



ONR GUIDE			
SAFETY OF NUCLEAR FUEL IN POWER REACTORS			
Document Type:	Nuclear Safety Technical Assessment Guide		
Unique Document ID and Revision No:	NS-TAST-GD-075 Revision 3		
Date Issued:	October 2020	Review Date:	October 2025
Approved by:	R Exley	Professional Lead: Fault Analysis	
Record Reference:	CM9 Folder 1.1.3.978. (2020/207899)		
Revision commentary:	<p>Minor update to reference the Ionising Radiation Regulations 2017.</p> <p>Updated November 2018.</p> <p>Further updated October 2020, incorporating review of IAEA specific safety guide SSG-52.</p>		

TABLE OF CONTENTS

1. INTRODUCTION	2
2. PURPOSE AND SCOPE OF FUEL ASSESSMENT	2
3. RELATIONSHIP TO LICENCE AND OTHER RELEVANT LEGISLATION.....	2
4. RELATIONSHIP TO SAPS, WENRA REFERENCE LEVELS AND IAEA SAFETY STANDARDS ADDRESSED.....	3
5. ADVICE TO INSPECTORS	9
6. REFERENCES	22
7. GLOSSARY AND ABBREVIATIONS	23
8. TABLES.....	24
9. APPENDICES.....	26

1. INTRODUCTION

1 The Office for Nuclear Regulation (ONR) has established its Safety Assessment Principles (SAPs) (Ref. 1) which apply to the assessment by ONR specialist inspectors of safety cases for nuclear facilities written by potential licensees, existing licensees, or other duty-holders. The principles presented in the SAPs are supported by a suite of guides to further assist ONR's inspectors in their technical assessment work in support of making regulatory judgements and decisions. This technical assessment guide is one of these guides.

2. PURPOSE AND SCOPE OF FUEL ASSESSMENT

2 This guidance covers design and operation of nuclear fuel and core components in reactor and its transfer from the fuel storage pond. It deals with both the limits and conditions to be used during fuel operation in core and the design limits to be applied to confirm the resilience of the fuel in faults. Here fuel is taken to mean all components of the fuel assembly.

3 This Technical Assessment Guide (TAG) contains guidance to advise and inform ONR staff in the exercise of their regulatory judgment and to provide more detailed explanation of ONR interpretation of International Atomic Energy Agency (IAEA) safety requirements and Western European Nuclear Regulators Association (WENRA) reference level requirements.

4 This TAG is principally aimed at the operation of civil reactor uranium oxide fuel and restricts itself to information that can be openly published. However, where the ONR inspector considers it reasonable to do so the TAG can be applied to the use of other fuels.

5 Requirements for compliance with nuclear safeguards and measures to address threats from hostile third parties are outside the scope of this TAG. Some nuclear safety related topics of interest to fuel & core inspectors are captured within other, interfacing TAGs (Ref. 2) – these are listed in Section 4.6.

3. RELATIONSHIP TO LICENCE AND OTHER RELEVANT LEGISLATION

6 In the context of the Nuclear Installations Act 1965, a holder of a nuclear site license (the licensee) has a number of duties which relate specifically to fuel performance:

- LC 14 requires the licensee to make and implement adequate arrangements for the production of safety cases to justify the design, construction, manufacture, commissioning, operation and decommissioning of a facility.
- LC 20 and 22 require adequate control of modifications which may affect safety.
- LC 23 requires an adequate safety case to demonstrate safe operation and to identify the limits and conditions of operation to form the basis of operating rules.

7 In respect of other legislation, The Health and Safety at Work Act 1974 places duties on employers to provide and maintain plant and systems of work that are, so far as is reasonably practicable, safe and without risks to health.

8 The Ionising Radiations Regulations 2017 lay down the statutory requirements for the protection of persons against ionising radiation.

9 The Environment Agency, Natural Resources Wales and the Scottish Environmental Protection Agency regulate the disposal of radioactive waste from nuclear licensed sites under the Environmental Permitting (England & Wales) Regulations 2016 for England and Wales and the Environmental Authorisations (Scotland) Regulations 2018 for Scotland respectively. Environmental permits/authorisations given to such sites

include conditions that set quantified limits on radioactive discharges for normal operations. Inspectors should be cognisant that sites may need to account for these discharge limits when setting failed fuel management policy, or when considering the options available to them following the detection of failed fuel during operation.

- 10 Duty holders under the above legislation are referred to as the licensee throughout this document. However, the guidance may be applied in appropriate circumstances to the assessment of safety cases written by organisations which are not licensees, for example Requesting Parties participating in a Generic Design Assessment (GDA).

4. RELATIONSHIP TO SAPS, WENRA REFERENCE LEVELS AND IAEA SAFETY STANDARDS ADDRESSED

- 11 The ONR SAPs have a number of key engineering principles which apply to the fuel and are generally also present in similar words in IAEA safety standards and requirements (Ref. 3, Ref. 4), WENRA safety reference level requirements for existing reactors (Ref. 5) and the WENRA Reactor Harmonisation Working Group Report on Safety of new Nuclear Power Plant designs (Ref. 6). These documents are considered examples of relevant good practice and should be considered as basic expectations when making As Low As Reasonably Practicable (ALARP) judgements (see NS-TAST-GD-005 on demonstration of ALARP, Ref. 2).

- 12 WENRA safety reference levels for existing reactors judged to be particularly relevant to fuel are summarised in Table 1, which identifies the sections of this document in which they are addressed. IAEA provide a specific guidance document relevant to the design of the reactor core for nuclear power plants (Ref. 7). It is recommended as further reading and has been used extensively in benchmarking this guidance.

- 13 Common to these source documents is the requirement to preserve, as far as reasonably practicable, the integrity of the fuel as a barrier to the release of fission products. Ref. 7 states that:

- Physical barriers considered as part of, or affecting the design of, the reactor core include the fuel matrix, the fuel cladding and the boundary of the reactor coolant system.
- For normal operation and anticipated operational occurrences, fuel rods are required to be designed such that their structural integrity and a leak-tight barrier are maintained to prevent the transport of fission products into the coolant.
- For accident conditions (design basis accidents and Design Extension Conditions (DEC) without significant fuel degradation), the design should ensure no fuel rod failures where this is reasonably practicable; otherwise, only a limited number of fuel rod failures should be allowed.
- The reactor core is required to be designed to maintain a configuration such that it can be shut down and remains coolable for design basis accidents and DEC without significant fuel degradation.

- 14 The application of this guidance in a UK context is explained in Subsection 4.3 with respect to quantified fault frequencies. The IAEA terms 'anticipated operational occurrence' and 'design basis accident' are not used in this TAG except where IAEA or WENRA guidance is directly quoted. Instead, the term 'fault' is used to refer to any unplanned departure from the specified mode of operation due to a malfunction, defect, external influences or human error. The term 'design basis fault' is sometimes used to refer to all faults within the design basis. The terms 'frequent faults' and 'infrequent faults' are also used to refer to design basis faults in particular quantified frequency bands. The IAEA term 'DEC' is retained to refer to faults outside the design

basis. The use of this term and the relevant scope of this TAG in the context of DEC is further explained in paragraphs 32-33.

