aspects of the plan should be consistent with the site's waste management strategy (see Principle RW.1).

904. The plan should include survey, investigation, monitoring, surveillance and analysis activities to measure the extent and levels of contamination both before and after remediation. The effectiveness of these activities should be substantiated, for example in regard to their suitability to demonstrate that specified end-states have been achieved.

Records for radioactively contaminated land

Land quality management	Records for radioactively contaminated land	RL.7
Arrangements should be made and implemented for recording and preserving information needed for the safe and effective control and remediation of radioactively contaminated land now and in the future.		

905. The arrangements should include the following types of record:

(a) records from surveys, investigation, monitoring and surveillance work and the analysis of their results;

(b) records concerning the processes used in deciding management options and the setting of strategies;

(c) records of any incidents, leakages or accidents resulting in radioactively contaminated land, and of the management actions taken in response;

(d) reports on the remediation of contaminated land;

(e) relevant information related to the history and use of the site; and

(f) aspects listed in paragraph 823 (radioactive waste records) relevant to contaminated land.

Safety cases for radioactively contaminated land

906. *General guidance for assessing safety cases is provided at paragraph 79 ff. This section provides specific additional guidance on safety cases for radioactively contaminated land.*

Land quality management	Radioactively contaminated land safety cases	RL.9
A safety case should be provided to demonstrate the safety of the plan for managing radioactively contaminated land and its associated control and remediation activities. The safety case should be kept up to date as the work progresses.		

907. Guidance on assessing plans for managing radioactively contaminated land is provided under Principle RL.6. The safety case should be proportionate to the extent, nature, risks and hazards posed by the contamination and its spread or potential to spread. It should include all aspects of how the contaminated land, or its management might affect safety on the site, eg where the presence of contamination near a facility might impact the safety of its operations. Where conventional (non-radiological) hazards such as biological or chemical hazards affect how the radioactively contaminated land will be managed, the overall balance of risks should be justified (see paragraph 18).

908. Information contained in the safety case should include, where relevant:

(a) details of the extent and nature of the radioactively contaminated land, and geological and hydrogeological conditions, taking account of survey, investigation, monitoring and surveillance results and their analysis (see Principles RL.4 and RL.5);

(b) a demonstration that modern standards and good engineering practice will be applied;

(c) an assessment of potential harm and risks, taking account of all environmental pathways and including assessment uncertainties. Environmental pathways might include personal contamination, and direct

radiation exposure to airborne or waterborne activity within and beyond the site boundary;

(d) identification and substantiation of any restrictions needed to protect the public, workers or the environment (operating rules);

(e) future survey, investigation, monitoring and surveillance arrangements (including sampling devices and the location of boreholes); and

(f) a description of how any requirements of the relevant environmental regulator or of environmental law will be met.

Construction on radioactively contaminated land

Land quality management	Construction on radioactively contaminated land	RL.8
Radioactively contaminated land should be remediated and controlled as appropriate before any construction of new facilities upon it.		

909. Where new facilities are proposed on, or in the vicinity of, a licensed site:

(a) the vicinity of the proposed construction site should be surveyed to establish if there is any radioactive contamination;

(b) any radioactively contaminated land should be remediated to appropriate standards prior to construction commencing upon it;

(c) any construction in a location that would impede the control and remediation of radioactively contaminated land should be avoided; and

(d) any proposal not to remediate prior to construction should be supported by a demonstration that alternative options are not reasonably practicable.

ANNEX 1: ONR 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 ONR most frequently interface with during assessment are listed in this annex, together with details of the nature of the regulatory interface.

The Health and Safety Executive

The Health and Safety Executive (HSE) is one of the regulatory organisations for the Health and Safety at Work etc Act 1974 (HSWA), and is the enforcing authority for most work related industrial activities in Great Britain. However, ONR is specifically the enforcing authority for HSWA for nuclear licensed sites (termed GB Nuclear Sites in the Energy Act 2013), defence related nuclear sites, associated warship berths (for IRR99 and REPPIR), the wider construction site for new nuclear build sites, and the supply chain for equipment to be used exclusively or primarily on nuclear sites. ONR enforces HSWA as it relates to safety in the nuclear context for these sites and activities, and also more widely as it relates to conventional safety matters. ONR has a close working relationship with HSE to ensure consistent enforcement of this legislation within Great Britain, and also to ensure that good regulatory practice is shared between the organisations. ONR may on a case by case basis use expertise from HSE to assist with its regulatory activities, and in some cases may directly provide HSE inspectors with ONR warrants such that they could exercise HSWA powers on sites and for activities where ONR is the enforcing authority, subject to ONR's policies and guidance.

Environment Agency/Scottish Environment Protection Agency/Natural Resource Wales

ONR is responsible for regulating nuclear safety, including the safe management, conditioning and storage of radioactive waste on nuclear licensed sites. The Environment Agency, Scottish Environmental Protection Agency (SEPA) and Natural Resources Wales (NRW)[6] are responsible in England, Scotland and Wales, and in Scotland respectively, for regulating the discharges to the environment and disposal of radioactive waste on or from nuclear licensed sites.

ONR, EA, SEPA and NRW have a number of areas of mutual interest, including:

(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 wastes;

(c) permitting or authorisation of radioactive discharges and waste disposals;

(d) decommissioning and de-licensing of existing facilities, including Quinquennial Reviews;

(e) ONR's Periodic Safety Reviews;

(f) EA/SEPA/NRW's Periodic Permit or Authorisation Reviews;

[6] The Environment Agency's responsibilities for regulating nuclear sites in Wales passed to a new body, Natural Resources Wales, on 1 April 2013

(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: ONR'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 and NRW's responsibilities being centred on the regulation of discharges and disposals from normal operations including decommissioning.

Separate, but similar, Memorandums of Understanding (MoU) provide frameworks for the ways of working, and the interaction between ONR and each of the environmental regulators.

The Defence Nuclear Safety Regulator

The Defence Nuclear Safety Regulator (DNSR) is the MoD regulator of nuclear and radiological safety for the Defence Nuclear Programme (DNP) comprising of the Naval Nuclear Propulsion Programme and the Nuclear Weapons Programme with a responsibility for regulating those aspects of the DNP 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, that standards of nuclear and radiological safety throughout the DNP are, so far as reasonably practicable, at least as good as those required by legislation in the civil sector. In carrying out this role, DNSR works very closely with the relevant statutory regulators, particularly ONR (including ONR's Radioactive Materials Transport Team), EA and SEPA, and similarly empowered Defence Regulators.

DNSR has introduced a system of Authorisation of dutyholders in direct control of nuclear activities within these programmes, which closely parallels ONR's licensing system. Authorisation provides scope for a similar permissioning regime to DNSR as that afforded to ONR by the licence conditions. Compliance with Authorisation Conditions provides assurance that the Secretary of State's Policy Statement for health, safety and environmental protection in defence is being complied with.

