Office for Nuclear Regulation

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 2		
Date Issued:	September 2017	**Review Date:**	September 2020
Approved by:	R Moscrop	Professional Lead: Fault Analysis	
Record Reference:	Trim Folder 1.1.3.776. (2018/394015)		
Revision commentary:	Minor update to reference the Ionising Radiation Regulations 2017. Updated November 2018.		

TABLE OF CONTENTS

Published 09/2017

1. INTRODUCTION

1 The Office for Nuclear Regulation (ONR) has established its Safety Assessment Principles (SAPs) which apply to the assessment by ONR specialist inspectors of safety cases for nuclear facilities that may be operated by potential licensees, existing licensees, or other duty-holders (Ref.1). 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 anticipated transients and accidents. 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. Storage of fuel waiting onward processing or disposal is addressed in TAG 0081 (Ref. 2) and therefore storage of spent fuel is also outside the scope of this document.

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 has a number of duties which relate specifically to fuel performance:

7 LC 14 requires the production of safety cases to justify the design, construction manufacture, commissioning, operation and decommissioning of a facility.

8 LC 20 and 22 require adequate control of modifications which may affect safety.

9 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.

10 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.

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

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

12 The ONR Safety Assessment Principles (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) and WENRA reference level requirements Ref. 4. These documents are considered examples of relevant good practice and should be considered as basic expectations when making ALARP (As low as reasonably practicable) judgements (see TAG 005 ALARP). Key safety requirements taken from Ref. 3 are summarised in Appendix 1. Where a system or component in the reactor core is necessary to fulfil one of these safety functions, this should be specifically addressed in the fuel safety case.

13 WENRA reference levels judged to be particularly relevant to fuel are summarised in Table 1, which identifies the sections of this document in which they are addressed.

14 Common to these source documents is the requirement to preserve, as far as reasonably practical, the integrity of the fuel as a barrier to the release of fission products so that:

- Fuel pellets do not release an inordinate amount of radioactive fission products;
- the fuel does not challenge the integrity of the fuel cladding;
- the integrity of the fuel cladding is maintained under all operating conditions and under transient conditions as far as practicable;
- and failure of fuel cladding does not propagate and result in failure of the reactor vessel or of pressure tubes.

15 IAEA provide a specific guidance document relevant to the design of the reactor core for nuclear power plants (Ref. 5). It is recommended as further reading and has been used extensively in benchmarking this guidance.

16 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 requirements for the reactor core are explained.

4.1 Inherent Safety

17 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.		

18 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.

19 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.

20 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 systems to protect the fuel.

21 Further detailed expectations are given in Section 5 below and in Ref. 5.

4.2 Fault Tolerance

22 This requirement is an extension of the principle of inherent safety to reasonably foreseeable events. Ref. 5 requires 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 requirement:

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

23 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.

24 From the fuel neutronic perspective, this is achieved by ensuring that adequately conservative assumptions are made for reactivity coefficients in the analysis of all design basis accidents and anticipated operational occurrences. The role of core design is to substantiate these assumptions for particular core loading and management strategies.

25 Key reactivity parameters such as reactivity coefficients should be evaluated for each core state and for the corresponding strategy for fuel management, with appropriate allowance for uncertainty; consistent with review and acceptance criteria used in reactor physics testing. See Section 5.4 below.

4.3 Defence in Depth

26 Defence in depth is generally 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 IAEA Design-specific Requirements (Ref. 6). The SAPs contain the following requirement:

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.		

27 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.

28 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.

29 These 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. In the UK, we require that frequent faults should not be expected to result in breaches of the fuel cladding, while anticipated faults in general, should be mitigated without loss of coolable geometry so that dispersal of nuclear material can be minimised and remaining barriers to release preserved.

30 The role of fuel design is to substantiate appropriate design criteria for the fuel so that these functional requirements can be confirmed by fault analysis. 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.

31 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. 6).

4.4 Analysis of Safety Functions

32 As part of the safety case, the SAPs require 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.		

33 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.

34 A fuel safety case should for each significant system structure or component, identify specific functional requirements and provide a structured set of claims arguments and evidence to demonstrate that these requirements are met.

4.5 Reactor Core Design Requirements

35 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.		

36 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.

37 There should be suitable and sufficient margins between the normal operational values of safety-related parameters and the values at which the physical barriers to release of fission products are challenged. 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. 6). See Section 5.4 below.