- 15 The purpose of assessment of fuel and core safety cases is to ensure that the design and operation of the fuel supports the key safety principles that the plant operators are expected to respect. Key principles detailed in the SAPs are given below and the fuel context is discussed. In addition, specific principles for the reactor core are explained.

4.1 Inherent Safety

- 16 The design of a reactor core should be carried out to ensure that its dynamic response is acceptable within its anticipated operating domain. This is reflected in the following key principle:

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.		

- 17 An 'inherently safe' design is one that avoids radiological hazards rather than controlling them. It prevents a specific harm occurring by using an approach, design or arrangement that ensures that the harm cannot happen.
- 18 In the context of the fuel, this principle would initially be applied to the design of fuel storage racks, which ONR expect to be designed to retain the most reactive fuel subcritical irrespective of whether operating procedures have been followed correctly or soluble poisons in the pond water correctly controlled.
- 19 In the core, this principle would apply to the constraints placed by design on fuel reactivity. In particular, fuel reactivity should be constrained so as to avoid situations where anticipated moderator density changes can potentially result in unacceptable reactivity transients that require action of control or safety systems to protect the fuel.
- 20 Further detailed expectations are given in Section 5 below and in Ref. 7.

4.2 Fault Tolerance

- 21 This principle is an extension of the principle of inherent safety to reasonably foreseeable events. Ref. 7 states that the design of the reactor core should be such that the feedback characteristics of the core rapidly compensate for an increase in reactivity. The SAPs include the following principle:

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

- 22 Any failure, process perturbation or mal-operation in a facility should produce a change in plant state towards a safer condition, or produce no significant response. If the change is to a less safe condition, then systems should have long time constants so that key parameters deviate only slowly from their desired values.
- 23 From the fuel neutronic perspective, this is achieved by ensuring that adequately conservative assumptions are made for kinetics parameters (for example reactivity coefficients) in the analysis of all design basis faults. An important role of core design

in the safety case is to substantiate these assumptions for particular core loading and management strategies.

- 24 Key neutronic parameters such as reactivity coefficients and power peaking factors should be evaluated for each core state for the corresponding fuel management strategy. Appropriate allowance should be made for uncertainty; consistent with review and acceptance criteria used in reactor physics testing. See Sections 5.5, 5.6 and 5.7.

4.3 Defence in Depth

- 25 Defence in depth is applied in multiple levels; encompassing prevention, protection and mitigation of faults. The methodology ensures that if one level of defence fails, it will be compensated for, or corrected by the subsequent level. The aims for each level of protection are described in detail in Ref. 4. The SAPs contain the following principle:

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.		

- 26 The concept of defence in depth should be applied to ensure:
1. Prevention of abnormal operation and failures by design;
 2. Prevention and control of abnormal operation and detection of failures;
 3. Control of faults within the design basis to protect against escalation to an accident;
 4. Control of severe plant conditions in which the design basis may be exceeded, including the prevention of fault progression and mitigation of the consequences of severe accidents; and
 5. Mitigation of radiological consequences of significant releases of radioactive material.
- 27 The reactor core design has a key role in a number of these levels:
- The fuel cladding is a passive barrier to release of nuclear material from the fuel;
 - The core design has a substantial influence on the worth of protection systems;
 - The selection of core material and the analysis of severe accidents has an influence on the likely success of accident mitigation measures; and
 - Analysis of potential radiological releases can have a significant effect on accident management measures.
- 28 The fuel design activities undertaken by the licensee or its fuel vendor should identify and substantiate appropriate design criteria for the fuel, such that these can be confirmed as being met by fault analysis undertaken for a specific or bounding core design. There may also be a need to confirm adequate performance by explicit fuel performance modelling. Furthermore, the fuel itself needs to be designed to acceptable standards and sound principles so that it continues to fulfil its safety function throughout its design life.

- 29 IAEA advise that a primary objective shall be to manage all design basis accidents so that they have no, or only minor, radiological consequences, on or off the site, and do not necessitate any off-site protective actions (Ref. 4).
- 30 Measures are applied as part of a graded approach; where the expected level of confidence in a particular measure should depend on the likelihood of the potential hazard, often measured by the initiating event frequency (IEF). Relevant good practice for UK nuclear power plant safety cases is:
- It should be demonstrated with a high degree of confidence that frequent design basis faults ($IEF > 10^{-3}/yr$) do not result in breaches of the fuel cladding.
 - For infrequent design basis faults ($10^{-3}/yr < IEF < 10^{-5}/yr$), the integrity of the fuel cladding should be maintained so far as is reasonably practicable. If it is not possible to demonstrate that cladding integrity is maintained in these faults then the radiological consequences should be reduced to ALARP.
 - All design basis faults should be mitigated without loss of coolable geometry or the ability to shut down the reactor, so that dispersal of nuclear material can be minimised and remaining barriers to release preserved.
- 31 This is consistent with paragraph 13 above and also with the expectations of SAP FA.7 and Numerical Target 4.
- 32 Modern safety case expectations, as established by IAEA and WENRA, are that events and sequences outside of the design basis should be analysed deterministically and probabilistically to show that they will not escalate into a severe accident. Both international organisations have adopted the term DEC for onerous reactor plant states outside the design basis. A distinction is made between DEC-A which occur without significant fuel degradation (DEC-A) and DEC-B progressing to core melt (DEC-B).
- 33 The behaviour of fuel in a severe accident (i.e. DEC-B plant states) and the associated safety case expectations are beyond the scope of this TAG, being captured separately in NS-TAST-GD-007 on Severe Accident Analysis (Ref. 2.). The expectations for DEC-A plant states are effectively the same as those set out for infrequent design basis faults above, although the level of conservatism included in calculations may be reduced, and judgements on what is ALARP may be different. Further guidance is provided in NS-TAST-GD-006 on Design Basis Analysis (Ref. 2) and IAEA guidance on deterministic safety analysis (Ref. 8).

4.4 Analysis of Safety Functions

- 34 As part of the safety case, the SAPs expect a systematic analysis of safety functions:

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.		

- 35 For fuel and core systems and components, the following functional requirements may be relevant:
- Confinement of activity;
 - Maintenance of geometry acceptable for cooling and nuclear considerations;
 - Enabling reactor shutdown and hold down;
 - Facilitating safe handling and transport of nuclear material.
- 36 A fuel safety case should for each significant system, structure or component, identify specific functional requirements and provide a clear set of claims, arguments and evidence to demonstrate that these requirements are met.

4.5 Reactor Core Design Requirements

- 37 ONR expectations relating to specific design requirements for the reactor core are found in SAPs ERC 1 to 4.

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.		