Accordingly, ONR and DNSR have agreed to work together to regulate the defence nuclear programmes to:

- Maximise the effectiveness of joined up regulation.
- Minimise the duplication of regulatory resource by recognising each other's differing but complementary responsibilities.
- 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 (now ONR) and DNSR and the joint regulatory framework. These are both currently under revision and a new MoD/ONR agreement and ONR/DNSR Letter of Understanding is being developed.

ANNEX 2: BASIS AND DERIVATION OF NUMERICAL TARGETS

This annex explains the basis and derivation of the Numerical targets set out in the section starting at paragraph 695. It is based on the Explanatory Note prepared to accompany the issue of the 2006 SAP. The technical content of the annex is largely unchanged from the Explanatory Note, though the opportunity has been taken to improve the explanation in places.

Introduction

A1. Following comments, questions and requests for clarification raised during the stakeholder engagement on the 2006 SAPs, an Explanatory Note was written to explain the background and basis for ONR's Numerical targets, and in particular those that were new in the 2006 SAPs. The Note also provided clarification of some of the terms used and reasons for the reductions in several of the Basic Safety Levels (BSLs) and Basic Safety Objectives (BSOs) compared to the 1992 SAPs.

A2. Most of the targets are not mandatory. However, some of the BSLs are legal limits in the Ionising Radiations Regulations 1999 (IRR99). They are identified as BSL(LL).

BACKGROUND CONSIDERATIONS

BSL/BSO

A3. The BSLs and BSOs translate the Tolerability of Risk (TOR, Ref. 2) framework written to guide decision making by inspectors. ONR policy is that the BSLs indicate doses/risks which new facilities should meet and they provide benchmarks for existing facilities (see paragraph 699). It is important to recognise that the BSO doses/risks have been set at a level where ONR considers it not to be a good use of its resources or taxpayers' money, nor consistent with a targeted and proportionate regulatory approach, to pursue further improvements in safety. In contrast, facility operators and owners have an overriding duty to consider whether they have reduced risks to as low as reasonably practicable (ALARP) on a case by case basis, irrespective of whether the BSOs are met. As such, it will in general be inappropriate for operators (etc) to use the BSOs as design targets, or as surrogates to denote when ALARP levels of dose or risk have been achieved. Although ALARP is the commonly used term, the legal phrase is So Far As Is Reasonably Practicable (SFAIRP).

Occupational dose trends in normal operation

A4. There has been a sustained downward trend in occupational doses since the early 1990s. When the 1992 SAPs were reviewed and updated in 2006, average doses were significantly lower than when the previous targets were set. According to statistics from the Central Index of Dose Information ((CIDI), Refs. 15 and 16), average doses in the nuclear industry reduced by more than a factor of three during the period 1992-2004. In consequence, a number of the BSO levels were reduced to reflect this trend. It is important to note that these reductions in the BSO levels were not prompted by reviews of risk estimates, which did not change significantly.

Dose Estimates

A5. In estimating doses for comparison with these targets, all relevant sources of ionising radiation should be considered. If the target is a site target, all sources on the site should be included, not just those in a particular facility. Where relevant, the dose contribution from any authorised discharge of radioactivity arising from planned

operations should also be taken into account. Natural background radiation should however be omitted from the dose estimates, although radon may require consideration. The sources of interest are those that are introduced to the site by man for the purposes of work with ionising radiation, or that result from such work.

NUMERICAL TARGETS FOR FAULT ANALYSIS

A6. The Fault Analysis section of the SAPs describes three forms of analysis used to establish the safety case for fault and accident conditions, namely design basis analysis, probabilistic safety analysis and severe accident analysis. These all provide important qualitative and complementary inputs to the design, operation and emergency preparedness of the facility. The results of the fault analysis are also quantitative; these aspects should be judged against the SAPs' numerical targets (Principle NT.1). The targets to be applied and their basis are described in the following paragraphs.

Design Basis Analysis (DBA)

A7. Principle FA.4 seeks DBA that provides a robust demonstration of the fault tolerance of the engineering design and the effectiveness of the safety measures. This means having high confidence that there will be no significant radiological consequences, either off the site or on the site, from any reasonably foreseeable event. The SAPs ask for this to be achieved by the provision of safety measures to prevent or terminate fault sequences before exposure to direct radiation or any release/significant unintended relocation of radioactive material occurs. If this cannot be achieved, the safety measures should mitigate the radiological consequences of such fault sequences (Principle EKP.5)

A8. DBA is focussed on the key safety measures for those initiating events that are most significant in terms of frequency and unmitigated potential consequences. Paragraph 635 sets out qualitative success criteria that these safety measures should ideally achieve in a design basis fault sequence (in accordance with the conditions specified in paragraphs 630 to 634). These qualitative criteria are interpreted numerically in the BSOs of Target 4, which is set in terms of mitigated radiological doses (ie those following successful application of the safety measures). Target 4 also provides advice to inspectors in cases where it is demonstrated that it is not reasonably practicable to provide safety measures that meet the BSO by setting BSLs (again set in terms of mitigated radiological doses). Since DBA is intended to provide a robust demonstration of the fault tolerance of the engineering design, the associated consequence calculations should be carried out applying a conservative methodology; the BSOs and BSLs in Target 4 have been set on this basis.

A9. Experience with the 1992 SAPs indicated that strict application of the DBA criteria as defined by P20-27 of the 1992 SAPs was disproportionate for many facilities containing radioactive material in smaller quantities and with less dispersion potential than power reactors. P16 of the 1992 SAPs called for all initiating faults with a "significant" consequence to be considered, and P21 of the 1992 SAPs called for all those with initiating fault frequencies greater than 1×10^{-5} pa to be included in the DBA. We therefore clarified this in the 2006 SAPs by introducing explicit dose thresholds to guide inspectors on the meaning of "significant" in different contexts. Principle FA.5 defines these thresholds with reference to Target 4 (see paragraph 628 (d)) so that faults deemed significant enough to warrant DBA are those whose unmitigated consequences (ie those that would arise in the absence of

safety measures or other interventions, calculated on a conservative basis) exceed a Target 4 BSL.

A10. Target 4 is thus intended to be applied in two different ways:

(a) Firstly, DBA should be employed for any qualifying fault sequence whose *unmitigated* consequences could exceed a Target 4 BSL. This sets ONR's expectations for where and when DBA should be undertaken.

(b) Secondly, the results of the DBA, namely mitigated dose consequences as a function of initiating fault frequencies, should be compared with the relevant BSOs and BSLs. This comparison should then be used to assist judgements on the type of assessment to be performed and the regulatory approach to be followed (see paragraphs 698 to 701).

The basis for the numerical values used in Target 4 is described below.