38 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.		

39 This requirement 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 below.

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.		

40 The SAPs require 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.

41 This requirement elaborates on key principle 2 above. It should be recognised that strong negative feedback can result in challenges to shut-down 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 below.

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.		

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

5. ADVICE TO INSPECTORS

43 Inspectors should consider the following topics in their assessment:

5.1 Fuel Cladding Failure in Normal Operation

44 The functional requirement of the fuel cladding, as set down in IAEA safety standards, is to provide a barrier to the release of fission products in normal operation and anticipated occurrences, or where this is not possible to limit the release of radiation to the environment to acceptable levels. Experience has shown that fuel failures can not 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.

45 Where frequent fuel failures do occur, 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.

46 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

47 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.

48 ONR expects the licensee to include limits and constraints on coolant activity in their operating rules and the inspector should consider whether this is consistent with safety case assumptions and whether the plant can realistically be operated within this limit.

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

50 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.

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

52 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

53 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 mechanical interaction caused by operational transients; and
- Cladding creep failure.

54 The main method by which fuel failure is avoided is the quantification of fuel design limits which ensure fuel integrity.

55 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.

56 It should be recognised that fuel design is essentially empirical. Significant changes in fuel design should therefore be regarded with caution and introduction should be progressive and reversible.

57 Inspectors should verify that introduction of design changes should be supported by a programme of pilot loadings and sufficient relevant operating experience and testing. Furthermore, they should examine the mitigation strategy should the design fail. The industry has a history of examples of undue optimism.

58 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

59 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 AGR and LWR have experienced ill-advised design changes leading to multiple pin failures by flow-induced vibration.

60 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.

61 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).

62 Particular concern is required 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 and suitable measures are required to address this.

63 Similar arguments apply to control-rod assemblies and other in-core components such as neutron sources. These also need justification.

5.3.2 Corrosion, Hydriding and Surface Deposits

64 The inspectors should satisfy themselves 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 anticipated 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 on cladding integrity, the chemistry of the primary circuit needs to be closely controlled. This is an area where interaction with the chemistry assessment is recommended.

For Light Water Reactor (LWR) designs:

- The inspector should be satisfied that the limits on cladding external surface corrosion and the associated hydrogen pickup will be consistent with the discharge irradiation levels. Generally, this will be acceptable if it can be shown that the accumulated oxide layer remained 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 subcooled boiling are required to limit the concentration of radiolysis products in the coolant and to restrict the rate of deposition of crud.

65 Surveillance programmes should be used to ensure that the state of the cladding is consistent with safety case assumptions.

5.3.3 Debris-fretting

66 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.

67 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.

68 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.

69 While the use of fuel assembly debris filters is good practice, they do introduce the risk that ingress of fibrous material (such as insulation) into the coolant has the potential to block the filter and starve the fuel of coolant flow. Discussion with other regulators indicates that it is good practice to exclude potential sources of foreign material from affected areas of the plant by design.

5.3.4 Fuel-pin Closure Welding

70 The inspector should be satisfied that suitable arrangements are in place to qualify and control welding operations on fuel components; end-caps in particular.

71 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.

72 Good practice is to formally qualify the process after any changes and periodically. Checking 100% of the pressurised pins for leaks is also expected.

5.3.5 Design Against Pellet-Cladding Interaction

73 IAEA provide the following guidance: Fuel pellet–cladding interaction, which is stress corrosion cracking caused when the fuel pellet expands and stresses the cladding in the presence of a corroding agent, should be taken into consideration in fuel design.

74 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 anticipated frequent fault transients.

75 Several approaches may be considered for limiting failures due to stress corrosion cracking. For example:

- Tensile stresses may be lowered by means such as limiting the rate of change in power of the reactor;
- A fission product barrier may be placed at the inner surface of the cladding;
- The fission products may be immobilized by means of an additive;
- Local power peaking may be reduced by the appropriate overall design of the core.

76 In Advanced Gas-cooled Reactor (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.

77 For LWR, IAEA advise that, there is an extensive database on operating experience, prototype testing and out-of-reactor testing. However, the phenomenon of stress corrosion cracking is only partially understood in this context. This requires an empirical approach to protection.

78 The failure 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. Failure is prevented by limiting local power levels and rates of power change.