- 38 The above principle covers normal operation, refuelling, testing and shutdown and design basis fault conditions. The fundamental safety functions are:
- control of reactivity (including re-criticality following an event);
 - removal of heat from the core; and
 - confinement or containment of radioactive substances.
- 39 There should be suitable and sufficient margins between the normal operational values of parameters important to safety and the values at which the physical barriers to release of fission products are challenged. At a principle level IAEA require that a set of design limits consistent with the key physical parameters for each structure, system or component shall be specified for operational states and design basis accidents (Ref. 4). See Section 5.4 below.
- 40 A strategy for dealing with fuel failures should be specified. This will generally involve removing the failed fuel so that measures can be taken to mitigate the release of fission products and the further degradation of the fuel structure. The timing of this action will be dependent on compliance with defined limits for activity release and the suitability of measures designed to prevent further degradation of the fuel pin in situ. See Section 5.2 below.

Engineering principles: reactor core	Shutdown systems	ERC.2
At least two diverse systems should be provided for shutting down a civil reactor.		

- 41 This principle is generally satisfied by the provision of a system of control rods, with a backup of a fluid system acting over a slower time scale in the case of failure of the mechanical system. This is discussed in Section 5.

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.		

- 42 The SAPs expect that 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.
- 43 This principle elaborates on SAP EKP.2 above. It should be recognised that strong negative feedback can result in challenges to shutdown systems in the event of excess power demands and can in severe cases cause rapid power transients. Positive feedback on the other hand, can result in an uncontrollable power transient. All core designs need suitable characteristics to ensure tolerable response within the limits of reasonably foreseeable operation. Detailed advice to the inspector is given in Section 5.

Engineering principles: reactor core	Monitoring of safety-related parameters	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.		

- 44 This SAP relates to the monitoring of core performance and fuel condition. Advice to inspectors is found in Section 5.6 below, with expectations relating to failed fuel in Section 5.2.

4.6 Interfacing TAGs

- 45 The following TAGs (Ref. 2) also include advice that may be relevant to fuel & core inspector activities and which is not repeated in this TAG. The inspector should therefore also refer to these other TAGs as appropriate:
- Guidance on the Demonstration of ALARP is provided in NS-TAST-GD-005.
 - Design basis analysis is addressed in NS-TAST-GD-006. NS-TAST-GD-006 focuses on the high level principles and concepts of design basis analysis.
 - Severe Accident Analysis is addressed in NS-TAST-GD-007.
 - Detailed additional guidance on graphite reactor cores is provided in NS-TAST-GD-029.
 - Limits and Conditions for Nuclear Safety (Operating Rules) are addressed in NS-TAST-GD-035. NS-TAST-GD-035 gives generic advice about Operating Rules.
 - Criticality Safety is addressed in NS-TAST-GD-041. NS-TAST-GD-041 applies to all situations where the fuel is outside of the reactor core.
 - Validation of Computer Codes and Calculation Methods is addressed in NS-TAST-GD-042. The scope of NS-TAST-GD-042 includes all such codes and methods used for fuel and core design.
 - Nuclear Lifting Operations are addressed in NS-TAST-GD-056. NS-TAST-GD-056 includes the design and operation of equipment used for fuel handling.
 - Storage of spent fuel waiting onward processing or disposal is addressed in NS-TAST-GD-081.
 - Chemistry assessment is addressed in NS-TAST-GD-089.

5. ADVICE TO INSPECTORS

46 Inspectors should consider the following topics in their assessment.

5.1 Fuel Cladding Failure in Normal Operation

47 The functional requirement of the fuel cladding is to provide a barrier to the release of fission products, or where this is not possible to limit the release of radiation to the environment to acceptable levels. Experience has shown that fuel failures cannot be entirely eliminated, but by study of failure mechanisms and the use of systematic quality improvement programmes, the incidence can be reduced by an order of magnitude.

48 Where fuel failures do occur (or have done so historically for similar designs), the inspector should consider whether the licensee (and other duty holders such as equipment suppliers) have taken practical measures to identify the root causes and reduce their frequency. Benchmark failure rates are less than one in 100,000 pins and the best performing utilities often operate reactors for years without any failures.

49 Compliance with good practice requires design to achieve conditions where failure of any individual pin would be an extremely low probability event.

5.2 Mitigation of Fuel Cladding Failure

50 The inspector should consider whether adequate measures are in place to mitigate the consequences of fuel failures. ONR expects that the release of activity into the coolant should be detected and procedures followed to ensure that the dispersal of nuclear material is minimised. Furthermore, our initial expectation is that a clean-up system should be employed to control contamination levels unless it can be shown that failed fuel management alone can keep this within acceptable levels.

51 ONR expects the licensee to include limits and constraints on coolant activity in their operating rules. The inspector should consider whether these are consistent with safety case assumptions and whether the plant can realistically be operated within the limits. Fuel & core inspectors should co-ordinate with chemistry and fault studies inspectors on these topics. Co-ordination with the Environment Agency may also be required where the same coolant activity limits are used in determining environmental discharge limits or where actions proposed under failed fuel management policy may increase the radioactivity contained in environmental discharges.

52 The inspector should examine the licensee's policy on failed fuel management.

53 In the event of a failure, ingress of coolant into the fuel pin can cause chemical degradation of the cladding material. Measures are expected to limit such degradation.

54 Good practice is to identify the failed assembly and to retrieve it from the reactor core at the earliest practical opportunity.

55 In some reactor designs, fuel degradation can be minimised by locating the failure and reducing local power levels to relieve the cladding stress. This can be used to delay fuel removal.

5.3 Fuel Failure Mechanisms

56 The inspector should consider whether the design has made adequate provision against failure by established failure mechanisms. The following should be considered:

- Flow-induced vibration, resulting in wear at the contact between the rods and spacer grids;

- Cladding corrosion and related embrittlement, including the effect of surface deposit layers where appropriate;
 - Debris-fretting caused by foreign material (such as swarf) becoming trapped between fuel pins and spacer grids (or similar structures);
 - Defects in the closure welds;
 - Pellet-cladding interaction caused by operational transients; and
 - Cladding creep failure.
- 57 The main method by which fuel failure is avoided is the quantification of fuel design limits which ensure fuel integrity.
- 58 The inspector should ensure that suitable operating limits have been defined which have sufficient safety margin to allow for both uncertainty in manufacturing parameters and transient events.
- 59 It should be recognised that fuel design and qualification is essentially empirical. Significant changes in fuel design should therefore be regarded with caution and introduction should be progressive and reversible. Modelling should be undertaken but not solely relied upon. Inspectors should satisfy themselves that design changes are supported by a programme of pilot loadings and sufficient relevant operating experience and testing. Furthermore, they should examine the mitigation strategy should the new fuel design fail.
- 60 The results of blind benchmarking exercises such as Ref. 9 demonstrate a generally poor ability of existing fuel codes to predict fuel performance when faced with new conditions. The use of multi-scale modelling of fuel rods is unlikely to remove the need for integral testing of fuel rods in-reactor, in particular because the key physical processes are currently not all fully understood (Ref. 10 contains further detail on this topic).
- 61 ONR expects licensees to have a systematic programme of post-irradiation component examination and testing to ensure that the arguments made in the safety case remain valid. This should include robust systems for maintaining records.