Probabilistic Safety Analysis (PSA)

A11. PSA looks at a wider range of fault sequences than DBA. For example, it includes sequences where there are additional failures in the safety measures over and above those specified in paragraphs 630 to 633, and initiating faults excluded from the DBA by virtue of paragraph 628. PSA 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 651. 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 (see paragraph 655). The PSA results can be grouped to give estimates of the frequency of occurrence of consequences within specified ranges of dose, both on the site and off the site. Targets 6 and 8 provide BSOs and BSLs for individual fault sequences, and in the case of Target 8, also for summed frequencies for all faults affecting a single facility. Similarly, Targets 5 and 7 provide BSLs and BSOs for the overall (summed) risk impact to individuals from all the facilities on a site.

A12. The BSLs and BSOs in Targets 5 to 8 have been set at a level judged appropriate for a full-scope PSA (ie one in which all qualifying faults at the site/facility are included). If a reduced-scope PSA is to be assessed then these BSLs and BSOs will need to be adjusted accordingly. Similarly, inspectors may need to apply other adjustments to these targets to take account of aspects of the licensee's methodology that differ from what was assumed when setting these targets (see paragraphs 703 and 738).

Severe Accident Analysis (SAA)

A13. The third element of the fault analysis, severe accident analysis, considers significant but unlikely accidents and provides information on their progression and consequences, within the facility, on the site and also beyond the site boundary. This is used, for example, to inform emergency response measures that could be taken to limit doses. The SAA forms an input to the PSA, and thus there is no separate Numerical target specific to SAA. However the SAA will be particularly important in assessing the overall impact of the site in terms of the risks of major accidents that could lead to significant societal effects. This is addressed in Target 9 on societal risk.

TARGETS

Normal operation

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 (IRR99). Normal operational doses should also be reduced ALARP.*	

A14. This target, which relates to normal operation doses, was updated in 2006 from P11 in the 1992 SAPs. Some of the terms were changed, for example reference is made to 'employees working with ionising radiation' and 'other employees' in order to be more consistent with IRR99.

Employees working with ionising radiation

A15. 'Work with ionising radiation' has the same interpretation as in IRR99. Employees involved with such work are likely to require regular and frequent access to areas where they are exposed to ionising radiation or where special precautions are required to restrict their exposure and their dose can be continuously monitored to ensure they are within the legal limits. Such employees are regarded as 'employees working with ionising radiation'.

A16. The BSL value of 20 mSv pa for employees working with ionising radiation is the IRR99 annual dose limit for employees and is denoted by BSL(LL). Using the currently accepted risk/dose value of 4% per Sv for a working population, the value of 20 mSv equates to an annual risk of death of 8×10^{-4} pa, which is slightly lower than 1×10^{-3} pa proposed in Reducing Risks, Protecting People (R2P2, Ref. 1) as the limit of tolerability for the risk to workers from all sources. R2P2 remains the basis of ONR's risk policy.

A17. R2P2 sets the corresponding broadly acceptable risk level at 1×10^{-6} pa. This value equates to an annual dose of 0.025 mSv, which is well below dose levels that would normally be reasonably practicable for employees working routinely with ionising radiation. Recognising this, the BSO was set in the 1992 SAPs at 2 mSv pa. However, this was reduced to 1 mSv pa in 2006, in view of the trends in dose reduction discussed earlier. It remains ONR's view that a BSO of 1 mSv pa is representative of a level of dose that is consistent with the ALARP principle. This view is held, even though 1 mSv pa equates to a fatality risk of about 4×10^{-5} pa, which exceeds the broadly acceptable level of risk proposed in R2P2.

Other employees on the site

A18. 'Other employees on the site' are people who work on sites where work with ionising radiation is carried out, but who do not normally participate in such activities. These include, for example, employees who would not normally enter radiation controlled areas, or who would not be required to take special precautions to restrict their exposures to ionising radiation, eg by wearing personal protective equipment.

A19. Paragraph 60 of the Approved Code of Practice (ACoP, Ref 12) for IRR99 states that particular steps should be taken to restrict the exposures of any employees who would not normally be exposed to ionising radiation in the course of their work, and that dose control measures should make it unlikely that such persons would receive a dose greater than 1 mSv pa. The BSL is therefore set at 2 mSv pa; a value which should readily accommodate the unlikely doses greater than 1 mSv pa, and below which reasonably practicable dose control measures should be capable of restricting exposures.

A20. The BSO for 'other employees on the site' has been set to be significantly lower than 1 mSv pa (the BSO for employees working with ionising radiation) and also lower than 0.5 mSv pa (the corresponding BSO in the 1992 SAPs) to reflect the downward dose trends described above. The value chosen, 0.1 mSv pa is a factor of 20 below the BSL and corresponds to an annual risk of fatality of 4×10^{-6} pa. This is broadly in line with the risk level (1×10^{-6} pa) proposed in R2P2, and is considered appropriate given the conservatisms that are often included in dose estimates of this sort.

Other persons on the site

A21. In the 1992 SAPs there is reference in P11 to members of the public. The dose limit for 'other persons' (see Schedule 4 of IRR99) also applies to members of the public whether they are on or off the site and therefore no additional limit is specified for members of the public on the site. As it is unlikely that a member of the public would be on a site to the extent that this would influence facility design or operation, we consider it more appropriate for doses to such persons to be controlled by management arrangements (see paragraph 715).

Defined groups of employees

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	

A22. Collective dose budgets are often determined at the design stage and, combined with the estimated number of employees working with ionising radiation, provide information on the average doses to defined groups of employees. Although there are no IRR99 limits for the average dose received by a group of employees, such doses should nevertheless be constrained to less than the maximum dose of an individual employee. The BSL and BSO values are therefore set at 10 mSv pa and 0.5 mSv pa respectively, ie half the values for individual employees working with ionising radiation in Target 1. This BSL is unchanged from the 1992 SAPs, where it was set based on TOR. The BSO has however been reduced in line with reducing dose trends as explained above.

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 (IRR99).*	

A23. A person off the site is regarded as any person outside the site where the facility being assessed is situated.

A24. The BSL is set at 1 mSv pa, which is the IRR99 dose limit for 'other persons' (see above) and as such is denoted by BSL(LL). This dose equates to a fatality risk of 5×10^{-5} pa (based on 5% per Sv for members of the general population) which, although more demanding than the analogous fatality risk of 1×10^{-4} pa proposed in R2P2, retains the value used in the 1992 SAPs.

A25. The BSO (0.02 mSv pa) is also unchanged from the 1992 SAPs. It equates to the 1×10^{-6} pa level proposed in R2P2 as the broadly acceptable risk to an individual of dying from a particular cause. Though this is a relatively low dose rate, evidence to the 1990 Hinkley Point 'C' Public Inquiry (Ref. 13) suggests it corresponds to an ALARP level for new facilities on 'green-field' sites. This BSO is therefore appropriate for new facilities designed to modern standards, although a less onerous ALARP level may be more realistic on multi-facility sites with older facilities.

A26. Where there are multiple sites in close proximity, it is important to ensure that the overall dose to persons near these sites is below the relevant IRR99 limits. For this reason, a suitable dose constraint should be applied to each site. In cases where there is more than one employer, they should co-operate to derive suitable constraints for their respective sites (see Regulation 8(3) and 15 of IRR99). Public Health England (which includes the former National Radiological Protection Board) has recommended that the "constraint on optimisation for a single new source" should not exceed 0.3 mSv pa. ONR considers that a single source should be interpreted as a site under a single duty holder's control, in that it is an entity for which radiological protection can be optimised as a whole.

Fault Analysis

Design Basis Analysis

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 1×10^{-3} pa 200 mSv for initiating fault frequencies between 1×10^{-3} and 1×10^{-4} pa 500 mSv for initiating fault frequencies between 1×10^{-4} and 1×10^{-5} pa BSO: 0.1 mSv **Off site:** BSL: 1 mSv for initiating fault frequencies exceeding 1×10^{-3} pa 10 mSv for initiating fault frequencies between 1×10^{-3} and 1×10^{-4} pa 100 mSv for initiating fault frequencies between 1×10^{-4} and 1×10^{-5} pa BSO: 0.01 mSv	

A27. The conceptual background for this target is explained in paragraph A7 ff. The off-site target is depicted in Figure 1 (page 210).

A28. DBA is a rigorous and demanding method of fault analysis aimed at providing a robust demonstration of the fault tolerance of a facility. Consequently, Target 4 has been set to ensure that DBA is applied in all cases where significant consequences could arise with reasonable likelihood. The target was included in the 2006 SAPs to quantify the qualitative criteria set by Principle P25 in the 1992 SAPs. The target is intended to engender a targeted and proportionate approach in which this type of fault analysis is focussed on fault sequences making a significant contribution to overall risks.

A29. In this approach, faults selected for DBA are chosen on the basis of their initiating fault frequency (IFF) and potential unmitigated radiological consequences as shown in Figure 1. This figure has been derived as follows: following the approach adopted in the 1992 SAPs, only faults with IFF greater than 1×10^{-5} pa should be considered for DBA. This defines the lowermost section of the boundary of the DBA Region (depicted by red hatchings in the Figure). Furthermore, 1992 SAP P25(b) indicates that doses off the site of up to 100 mSv may be allowable in “severe” design basis fault sequences. Hence, faults with the lowest IFFs whose potential consequences are less than 100 mSv are excluded. This defines the lowest portion of the left-hand boundary of the DBA Region. The 100 mSv dose level was chosen so that the analysis would address any initiating fault that might be expected to lead to an evacuation away from the immediate vicinity of the site, taking into account the conservatism of the analysis. Appendix 2 paragraph 1 of the 1992 SAPs and the textbox following paragraph 751 provide further details of the likely consequences of off-site radiological releases.

A30. For doses on the site, 1992 SAP P25(c) states that there should be no "excessive dose" following any design basis fault sequence. This was interpreted in the 2006

SAPs to equate to a dose of 500 mSv, since observable deterministic symptoms from accidental exposures to radiation are considered unacceptable following a design basis fault. This defines the lowest portion of the left-hand boundary of the DBA Region for doses on the site.

A31. For more frequent faults (ie those with a reasonable probability of occurrence during the lifetime of the facility), it is considered unacceptable for design basis protective safety measures not to be provided for faults capable of exceeding the corresponding BSLs of 1 mSv pa (off the site) or 20 mSv pa (on the site) in Targets 1 and 3. The IFF for such faults has been set at 1×10^{-3} pa based on long-standing DBA practices established for UK power reactors. This defines the upper portion of the left-hand boundary of the DBA Region in Figure 1.

A32. The remaining portion of the DBA Region boundary has been derived based on a broadly logarithmic interpolation between the limiting cases described above, in order to engender a proportionate approach. Target 4 is intended to provide a broad indication of where DBA might be expected to be applied and is not intended to be a rigid rule: dutyholders are expected to develop their own methods for defining the scope of DBA tailored to their specific circumstances (see paragraph 704). Target 4 is however provided as a generic starting point for ONR inspectors, particularly where there is no well-established licensee guidance.

A33. This definition of where DBA should be applied is not intended to imply that safety measures are not needed elsewhere. Initiating faults with consequences below the BSL still require consideration of possible safety measures and the application of relevant good practice to ensure risks are reduced to ALARP (see note to paragraph 628). The identification and design of these safety measures should be informed through application of PSA and SAA and the risks compared with Targets 5 to 9.

A34. The second purpose of Target 4 (see paragraph A10) is to define success criteria (ie performance requirements) for the design basis safety measures. These are set in terms of the residual dose consequences from the faults assuming successful operation of the safety measures. In keeping with the preference for safety measures that fully protect against, or terminate fault sequences in their early stages, the BSOs have been set at a level comparable with the BSOs for operational doses in Targets 1 and 3. In cases where it is not reasonably practicable to provide safety measures protecting to these levels (see also paragraph 635), the DBA should demonstrate suitable safety measures are nevertheless in place to reduce (i.e. mitigate) potential doses to levels below the relevant Target 4 BSLs. The logic for this is as follows: any fault in the DBA Region whose mitigated consequences cannot be reduced below the BSLs would then constitute a further DBA initiating fault in its own right. However, this fault would be unprotected, in breach of paragraph 635). Hence Target 4 defines where ONR expects to see DBA applied; the success criteria for DBA safety measures; and a region where inspectors should explore the reasonable practicability of providing protective safety measures rather than mitigating ones.

Probabilistic Safety Analysis

Individual risk of death from accidents – any person on the site	**Target 5**
The targets for the individual risk of death to a person on the site, from accidents at the site resulting in exposure to ionising radiation, are: BSL: 1×10^{-4} pa BSO: 1×10^{-6} pa	

A35. Target 5 addresses the summed risk to individual persons on the site from exposure to ionising radiation from accidents at any facility on the site. This risk will however, likely be dominated by risks from the facility where the person works. Also employees working with ionising radiation are likely to be at greater risk than other employees on the site.

A36. The limiting risk to persons on the site from normal operation is set by Target 1 at 8×10^{-4} pa (see paragraph A16). Hence the risk apportioned to accidents needs to be less than 2×10^{-4} pa, in order to meet the upper level of 1×10^{-3} pa set by R2P2. The BSL for accidents was therefore set in the 2006 SAPs at 1×10^{-4} pa which, though slightly lower, provides an allowance for the difficulties and uncertainties in estimating worker risks. However, as pointed out in paragraph 732, in cases where the risk from normal operation is predicted to be well below the BSL of Target 1, higher accident risks could potentially be allowable based on the totality of the summed risks and applying a different apportionment. Any such revised apportionment would need to be adequately justified.