5.3.1 Flow-induced Vibration

- 62 Inspectors should satisfy themselves that either the fuel loading lies within the operational domain of previous fuel, or that sufficient testing has been performed to establish operating limits. Both Advanced Gas-cooled Reactors (AGR) and Light Water Reactors (LWR) have experienced design changes that unexpectedly led to multiple pin failures by flow-induced vibration.
- 63 The main constraint on power density in most reactor designs is the rate at which coolant can be pumped through an assembly of fuel pins. Ultimately a point is reached where flow-induced vibration is at intolerable levels. The fuel design should operate with a suitable safety margin to this condition.
- 64 Models do exist which claim to predict the rate of wear at the interface between the rods and the spacer grids, but these should not be regarded as more than extrapolation of experimental data. Generally, full-scale experiments are made to determine wear rates at conditions representing flow rates marginally above the limiting conditions expected in reactor (with due allowance for irradiation creep).
- 65 Where the flow distribution at the entry to the core is not uniform so that cross-flow occurs near the bottom of an open-matrix fuel element, this is a potential cause of vibration. The inspector should be satisfied that suitable measures have been taken to address this.

- 66 Flow-induced vibration of control rod assemblies and other in-core components such as neutron sources can also cause excessive wear of these components at contact points. The inspector should be satisfied that the design life of in-core components suitably caters for these effects. Some modern designs utilise improved surface finishing technologies to reduce susceptibility to wear. It is also possible to reduce wear in some circumstances through operational practices, for example swapping a control rod assembly to a different bank in an outage to avoid wear on the same location through-life.

5.3.2 Corrosion, Hydridding and Surface Deposits

- 67 The inspector should be satisfied that sufficient measures are in place to limit cladding embrittlement to tolerable levels so that the cladding can continue to fulfil its function in normal operation and faults. Some specific issues are detailed below:
- Hydride pickup has been a general concern for metal clad oxide fuel. The inspector should be satisfied that there is sufficient control on pellet moisture levels during manufacture.
 - Given the potentially adverse impact of thick layers of deposit (also known as crud) on cladding integrity, the chemistry of the primary circuit needs to be closely controlled. Failure can occur due to enhanced corrosion in the presence of thick deposits within a single cycle of operation if chemistry control is inadequate. This is an area where interaction with the chemistry assessment is recommended.
 - For LWR designs, the inspector should be satisfied that the limits on cladding external surface corrosion and the associated hydrogen pickup are justified and will not be exceeded at fuel discharge. Generally, it should be shown that the accumulated oxide layer remains intact and therefore significant hydride-assisted cracking is avoided in reactor operation and subsequent storage. The inspector should consider whether limits on the rate of sub-cooled boiling are required to limit the concentration of radiolysis products in the coolant and to restrict the rate of deposition of crud.
- 68 The licensee should undertake surveillance programmes to ensure that the state of the cladding is consistent with safety case assumptions. For fuel deposits, operating experience shows that surveillance of fuel assemblies can be appropriate even directly after the first operating cycle to verify the expected behaviour.

5.3.3 Debris-fretting

- 69 The inspector should consider whether there are sufficient measures in place to limit the effects of debris inadvertently introduced into the primary circuit by poor operational practice or component degradation in normal operation, including shutdown, maintenance and refuelling.
- 70 Small items of debris, trapped in spacer grids, remain a significant cause of fretting failures. Typically, a short section of wire or swarf is trapped between the grid and the fuel rod and vibrates, causing wear on the surface of the adjacent fuel pin.
- 71 Most fuel designers have responded to this issue by fitting a debris filter at the entry to the fuel assembly and this has been successful in reducing debris-induced failures by an order of magnitude. However, this is an issue which should also be addressed by housekeeping measures aimed at foreign material exclusion. In particular, suitable arrangements are necessary to control machining operations during outages and fuel receipt inspections. IAEA advise ensuring by design that the coolant system is free of foreign materials, prior to initial start-up and following outages through-life (Ref. 7).

5.3.4 Debris Blockage Considerations

- 72 While the use of fuel assembly debris filters is good practice, they do introduce the risk that foreign material or debris present in the reactor coolant system could block the filter and starve the fuel of coolant flow.
- 73 In LWR, even if foreign material is effectively excluded during normal operation, it is still possible for ingress to occur during cooling after a Loss of Cooling Accident (LOCA) or other high energy pipe failure, via coolant re-circulated from containment. The source of this material can be either latent debris in containment or debris released from plant materials (for example insulation) as a consequence of the LOCA event. This topic is discussed extensively in Ref. 11, although the discussion of impact on the fuel assembly (what Ref. 11 calls 'downstream effects') is limited due to constraints on the use of proprietary information in the public domain.
- 74 The holistic assessment of such a fault including definition of the debris source-term is outside the scope of this TAG. However, from a fuel perspective, the inspector should satisfy themselves that the consequences of debris on pressure drop and heat transfer in the fuel assembly under post-LOCA cooling conditions have been adequately addressed. This usually relies on experimental evidence of the impact of the predicted accumulation of debris on the fuel assembly. Data used in the thermal hydraulic analysis of post-LOCA cooling (for example, the fuel assembly pressure drop) should be bounding of these effects.
- 75 In AGR, following sufficient irradiation to cause graphite cracking in the core, blockages are possible due to relocation of graphite debris within the core during normal operation. These blockages can cause a degradation in heat transfer due to a reduction in cooling flow, particularly immediately downstream of the blockage. The inspector should be satisfied that adequate allowance is made within the safety case for these effects. Where computational fluid dynamics techniques are used to predict the flow field, these should be validated through experiment. The inspector should refer to NS-TAST-GD-042 (Ref. 2) for guidance in assessing this validation.

5.3.5 Fuel-pin Closure Welding

- 76 The inspector should be satisfied that suitable arrangements are in place to qualify and control welding operations on fuel components; end-caps in particular.
- 77 The process of welding the end caps of fuel pins is a significant technical and metallurgical challenge. Defect rates have been reduced by efforts to control contamination of the weld during manufacture and to optimise the manufacturing process.
- 78 Good practice is to formally qualify the process after any changes and periodically. Checking 100% of the pressurised pins for leaks is also expected.

5.3.6 Design Against Pellet-Cladding Interaction

- 79 IAEA guidance (Ref. 7) advises that stress corrosion cracking induced by pellet-cladding interaction in the presence of corrosive fission products should be prevented.
- 80 The inspector should be satisfied that there are sufficient operating limits and automated protection in place to prevent fuel failures by pellet-cladding interaction in normal operation and frequent faults.