A37. It is acknowledged that the BSO is set at a demanding level and that in some cases it may not be reasonably practicable to reduce risks to this degree. Such instances are acceptable provided it can be demonstrated that doses satisfy BSLs and have been reduced to ALARP.

A38. In addition, management arrangements should identify appropriate controls to limit the doses and risks to other persons such as visitors, trainees and women of reproductive capacity. Such persons are not explicitly covered in Target 5.

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}

A39. This target, which is subsidiary to the site Target 5, relates to the risk to persons on the site from accidents in individual facilities. This was a new target in the 2006 SAPs, with no analogue in the 1992 SAPs. It was originally intended that the dose-

frequency staircase given here should be applied to the totality of accidents at the facility that could affect any person on the site, ie the values in the table referred originally to the summed frequencies of all the accidents giving rise to doses in the respective dose bands. However, it was later realised that such an approach would be unduly onerous, being almost an order of magnitude more demanding than other ONR guidance. Hence this target was set instead to apply to any single accident at the facility (ie at levels consistent with wider guidance).

A40. The dose-frequency staircase is similar in appearance to the staircase for persons off the site in Target 8. Like Target 8, this target is designed to ensure that the greatest levels of protection are applied to faults with the most significant consequences. For each step of the staircase, the limiting values of the BSL dose and frequency correspond to a risk of death of roughly 1×10^{-4} pa for any person at the location of maximum exposure. However, although this risk equals the site BSL in Target 5, these values are not directly comparable since the frequencies in Target 6 are predicted accident frequencies rather than predicted frequencies of exposure. These differ in that accident frequencies should not normally take credit for occupancy. Setting the target in terms of accident frequencies rather than exposure frequencies is intended to place focus on preventing accidents at source, or providing protection via means high up in the Principle EKP.5 hierarchy, rather than relying on measures to control occupancy or proximity (see paragraph 734).

A41. In setting Target 6 at these levels we have assumed that any individual on the site is only likely to be at risk from relatively few potential accident scenarios, and these will not likely be at a limiting frequency, dose or occupancy level. In consequence, the dominant contribution to their risks can be assumed to fall within a single band of the staircase. Setting risk levels in each band so that the limiting risk is roughly the same as the summed risk in Target 5 then results in reasonable consistency between the two targets. In particular, Target 6 ensures that no single accident can make an excessive contribution to the overall site BSO and BSL in Target 5. Moreover, the target promotes a balanced approach to addressing on-site risks that focuses attention on measures that protect or mitigate the risks to groups of persons on site, even though the risk to any individual member of the group may be low.

A42. The doses used for Target 6 were selected based on the IRR99 annual dose limit of 20 mSv, multiplied by powers of 10 so that each step of the staircase represents an equal level of risk.

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 accidents at the site resulting in exposure to ionising radiation, are: BSL: 1×10^{-4} pa BSO: 1×10^{-6} pa	

A43. Target 7 addresses accident risks to the public, summed for all facilities on a site. Although this was a new target in the 2006 SAPs, the BSL and BSO levels were implicit in the 1992 SAPs (see Appendix 2, paragraph 6 and its references to TOR). The target was introduced for consistency with the approach for on-site risks in Target 5.

A44. The BSL for normal operation doses in Target 3 equates to a risk of fatality of 5×10^{-5} pa. When combined with the Target 7 BSL for accidents, the total risk sums to 1.5×10^{-4} pa, which is slightly above the level proposed in R2P2 for members of

the public. In practice however, it is very unlikely that the predicted risks from normal operation and from accidents will both reach their corresponding BSL levels. As such, and given the inherent uncertainties in numerical predictions of accident risk, it is argued that the chosen BSL is appropriate. Similar arguments may be employed to justify the choice of BSO.

A45. It should also be noted that the BSL in this target is the same as that for on-site risks in Target 5. This is purely coincidental and arises because the on-site risks arising from normal operation contribute a significant fraction of the R2P2 upper risk level, so that the 'available' risk from accidents is then relatively small (see paragraph A36). This causes the two targets to become equal even though the R2P2 level for workers is an order of magnitude greater than that set for the public.

A46. The two BSOs are also equal; both having been set at the level proposed by R2P2. No reduction has been made here for contributions from normal operations since this would lead to risk targets beyond what is considered to be reasonably practicable.

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	1×10^{-2}
1–10	1×10^{-1}	1×10^{-3}
10–100	1×10^{-2}	1×10^{-4}
100–1000	1×10^{-3}	1×10^{-5}
>1000	1×10^{-4}	1×10^{-6}

A47. The dose frequency staircase in Target 8 is unchanged from the 1992 SAPs (Principle P42).

A48. Target 8 sets limits on the frequencies of classes of accident at individual facilities that could give rise to doses off the site within the specified bands. Summing the risk from each band, and assuming a probability of death equal to 1 for doses in excess of 1Sv, a facility just satisfying the BSLs would pose a fatality risk of 3×10^{-4} pa. However, to derive the risk to a person living nearby, account also needs to be taken of the variability of wind and weather conditions. Including these factors reduces the risk of death to an individual just outside the site from a single facility that just meets the BSLs to about 2×10^{-5} pa. Similarly, a facility just meeting the BSO frequencies gives an individual risk of fatality of about 2×10^{-7} pa. These single facility values are consistent with the levels set in Target 5 (1×10^{-4} and 1×10^{-6} pa) for whole site risks.

A49. Target 8 also defines limits for single fault sequences (set at one tenth of the given BSOs and BSLs – see paragraph 749). Comparing this aspect of the target with Target 6, it is evident that Target 8 is broadly a factor of 10 more stringent for fault sequences affecting persons off the site than Target 6 is for sequences affecting persons on the site at the same dose consequences. This seems reasonable.

A50. Although conceptually it would be possible to extend Target 8 to include further dose bands beyond 1Sv, accidents of this magnitude would, in all likelihood, affect

relatively large numbers of people. As such, accidents leading to doses off the site significantly in excess of 1Sv should also be assessed against Target 9.

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 accidents at the site resulting in exposure to ionising radiation, are: BSL: 1×10^{-5} pa BSO: 1×10^{-7} pa	

A51. In the 1992 SAPs, the target for frequencies of accidents that could give rise to societal consequences was given by P44, the large release SAP. P44 was couched in terms of the release of specified quantities of two particular radionuclides chosen based on the predicted resultant total number of cancer deaths that could arise. However, a number of issues related to P44 were identified following publication and application of the 1992 SAPs. In particular problems were encountered in regard to the relationship between releases and the number of deaths, and how to define equivalent source terms for sites where the radionuclides specified in P44 are not the ones of principal concern. Although research was commissioned to try to resolve these problems, no satisfactory conclusion was reached.

A52. In developing the 2006 SAPs, the issue of societal risk was re-examined and a variety of options considered for setting societal risk frequency targets. These included estimating the potential number of radiation-related deaths from a major accident, the extent to which such an accident would lead to a need to extend the REPPIR off-site emergency planning area around the site, and a combination of these two considerations.

A53. Research was commissioned from the Health Protection Agency (HPA, now Public Health England) to look at how these aspects would vary at specific UK sites encompassing a variety of source terms. Based on this research, we concluded that P44 should be replaced by a target set in terms of the total risk of occurrence of 100 or more immediate or eventual fatalities, on and off the site, from accidents resulting in exposure to ionising radiation. This formulation also had the advantage of being of a similar form to the approach in R2P2 to judging the risk of multiple fatalities occurring in one event from a single major industrial activity (see R2P2 paragraph 136). An alternative formulation in which the target was based on consideration of emergency countermeasures could not be supported technically to a suitable degree. Based on the HPA studies, we also concluded that the calculations of accident consequences should be truncated at 100 years and limited to the effects on the UK population.

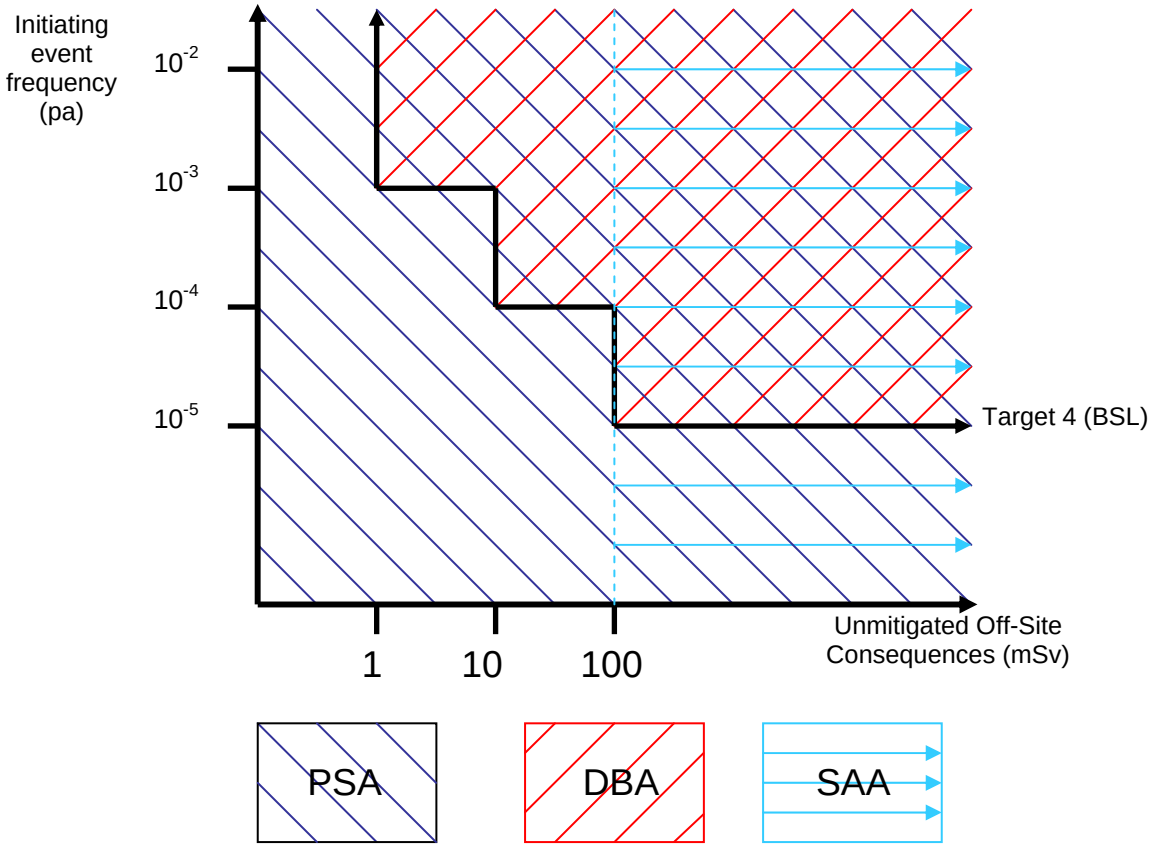
A54. Target 9 is intended to be used as a guide to assist in judging whether more detailed analysis is warranted. As with other numerical targets, target 9 is a pragmatic approach to enable targeted and proportionate use of our resources. ALARP considerations by dutyholders below the BSO should, however, not be ruled out.

A55. The approach taken for Target 9 is consistent with the findings of the 1990 Barnes Report on Hinkley Point ‘C’ (which P44 was intended to address): that an event leading to one hundred to several hundred immediate or eventual deaths should not be more frequent than one in a hundred thousand years. ONR considers that there is sufficient international technical consensus on methods, data and assumptions to allow it to be applied appropriately by dutyholders. ONR recognises that the aggregation of very low individual doses over extended time periods is inappropriate,

and in particular, the calculation of the number of cancer deaths based on collective effective doses from trivial individual doses should be avoided.

FIGURES

Figure 1: Schematic showing the general ranges of applicability of the 3 methods of Fault Analysis.



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 kilogramme (NRPB, now PHE).
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). *In this document, the term 'accident' describes undesired circumstances beyond fault conditions giving 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 exposures 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 material within the facility.* *In the context of radiation protection, an accident should be considered to be equivalent to the international term 'emergency exposure situation'.*
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).
Barrier	A barrier means to: ▪ prevent the further progression of a fault; ▪ prevent or inhibit the movement of people or radioactive material, or some other phenomenon (eg fire); ▪ provide shielding against radiation.
Best estimate	When used to describe analysis, this refers to an approach 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 and the knowledge of the analysts, without any deliberate bias being introduced. When used to describe the data (eg from experiment or operating experience), it refers to the unbiased estimate of the variable that minimises its variance. Where

	there is inadequate evidence, and no credible best estimate is possible, then bounding or conservative values should be used.
Bounding case	A single situation used to represent a wider class of situations that is more extreme than any member of the class in all important respects.
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 and conditions within which the function(s) can be sustained; and (b) the circumstances 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 examination, inspection, maintenance and testing programme.
Class of fault	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 exposed to a given source of ionising radiation. Measured in man-Sieverts (manSv) (NRPB, now PHE).
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).
Common cause failure	Failure of two or more structures, systems or components due to a single specific event or cause (IAEA Safety Glossary).
Conservative	In analysis, an approach where the use of models, data and assumptions 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 both 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 material (based on IAEA Safety Glossary).