- 81 Several approaches may be considered for limiting failures due to stress corrosion cracking. For example:
- Tensile stresses may be lowered by restricting rates of power change (allowing for the cladding stresses to relax) or by delaying the time at which the pellet-cladding gap closes (this can be achieved by increasing the initial fill gas pressure in the fuel rod or by optimizing the creep properties of the cladding).
 - A fission product barrier may be placed at the inner surface of the cladding to reduce the corrosive effects of the fission products generated by the pellet. This liner can also even out local stress concentrations in the cladding.
 - The availability of corrosive fission products at the pellet-cladding interface may be reduced by using additive fuels that are able to better retain the corrosive fission gas products within the fuel matrix.
 - Local power peaking may be reduced by the appropriate overall design of the core.
- 82 In AGR, a small number of failures have occurred that are not fully understood. The approach has been to seek better understanding of the mechanism and to take appropriate mitigation measures, including setting appropriate operating rules.
- 83 For LWR, extensive international in-reactor prototype and out-of-reactor testing has been conducted to better understand the phenomena influencing fuel failure due to stress corrosion cracking, but the phenomena are still only partially understood. The mechanism appears to be related to the release of aggressive chemical species from the fuel pellet during power ramps and the action of these chemicals on the cladding at points of high stress to assist in the initiation and propagation of cracks within the cladding. The inspector should therefore be satisfied that operating rules are set to prevent failure in this manner and are justified with suitable reference to experimental data.
- 84 IAEA (Ref. 7) advise that fuel performance analysis codes can be used to analyse and interpret the data from power-ramp tests and to determine a failure threshold. The parameter used to define this threshold is usually the maximum cladding stress but the strain energy density can also be used. They advise that the power-ramp failure threshold should be established in test reactors by means of power-ramp tests for each type of fuel or cladding and that the data collected should cover the entire burn-up range.
- 85 ONR's usual expectations for fuel integrity in faults are discussed in paragraph 30. For frequent faults, a demonstration of tolerance to a single failure of protection is usually expected in accordance with SAP EDR.4. However, ONR has previously judged that this expectation can be relaxed for the PCI failure mechanism. This is on the basis that the hazard associated with PCI fuel failures is generally contained and for the faults assessed, the damage to the cladding was judged likely to be limited to pin-hole failures, so that only a small fraction of the mobile fission products was likely to be released into the coolant. The inspector will need to reach judgements on a case-by-case basis using the claims, arguments and evidence presented by the licensee.
- 86 Manufacturing defects can reduce safety margins in this context. In particular, damage to the pellet surface can lead to short sections of unsupported cladding. Good practice is to set inspection criteria to require such defects to be sufficiently small that the stress concentration is comparable to that of pellet cracks arising during normal irradiation. Manufacturers should be expected to follow this practice or provide suitable justification.

5.3.7 Cladding Creep Collapse

- 87 The inspector should satisfy themselves that there is suitable substantiation of the fuel design against plastic collapse.
- 88 Fuel pins are initially pressurised with helium to increase the conductivity of the gap between the pellet and the cladding and to limit the stresses in the cladding caused by the action of the coolant pressure. However, this pressure is generally not sufficient to prevent inwards creep of the cladding.
- 89 Two safety concerns apply:
- The pellet may not provide sufficient support to prevent the cladding ductility being exceeded.
 - Contact between the pellet and the cladding can lead to axial gaps developing in the pellet stack; causing local increases in thermal neutron flux.
- 90 In LWR, the practice has been to retain a continuous axial pellet stack by the action of a coil spring and to harden the cladding sufficiently to prevent creep collapse until densification of the fuel pellet stack is complete.
- 91 In AGR, this is not practical, so axial movement of the fuel is prevented by crimping the cladding into grooves in the pellet and no end plena are present.

5.4 Design Criteria

- 92 The inspector should be satisfied that appropriate design limits are specified for key fuel physical parameters so that deterministic analysis can demonstrate the effectiveness of safety measures claimed in the safety case for fault conditions (see Ref. 4 and NS-TAST-GD-006, Ref. 2). Advice on key parameters is given below.

5.4.1 Peak Fuel Temperature

- 93 A limit on peak fuel temperature prevents cladding failure as a result of rapid fuel pellet swelling (and consequential threats to the integrity of the primary circuit as a result of molten fuel-coolant interaction). The selected limit should be lower than the fuel melting temperature by a sufficient margin to prevent melting of the fuel, with allowance made for uncertainties due to experimental data and the effects of burnup.

5.4.2 Peak Cladding Temperature

- 94 Limitations on cladding surface temperatures are provided to ensure that the cladding retains its role as a confinement for fuel material. In order to achieve this, the cladding ductility needs to be retained and its geometry preserved as far as reasonably practical.
- 95 Fuel pin internal gas pressure and cladding temperatures need to be constrained to avoid the cladding failing by ballooning in normal operation and faults and to ensure that the cladding stress and strain levels are acceptable both in reactor and after discharge. However, it has been recognised that in a major primary-circuit depressurisation event, this may not be reasonably practical and fault-specific criteria need to be applied. In these cases, the objective is to ensure that the fuel remains in a coolable geometry and that fuel handling remains practical. Excessive clad oxidation or embrittlement should not be allowed to occur and limits are usually placed on hydrogen production to limit accident consequences. More detail on these topics is provided by the IAEA in Ref. 7.
- 96 In the UK, a major experimental and analytical programme was undertaken on LWR fuel cladding ballooning during the licensing process for Sizewell B. It was concluded that coolable geometry could be retained provided that cladding deformation could be delayed until reflooding of the core had started. Otherwise, the inspector should expect

sufficient evidence to justify the expected level of coolant blockage under the specific conditions anticipated.

- 97 In the case of gas-reactor fuel, inspectors should satisfy themselves that the effect of expected levels of insulating surface deposit has been taken into account as appropriate.

5.4.3 Critical Heat Flux

- 98 In LWR, the cladding surface temperature is generally guaranteed by respecting the critical heat flux¹ limit. Such limits are empirical in nature. Ref. 7 states that experiments should be conducted on representative fuel assembly designs over the range of expected operational states, including various axial heat flux profiles, to identify the limiting values of the minimum critical heat flux ratios. Inspectors should satisfy themselves that such experiments are adequately representative of the real fuel design and that scaling effects and uncertainties (see Section 5.5) have been accounted for.
- 99 In most cases, exceeding the critical heat flux will lead to some degree of fuel damage although it is recognized that in some designs, fuel clad dryout can be tolerated during transients if it can be shown by suitable methods that the cladding temperatures do not exceed the acceptable limits.
- 100 Further guidance on application of critical heat flux limits is provided in Ref. 7.
- 101 As discussed in paragraph 30, ONR's expectation is that cladding failure be prevented in frequent faults. The critical heat flux limit usually serves an important role in demonstrating this.

5.4.4 Pin Pressure Limit in Normal Operation

- 102 Irradiation needs to be limited so as to retain the integrity of the fuel material, in normal operation and faults. In particular, the effect of fission gas needs to be considered both during plant operation and spent fuel storage.
- 103 In normal operation, it is necessary to ensure that pin internal pressures do not exceed the normal coolant pressure sufficiently to open up a gap between the cladding and the pellet; leading to poor heat transfer within the pin.
- 104 In anticipation of spent fuel storage, the normal operational design limits should reflect the design stress and temperature transient assumed for transfer to and storage in a proposed storage facility. Consideration should be given to the potential for reorientation of hydrides within the cladding. The limits should be set to retain the integrity of the cladding as a barrier to fission-product release when transferred to that facility.