Contractors	All references to 'contractors' include proportionate consideration of the whole contracting and supply chain, whether for the provision of goods and services to the licensee or on the licensed site. This includes designers, vendors, suppliers, manufacturers etc as appropriate.
Countermeasures	An action aimed at alleviating the radiological consequences of an accident (IAEA Safety Glossary).
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).
Design basis fault	A fault sequence meeting the criteria set out in paragraph 628 of the Fault Analysis SAPs.
Design Extension Conditions	Accident conditions that are not considered for design basis accidents, but that are considered in the design process of the facility in accordance with best estimate methodology, and for which releases of radioactive material are kept within acceptable limits. Design extension conditions could include severe accident conditions (IAEA Safety Glossary).
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).
Design intent	The fundamental criteria and characteristics (including reliability levels) that need to be realised in a facility, plant or SSC in order that it achieves its operational and safety functional requirements.
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).
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, now PHE). *'Effective dose' is frequently abbreviated to 'dose'.*
Emergency exposure situation	See Accident
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).
Employees working with ionising radiation	The term 'employees' is used in IRR99. Working with ionising radiation has the same interpretation as in IRR99, namely work involving the production, processing, handling, use, holding, storage, transport or disposal of radioactive substances. For the purposes of assessment, employees can be regarded as the same as workers.
Essential services	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. *Essential services may also supply safety-related systems.*
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, now PHE).
Facility	A part of a nuclear site identified as being a separate unit for the purposes of nuclear or radiological risk. *A facility may, for example, 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 encompasses 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.
Failure	The situation where a structure, system or component no longer meets its safety function, or functions spuriously.
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 conditions	Unplanned operation of a facility beyond normal operations arising from a fault and with the potential to lead to an accident. Fault conditions include faults with consequences that have not (or cannot) be justified within the safety case as acceptable for normal operations.
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 an accident.
Government	For the purposes of this document, the term 'the Government' means the 'the UK Government and/or the Devolved Administrations, as appropriate'.
Geometrical constraint	In 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). *Hazard is also used in the terms internal hazard and external hazard, where it refers to an initiating or consequential event that directly challenges the safety of a nuclear facility (such as a fire, flood, or earthquake).*
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).
Incident	An undesired circumstance or 'near miss', eg an initiating event or a fault condition, that has the potential to cause an accident.
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. *Inherent safety is a higher standard than passive safety in that*

	the former requires a demonstration that it is physically impossible for the harm to arise.
Initiating fault/event	The starting point of a fault sequence. This may be an internal failure, or caused by an internal or external hazard or by human action, or a combination of these. *The definition does not include pre-existing latent failures that may be revealed once safety measures are called upon to function during a fault sequence.*
Intelligent customer	The capability of an organisation to understand where and when work is needed; specify what needs to be done; understand and set suitable standards; supervise and control the work; and review, evaluate and accept the work carried out on its behalf.
Ionising radiations	For the purposes of radiation protection, radiation capable of producing ion pairs in biological materials (IAEA Safety Glossary).
Licensed site	A site in respect of which a Nuclear Site Licence has been granted 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).
Lifecycle	All the stages in the life of a facility from conception through to de licensing. This includes design, build, commissioning, operation, maintenance, closure, decommissioning, disposal of waste and the return of a site to a safe state.
Normal operation(s)	Operation within specified operational limits and conditions. (IAEA Safety Glossary). *Normal operations include all the operating modes permitted at the facility, eg start-up and shutdown states and temporary situations arising due to maintenance and testing. They also include minor deviations from desired operating conditions provided these are appropriately justified in the safety case (ie they include what the IAEA terms Anticipated Operational Occurrences).* *The operational limits and conditions defining normal operations should be derived from the safety case and are Operating Rules for the purposes of compliance with Licence Condition 23.* *In the context of radiation protection, normal operations*

	should be considered to be equivalent to the international term 'planned exposure situations'.
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 operations. *See also Normal operations.*
Operating rule	Any condition or limit in place at a nuclear facility through which a licensee demonstrates compliance with its safety case. *An operating rule is any limit or condition necessary in the interests of safety defined in the safety case, and not just those that the licensee terms 'operating rules' – see Licence Condition 23.*
Passive safety	Providing and maintaining a safety function without the need for an external input such as actuation, mechanical movement, supply of power or operator intervention. In the context of decommissioning and the storage of nuclear matter, providing and maintaining a safety function by minimising the need for active systems, monitoring or prompt human intervention. See also Inherent safety: a passive safety system is not necessarily inherently safe.
Planned exposure situation	See Normal operations.
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).
Qualification	The process of demonstrating that a structure, system or component is fit for its intended purpose.

	Note: This is a generalisation of IAEA's definition of Equipment qualification – the 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).
Quality management	Co-ordinated activities to direct and control an organisation with regard to quality (ie ensuring that requirements are fulfilled). *Direction and control with regard to quality generally includes quality policy, quality objectives, quality planning, quality control, quality assurance and quality improvement.* *Licence Condition 17 requires adequate quality management arrangements in respect of all matters which may affect safety. Such matters include those derived from the safety case, facility design and licence conditions.*
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).
Radioactively contaminated land	Land containing radioactive contamination at levels that would preclude its delicensing.
Radioactive material	Radioactive material has the meaning given in Part 2 paragraph 3 of the Environmental Permitting (England and Wales) Amendment Regulations 2011, disregarding the exception in paragraph 9 (contaminated substances or articles).
Radioactive waste	Radioactive waste has the meaning given in Part 2 paragraph 3 of the Environmental Permitting (England and Wales) Amendment Regulations 2011.
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).
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).
Reliability	The probability that a system or component will meet its minimum performance requirements when called upon to do so (IAEA Safety Glossary).
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).
Risk	Risk is the chance that someone or something is adversely affected in a particular manner by a hazard (R2P2).
Safety	In this document, ‘safety’ refers to the safety of persons in relation to radiological hazards.
Safety actuation system	The collection of equipment required to accomplish the necessary safety actions when initiated by the protection system (IAEA Safety Glossary).
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 ONR. *Note: Licence Condition 1 defines ‘safety case’ as the document or documents produced by the licensee in accordance with Licence Condition 14.*
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).
Safety function	A specific purpose that must be accomplished for safety (IAEA Safety Glossary).
Safety measure	A safety system, or a combination of procedures, operator actions and safety systems that protects against 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). *Safety-related systems are therefore systems in place to perform an operational function but which also provide a safety benefit. This is distinct from safety systems, which are systems which do not perform any operational functions and are included solely because of the safety functions they perform.*
Safety system	A system that acts in response to a fault to protect against a radiological consequence. *See also Safety-related system.*

Safety system support features	The collection of equipment that provides services such as cooling, lubrication and energy supply required by the safety systems (based on IAEA Safety Glossary).
Segregation	Depending on the context: 1. The physical separation of structures, systems or components 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 (based on IAEA Safety Glossary).
Service	An organisation or utility supporting the safety of one or more facilities. *Examples include health physics or emergency services, or utilities such as steam, electricity, water, nitrogen or compressed air required for safety.*
Severe accident	An accident with off-site consequences with the potential to exceed 100 mSv, or to a substantial unintended relocation of radioactive material within the facility that 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 effects	Quantifiable aspects of an accident with widespread adverse repercussions regionally or nationally, eg numbers of deaths or injuries, numbers of people evacuated, area of land contaminated or general economic loss.
Societal risk	The risk of an accident with societal effects causing the deaths 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, the location of the release and other related parameters from the facility needed as inputs to radiological consequence calculations.
Stable, safe state	The state of the facility once stabilisation of any transient or fault has been achieved, ie the facility is subcritical, adequate heat removal is ensured and continuing radioactive releases are limited (based on IEC61226).

	A transient or fault is considered to be stabilised when for all safety-significant parameters, the margins (eg between heat removal capacity and heat generation) are either stable or increasing, or sufficient margin remains to cover all expected physical processes, and there is high confidence that this stability will be maintained.
Structure, system and/or component	An item important to safety within the facility design which provides a safety function *The safety function provided by the SSC may be direct or indirect, eg the SSC may be important to safety because it supports another SSC which provides a safety function.*
Task analysis	Systematic delineation and examination of the psychological and physical demands placed upon a human operator by specified task requirements.
Unmitigated consequences	The potential radiological consequences of a fault or accident evaluated assuming all safety measures are absent or fail to operate. This excludes passive safety features such as walls or pipes, unless the fault or accident affects that feature.
Validation	The process of confirming, eg by use of objective evidence, that the outputs from an activity will meet the objectives and requirements set for that activity.
Verification	The process of confirming, eg by use of objective evidence, that an activity was carried out as intended, specified or stated.

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
BSL	Basic safety level
BSL(LL)	Basic safety level (legal limit)
BSO	Basic safety objective
BSS	Euratom Basic Safety Standards (BSS) Directive (96/29/Euratom)
CBA	Cost benefit analysis
CCF	Common cause failure
CCCA	Component and core condition assessment
CID	Criticality incident detection
CIDI	Central Index of Dose Information
COMAH	Control of Major Accident Hazards
DBA	Design basis analysis
DBE	Design basis earthquake
DNP	Defence Nuclear Programme
DNSR	Defence Nuclear Safety Regulator
EIADR	The Nuclear Reactors (Environmental Impact Assessment for Decommissioning) (Amendment) Regulations 2006
ENSREG	European Nuclear Safety Regulators Group
EMIT	Examination, maintenance, inspection and testing

EPR	Environmental Permitting Regulations
HAZOP	Hazard and Operability study
HIRE	Hazard identification and risk evaluation
HPA	Health Protection Agency
HSE	Health and Safety Executive
The HSW Act/HSWA	The Health and Safety at Work etc Act 1974
IAEA	International Atomic Energy Agency
ILO	International Labour Organisation
IRR99	Ionising Radiations Regulations 1999
The Management Regulations	The Management of Health and Safety at Work Regulations 1999
MOD	Ministry of Defence
MoU	Memorandum of Understanding
NDA	Nuclear Decommissioning Authority
NEA	Nuclear Energy Agency (of the Organisation for Economic Cooperation and Development)
NEPLG	Nuclear Emergency Planning Liaison Group
NII	Nuclear Installations Inspectorate
NIA	The Nuclear Installations Act 1965 (as amended)
NRPB	National Radiological Protection Board (now part of Public Health England)
NRW	Natural Resources Wales
OBE	Operating basis earthquake
ONR	Office for Nuclear Regulation
Pa	Per annum

PHE	Public Health England
PPE	Personal Protective Equipment
PSA	Probabilistic safety analysis
PSR	Periodic safety review
R2P2	Reducing risks, protecting people: HSE's decision making process
RPV	Reactor pressure vessel
REPPIR	Radiation (Emergency Preparedness and Public Information) Regulations 2001
RoA	Report of Assessment
RSA	Radioactive Substances Act 1993
SAA	Severe Accident Analysis
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
WENRA	Western European Nuclear Regulators' Association

REFERENCES

While every effort has been made to ensure the accuracy of the references listed in this publication, their future availability cannot be guaranteed.

1 Reducing risks, protecting people: HSE's decision making process HSE Books 2001 ISBN 0 7176 2151 0. http://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. http://www.hse.gov.uk/nuclear/tolerability.pdf

3 ONR Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable). Technical Assessment Guide NS-TAST-GD-005 (Rev 6). http://www.onr.org.uk/operational/tech_asst_guides/index.htm

4 HSE Policy Statement. Our approach to permissioning regimes. First published 2003. http://www.hse.gov.uk/enforce/permissioning.pdf

5 ONR Enforcement Policy Statement. http://www.onr.org.uk/documents/2014/enforcement-policy-statement.pdf

6 ONR Licensing Nuclear Installations http://www.onr.org.uk/licensing-nuclear-installations.pdf

7 Successful health and safety management HSG65 (Third edition). HSE Books 2013 ISBN 978 0 7176 6456 6. http://www.hse.gov.uk/pubns/priced/hsg65.pdf

8 Columbia Accident Investigation Board Report August 2003. www.nasa.gov/columbia/home/CAIB_Vol1.html

9 The official report of The Fukushima Nuclear Accident Independent Investigation Commission. https://www.nirs.org/fukushima/naiic_report.pdf

10 IAEA Safety Requirements SSR-2/1 Safety of Nuclear Power Plants: Design. ISBN 978–92 –0–121510–9. http://www-pub.iaea.org/books/IAEABooks/Series/33/IAEA-Safety-Standards-Series

11 IAEA Safety Standard SSG-2 Deterministic Safety Analysis for Nuclear Power Plants. ISBN 978-92-0-113309-0. http://www-pub.iaea.org/books/IAEABooks/Series/33/IAEA-Safety-Standards-Series

12 Working with ionising radiation. Ionising Radiation Regulation 1999. Approved code of practice and guidance. L121 HSE Books 2000 ISBN 0 7176 1746 7. http://www.hse.gov.uk/pubns/books/l121.htm

13 The Hinkley Point Public Inquiries: A Report by Michael Barnes QC The Stationery Office 1990 ISBN 0 11 412955 X

14 https://www.gov.uk/government/publications/nuclear-emergency-planning-consolidated-guidance

15 Occupational exposure to ionising radiation 1990 – 1996. Analysis of doses reported to the Health and Safety Executive's Central Index of Dose Information www.hse.gov.uk/radiation/ionising/doses/cidi.htm

16 HSE Central Index of Dose Information, Summary Statistics for 2004. www.hse.gov.uk/radiation/ionising/doses/cidi.htm

Further information

This document is available web-only at: http://www.onr.org.uk/saps/index.htm

Any enquiries regarding this publication should be addressed to:

ONR communications team
Office for Nuclear Regulation
Redgrave Court
Merton Road
Bootle
Merseyside
L20 7HS
Email: onr@onr.gsi.gov.uk

Published 11/14

Further information about ONR is available at www.onr.org.uk