5.4.5 Radial-Average Peak Fuel Enthalpy

- 105 Fuel cladding failure can occur directly due to the stresses induced by pellet-cladding mechanical interaction in fast reactivity transients. Design limits on the maximum allowable radial-average peak fuel enthalpy (RAPFE) or change in RAPFE during a transient are commonly imposed to prevent this. IAEA (Ref. 7) advise that fuel failure is considered to occur if the radial average enthalpy of a fuel rod at any axial location, calculated with validated tools, exceeds a certain value to be determined based on representative experimental results by appropriately adjusting test conditions to represent in-reactor conditions.

¹ This limit is the maximum heat flux that can be removed by boiling processes before the surface becomes blanketed by a film of steam. In BWR, this criterion is often expressed as a critical power ratio, but this is mostly convention, the mechanism for cladding dryout in LWR is most likely deposition-controlled dryout. Steam cooling is generally less efficient than water cooling.

5.4.6 Limits on structural components

- 106 Inspectors should satisfy themselves that core components are suitably designed against appropriate design codes.
- 107 For some critical components such as the fuel cladding, demonstration of defect tolerance may also be required. The complexity of the argument required will depend on the component's safety significance and the magnitude of the safety margin demonstrated.
- 108 Inspectors should satisfy themselves that the analysis takes due account of fatigue and all relevant cracking mechanisms.
- 109 The loads considered should include those anticipated during handling operations, including anticipated events such as hoist snags and impacts. This applies to fuel assemblies and other core components including control rods.
- 110 Historically, the potential for interference between fuel assemblies during core unloading has limited discharge irradiations.
- 111 The inspector should be satisfied that the fuel assembly has been subject to a suitable and sufficient mechanical design process. The assembly is subjected to mechanical stresses as a result of:
- Fuel handling and loading;
 - Power variations;
 - Temperature gradients;
 - Hydraulic forces, induced by the core flow and hold-down forces required to maintain core geometry;
 - Irradiation (e.g. radiation induced growth and swelling);
 - Vibration and fretting induced by coolant flow;
 - Creep deformation;
 - External events such as earthquakes;
 - Postulated faults such as a LOCA.
- 112 As described in section 4.3, all design basis faults and DEC-A should generally be mitigated without loss of coolable geometry or the ability to shut down the reactor, so that dispersal of nuclear material can be minimised and remaining barriers to release preserved. IAEA guidance (Ref. 7) further advises that the design should prevent any interaction between fuel rods or fuel assemblies and fuel assembly support structures that would impede safety systems from performing their functions as specified in the safety analysis. However, in the case of large bore LOCA, ONR has previously judged that limited crushing of grids in the fuel assemblies at the edge of the core is acceptable, if it can be shown that the power density in these locations is low and therefore that consequences remain ALARP. This advice is applicable whether a large bore LOCA has been classified as within the design basis or as a DEC-A.
- 113 Ref. 7 advises that the clearance within and adjacent to the fuel assembly should provide space to allow for irradiation induced growth and bowing (for light water reactors) and bulging of the fuel channel (for boiling water reactors.)
- 114 If the space between fuel assemblies increases due to these phenomena, the thermal neutron flux can be affected. If the coolant is also the moderator, the flux can significantly increase, leading to locally increased fuel pin ratings. Conversely, if gaps between fuel assemblies are reduced or eliminated, a significant reduction in coolant flow may be experienced locally. This may affect heat transfer.

- 115 Design analysis and surveillance programmes should confirm that the limiting values of fuel assembly distortion used in the thermal analysis are respected. Any deformation of the fuel element or the fuel assembly should not affect the capability for the insertion of control rods for the safe shutdown of the reactor. The impact on fuel handling should also be addressed in the design.
- 116 The fuel assembly should be able to withstand the mechanical and hydraulic hold-down forces required to maintain core geometry without unacceptable deformation and bowing and fatigue loading should not be able to cause the failure of a fuel assembly.

5.5 Treatment of Uncertainty

- 117 The inspector should be satisfied that the fuel designer has substantiated key limits taking a precautionary approach to the treatment of uncertainties by selecting the appropriate level of minimum safety margin, in consultation with fault studies experts.
- 118 The appropriate margin in this context is designed to ensure a high confidence that the fuel design criterion is not exceeded. The acceptable probability level for such a test is informed by the principle of a graded approach to safety analysis; taking into account the magnitude of the hazard, the likelihood of the event and the novelty and complexity of the safety arguments (Ref. 3).
- 119 Generally, the benchmark would be an analysis where uncertainties in key parameters are set at limiting values of 95% probability determined at 95% confidence, with analysis performed from the most limiting operating condition in the permitted region of operation. However, if a fault can be shown to be low probability, more relaxed treatments of uncertainty can be agreed in consultation with the fault study assessors.
- 120 In some cases, licensees will argue that uncertainties can be combined statistically. This is acceptable provided that suitable justification is provided that any correlation between the key parameters has been suitably accounted for. Moreover, a distinction should be made between systematic uncertainty; which should be treated as a bias to the analysis and random variation which can be suitably combined statistically. The IAEA provide further guidance on treatment of uncertainty in Ref. 8.
- 121 Where complex computer codes have been used to quantify safety margins, inspectors should satisfy themselves that the limits of validity of the codes are demonstrated and adequately documented. NS-TAST-GD-042 (Ref. 2) should be consulted for detailed guidance on this topic. In particular for physics analysis using 2D lattice and 3D diffusion codes, which supply important input neutronic data for many fuel & core safety analyses, the inspector should consider whether the modelling approach and applied uncertainty adequately capture more complex regions of the fuel & core design. These regions include:
- The edge of the core and the radial reflector region;
 - Axially heterogeneous regions of the core including the ends of partially inserted control rods and any axial step changes in fuel enrichment;
 - Fuel rods with high burnable absorber content.

5.6 Core monitoring

- 122 Inspectors should satisfy themselves that adequate provision has been made for fuel and core monitoring to ensure that functional requirements are met, including those of fuel handling.
- 123 The extent of this monitoring needs to be informed by operational experience for the specific fuel design. SAPs relating to ageing and degradation are relevant and this

- monitoring should feed back on the declared design life of components important to safety.
- 124 The requirements for loading and unloading of fuel and core components should ensure that there are sufficient control and monitoring measures in place to ensure that the likelihood of an accident is adequately low and the magnitude of the associated hazard is clearly understood. For brevity, this TAG does not discuss the refuelling topic in detail. A detailed discussion is found in IAEA guide NS-G-2.5 (Ref. 12).
- 125 An appropriate strategy of core monitoring and physics testing is required to confirm that the core (as built) operates within the performance envelope defined by the safety case. This requirement is satisfied by defined acceptance criteria for physics tests that are consistent with safety case assumptions. In particular, Ref. 6 states that the effectiveness of the reactivity control devices such as neutron absorber rods should be verified by direct measurement. In LWR this is generally achieved as part of physics tests following fuel reloads. In reactors with at-power refuelling e.g. AGR, this can be achieved by suitable monitoring of control rod positioning.
- 126 IAEA standards (Ref. 4) require that adequate means of detecting the neutron flux distributions in the reactor core and their changes shall be provided for the purpose of ensuring that there are no regions of the core in which the design limits could be exceeded. Good practice in this area is to provide continuous monitoring of key core parameters in the control room, with more detailed measurements taken at a suitable frequency during core irradiation to ensure that any unexpected changes in the core power shape as a result of irradiation and other effects are detected.
- 127 In modern reactor designs, ex-core instrumentation is increasingly supplemented by in-core instrumentation which gives better spatial resolution of the power distribution. This is sometimes displayed in the control room as a comparison between measured and expected power maps.
- 128 The ability to diagnose faults in the power distribution is significantly enhanced by this practice, but experience has shown that the operator can be misled by faults in such a system. Where these systems are used to support significant safety claims, they should generally meet the requirements of appropriate safety classification. A reduced safety classification could be acceptable in some cases if a robust demonstration is provided of adequate measures to mitigate the effect of unrevealed in-core instrumentation system failure, or/and diverse means of monitoring are provided, with surveillances at appropriate time intervals. This should be judged on a case by case basis for a specific plant and set of in-core instrumentation functional requirements.
- 129 The inspector should consider whether there are sufficient controls in place to mitigate the risk of inadvertent criticality as fuel is loaded into the core and consider whether the potential for multiple errors during re-load (rather than only a single error) has been adequately addressed. The potential for fuel misloading in the fuel storage pond and fuel assembly drop events should also be considered. NS-TAST-GD-041 (Ref. 2) provides advice on criticality safety assessment outside of the reactor core.
- 130 In fuel storage, the expectation is that the most reactive fuel can be maintained in a configuration that is passively safe without relying on the absence of moderator or the presence of soluble poisons. The arrangements should not be reliant on administrative controls to ensure this configuration. See Section 4.1 above.

5.6.1 Ageing Management

- 131 Expectations for management of component ageing and degradation are set down in SAPs EAD.1 to 5. Both IAEA (Ref. 4) and WENRA (Ref. 5) require that the licensee shall assess structures, systems and components important to safety taking into account relevant ageing and wear-out mechanisms and potential age-related

- degradations in order to ensure the capability of the plant to perform the necessary safety functions throughout its planned life, under design-basis conditions.
- 132 The inspector should be satisfied that suitable monitoring, testing, sampling and inspection activities are provided to assess ageing effects and to identify unexpected behaviour or degradation during service.
- 133 Good practice for fuel is that regular inspection of fuel should take place when it is discharged from the reactor and that this should be informed by operational experience and the importance of the component to safety. Recorded information should be securely stored and systematically ordered so as to preserve knowledge. Useful advice in judging good practice is found in Ref. 13.
- 134 Topics of interest (see section 5.3 for further information) include:
- Irradiation growth and creep;
 - Fatigue;
 - Corrosion and fuel deposits (crud);
 - Fretting damage.
- 135 Periodic non-destructive examination of fuel is expected to confirm:
- Safety case assumptions and safety margins;
 - Fuel microstructure;
 - Isotopic compositions and irradiations.
- 136 Particular focus should be given to the performance of novel features and of components operating outside the normal experience.
- 137 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 design basis fault or DEC-A conditions. In particular, distortion of fuel assemblies or control rod channels (as a result of normal irradiation or seismic loading) should not reach such a level where control rod insertion would be inhibited. Acceptable levels of distortion should be quantified, and suitable levels of surveillance performed to demonstrate compliance. This is generally carried out by a combination of fuel assembly metrology and rod insertion testing.

5.7 Plant Operational Limits and Core Design Parameters

- 138 A set of operating rules and surveillance requirements should be defined to ensure that fault transients respect the boundaries imposed by the fuel design criteria, to the extent expected for a given fault in accordance with the expectations of paragraph 30 of this TAG. Generally, this involves modelling the fuel and core response to transients and providing fault analysis with fuel and nuclear performance data which can be applied to the calculation of specific fault sequences.
- 139 The inspector should be satisfied that limits have been placed on key core design parameters that influence the plant response to abnormal conditions and the worth of protection systems. These limits should be consistent with the data provided to fault analysis. Such limits place active constraints on the core design.
- 140 In a commercial pressurised-water reactor (PWR) core design, the fixed poison loading is selected so that the critical boron concentration does not reach a level where the moderator density coefficient of reactivity becomes significantly negative.
- 141 In Boiling-water Reactors (BWR), the fuel-to-moderator ratio is selected so that the void coefficient does not cause a damaging response to reactor pressure transients.

- 142 In some core designs, the inability to demonstrate adequate dynamic response may be a sufficient reason to refuse a license.
- 143 Ref. 7 provides the following list of typical key nuclear safety parameters:
- The temperature coefficients of reactivity for the fuel, coolant and moderator;
 - The boron reactivity coefficient and concentration (for pressurized water reactors);
 - The shutdown margin;
 - The maximum reactivity insertion rate;
 - The control rod assembly worth and control bank worth;
 - The radial and axial power peaking factors, including allowance for xenon induced oscillation;
 - The maximum linear heat generation rate;
 - The void coefficient of reactivity.
- 144 Other important parameters determining the kinetic response of the core include the delayed neutron fraction, prompt neutron lifetime and the effects of power redistribution on reactivity (due to xenon efficiency and moderator density.)
- 145 In pressurized water reactors, in the event that fuel deposits occur with boron trapped in the crud layer, the key nuclear safety parameters above may be affected. The inspector should be satisfied that the potential impact of fuel deposits on the neutronic performance of the core has been addressed.
- 146 The following additional limits may be relevant to LWR:
- The domain of stable operation to ensure no Ledinegg instability and a suitable decay rate for density-waves.
 - Sufficient margin to the critical heat flux including margin for undetected core misloadings and core distortion.
 - Suitable constraints on control rod insertion to ensure adequate shutdown margin and to limit potential for reactivity insertion.
 - Suitable constraints on coolant pressure and temperature to preserve vessel integrity.
 - Suitable limits on levels of poisons and solid moderator to ensure tolerable core kinetic response in normal operation and faults.

5.8 Shutdown Systems

- 147 As per section 4.5, SAP ERC.2 states that at least two diverse systems should be provided for shutting down a civil reactor. For example, AGR rely principally on control rods for shutdown (and have diverse designs of rods), but this is supplemented by shutdown systems using pressurised nitrogen and boron beads (the latter of which is not recoverable). Relying only on control rods would generally not meet our expectations.
- 148 Where a shutdown system is also used for the control of reactivity, a suitable and sufficient shutdown margin should be maintained at all times. This requires suitable justification of shutdown margin when operating at the limit of permitted operation (usually specified in terms of rod insertion limits).
- 149 Consideration should be given to the resilience of mechanical shutdown systems to one or more of the shutdown assemblies failing to insert.

- 150 IAEA standards (Ref. 4) require that at least one of the two shutdown systems shall be, on its own, capable of maintaining the reactor subcritical by an adequate margin and with high reliability, even for the most reactive conditions of the core. One of these systems should be, on its own, capable of maintaining the reactor in a subcritical state for any core coolant temperature. Ref. 7 gives details of measures that can be taken to ensure suitable reliability. These are reproduced in Appendix 1.
- 151 IAEA standards (Ref. 4) also require that in the design of shutdown systems, due account be taken of wear out and of the effects of irradiation on such devices, including burnup, changes in physical properties and production of gas. Further guidance is given in Ref. 7.

6. REFERENCES

- 1) Safety Assessment Principles for Nuclear Facilities. 2014 Edition Revision 1. ONR. January 2020. www.onr.org.uk/saps/saps2014.pdf
- 2) ONR Technical Assessment Guides (TAG)
http://www.onr.org.uk/operational/tech_asst_guides/index.htm
- 3) Safety Assessment for Facilities and Activities; General Safety Requirements, IAEA Standards Series No. GSR Part 4 Rev. 1, IAEA, Vienna (2016).
- 4) Safety of Nuclear Power Plants: Design, Specific Safety Requirements, IAEA Standards Series No. SSR-2/1 Rev. 1, IAEA, Vienna (2016).
- 5) WENRA Reactor Safety Reference Levels for Existing Reactors, Western European Nuclear Regulators Association, Update in relation to lessons learned from TEPCO Fukushima DAI-ICHI Accident. 24 September 2014. www.wenra.org
- 6) WENRA Report - Safety of new NPP designs, Western European Nuclear Regulators Association Reactor Harmonization Working Group, March 2013. www.wenra.org
- 7) Design of the Reactor Core for Nuclear Power Plants, Specific Safety Guide, IAEA Standards Series No. SSG-52 Rev. 0, IAEA, Vienna (2019).
- 8) Deterministic Safety Analysis for Nuclear Power Plants, Specific Safety Guide, IAEA Standards Series No. SSG-2 Rev. 1, IAEA, Vienna (2019).
- 9) Improvement of Computer Codes Used for Fuel Behaviour Simulation (Fumex-III), Report of a Coordinated Research, Project 2008–2012, IAEA-TECDOC-1697 (2013)
- 10) State-of-the-Art Report on Multi-scale Modelling of Nuclear Fuels: NEA/NSC/R(2015)5, <https://www.oecd-nea.org>
- 11) Update Knowledge Base for Long Term Core Cooling Reliability: NEA/CSNI/R(2013)12, <https://www.oecd-nea.org>
- 12) Core Management and Fuel Handling for Nuclear Power Plants, IAEA Safety Guide No. NS-G-2.5, IAEA, Vienna (2002).
- 13) PD 0008:2004 Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Digitally (ISBN 0 580 42774 9) is published by the British Standards Institution.

7. GLOSSARY AND ABBREVIATIONS

AGR	Advanced Gas-cooled Reactor
ALARP	As low as reasonably practicable
BSL	Basic Safety Level
BSO	Basic Safety Objective
BWR	Boiling-water Reactor
CHF	Critical Heat Flux
DEC	Design Extension Condition
DNB	Departure from Nucleate Boiling
IAEA	International Atomic Energy Agency
IEF	Initiating Event Frequency
LOCA	Loss of Coolant Accident
LWR	Light-water Reactor
ONR	Office for Nuclear Regulation
PWR	Pressurised-water Reactor
PSR	Periodic Safety Review
RAPFE	Radial Average Peak Fuel Enthalpy
SAP	Safety Assessment Principle(s)
SSC	Structures, Systems and Components
TAG	Technical Assessment Guide(s)
WENRA	Western European Nuclear Regulators' Association

8. TABLES

Table 1: Relevant WENRA Reference Levels (Ref. 5)		
Reference	Title / Description	Relevant Section Above
Design Basis Envelope for Existing Reactors E.3.1	During normal operation, anticipated operational occurrences and design basis accidents, the plant shall be able to fulfil the following fundamental safety functions: - control of reactivity; - removal of heat from the reactor core and from the spent fuel; and - confinement of radioactive material.	Section 4.5 (SAP ERC.1)
Design Basis Envelope for Existing Reactors E.7.2	Criteria for protection of the fuel rod integrity, including fuel temperature, Departure from Nucleate Boiling (DNB), and cladding temperature, shall be specified. In addition, criteria shall be specified for the maximum allowable fuel damage during any design basis accident.	Section 5.4
Design Basis Envelope for Existing Reactors E.8.7	The safety analysis shall: (a) rely on methods, assumptions or arguments which are justified and conservative; (b) provide assurance that uncertainties and their impact have been given adequate consideration.	Section 5.5
Reactor and fuel storage sub-criticality E.9.6	The means for shutting down the reactor shall consist of at least two diverse systems.	Section 4.5 (SAP ERC.2) Section 5
Reactor and fuel storage sub-criticality E.9.7	At least one of the two systems shall, on its own, be capable of quickly rendering the nuclear reactor sub critical by an adequate margin from operational states and in design basis accidents, on the assumption of a single failure.	Section 5
Safety limits, safety systems settings and operational limits H.5.2	Safety limits shall be established using a conservative approach to take uncertainties in the safety analyses into account.	Section 5
Ageing Management I.2.1	The licensee shall assess structures, systems and components important to safety taking into account of relevant ageing and wear-out mechanisms and potential age related degradations in order to ensure the capability of the plant to perform the necessary safety functions throughout its planned life, under design basis conditions.	Section 5.6

Ageing Management I.2.2	The licensee shall provide monitoring, testing, sampling and inspection activities to assess ageing effects to identify unexpected behaviour or degradation during service.	Section 5.6
----------------------------	---	-------------

9. APPENDICES

APPENDIX 1: Shutdown System Reliability Requirements (from IAEA Specific Safety Guide SSG-52, Ref. 6)

A high reliability of shutdown should be achieved by using a combination of measures such as:

- (a) Adopting systems with uncomplicated design and simple operation, and with automatic activation.
- (b) Selecting equipment of proven design.
- (c) Using a fail-safe design as far as practicable.
- (d) Giving consideration to the possible modes of failure and adopting redundancy in the activation of the shutdown systems (eg sensors). Provision for diversity may be made, for example, by using two different and independent physical trip parameters for each accident condition as far as practicable.
- (e) Functionally isolating and physically separating the shutdown systems (this includes the separation of control and shutdown functions) as far as practicable, on the assumption of credible modes of failure, including common cause failure.
- (f) Ensuring ease of entry of the means of shutdown into the core, with consideration of the in-core environmental conditions for operational states and accident conditions within the design basis.
- (g) Designing to facilitate maintenance, in-service inspection and operational testability.
- (h) Providing means for performing comprehensive testing during commissioning and periodic refuelling or maintenance outages.
- (i) Testing of the actuation process (or of partial rod insertion, if feasible) during operation.
- (j) Designing to function under extreme conditions (eg earthquakes.)

A reliability analysis of shutdown systems should be performed to quantify the effectiveness of the design.