79 Historically, ONR has required deterministic fault studies to demonstrate fuel integrity in frequent fault transients and tolerable radiological consequences in faults assessed as less frequent, but for LWR, ONR has not required the demonstration of tolerance of a single failure of protection. 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. These judgements need to be made for the particular fault, on the available evidence.

80 Manufacturing defects can reduce safety margins in this context. In particular, damage to the pellet surface can lead to short sections of unsupported cladding. Best 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.

5.3.6 Cladding Creep Collapse

81 The inspector should verify that there is suitable substantiation of the fuel design against plastic collapse.

82 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.

83 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.

84 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.

85 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

86 The inspector should verify that a set of design limits consistent with the key physical parameters for each structure, system or component is specified for operational states and design basis accidents (Ref. 6). Advice on key parameters is given below:

5.4.1 Peak Fuel Temperature

87 In all operational states, the peak fuel temperature should be lower than the fuel melting temperature by a sufficient margin to prevent melting of the fuel, with allowance made for uncertainties. This limit 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).

5.4.2 Peak Cladding Temperature

88 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.

89 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.

90 In the UK, a major experimental and analytical programme was undertaken on LWR fuel cladding ballooning as part of licensing 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 verify that there is sufficient evidence to justify the expected level of coolant blockage under the specific conditions anticipated.

91 In the case of gas-reactor fuel, the inspector should verify that the effect of expected levels of insulating surface deposit has been taken into account as appropriate.

5.4.3 Critical Heat Flux

92 In LWR, the cladding surface temperature is generally guaranteed by respecting the critical heat flux[1] limit. Ref. 5 requires that the margin to this limit be demonstrated based

[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,

on experiments encompassing the anticipated range of normal operating and fault conditions.

93 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.

94 ONR has historically required that cladding failure be prevented in frequent faults. The critical heat flux limit has served a role in demonstrating this.

5.4.4 Pin Pressure Limit in Normal Operation

95 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.

96 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.

97 In anticipation of spent fuel storage, the design limits should reflect the design stress and temperature transient assumed for a proposed storage facility and should be set to retain the integrity of the cladding as a barrier to fission-product release when transferred to that facility (Ref. 2).

5.4.5 Limits on structural components

98 The inspector should verify that core components are suitably designed against appropriate design codes.

99 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.

100 The inspector should verify that the analysis takes due account of fatigue and all relevant cracking mechanisms.

101 The loads considered should include those anticipated during fuel handling operations, including anticipated events such and hoist snags and impacts.

102 Historically, the potential for interference between fuel assemblies during core unloading has limited discharge irradiations.

103 The Inspector should verify 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;

---

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.

- 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 loss of coolant accident.

104 The following guidance is based on considerations given in Ref. 5.

105 The clearance within and adjacent to the fuel assembly should provide space to allow for irradiation growth and swelling. However, this needs to be balanced against the need to respect power distribution and hydraulic performance assumptions and limits. In particular, bowing of fuel elements should be limited so that neutronic and thermal-hydraulic behaviour and fuel performance are not significantly affected.

106 As the space between fuel assemblies increases, 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.

107 Design analysis and surveillance programme 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.

108 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

109 The inspector should verify that fuel designer has substantiated key limits taking into account the precautionary principle and has selected the appropriate level of minimum safety margin in consultation with fault study experts.

110 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).

111 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.

112 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 (Ref. 5). The SAPs FA.13-24 relating to evidence should be consulted.

113 Where complex computer codes have been used to quantify safety margins, the inspector should verify that the limits of validity of the codes are demonstrated and adequately documented. TAG 042 should be consulted.

5.6 Core monitoring

114 The Inspector should verify that adequate provision has been made for fuel and core monitoring to ensure that functional requirements are met, including those of fuel handling.

115 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.

116 The requirements for loading and unloading of fuel and core components should ensure that there are sufficient control and monitoring measures are 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 Ref. 7.

117 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 5 requires that the effectiveness of the reactivity control devices such as neutron absorber rods should be checked 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.

118 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.

119 In modern reactor designs, ex-core instrumentation is increasingly replaced with incore 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.

120 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 need either to meet the requirements of appropriate safety classification or diverse means of monitoring need to be provided, with surveillances at appropriate time intervals.

121 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. This should include the potential for fuel misloading in the fuel storage pond and also fuel assembly drop events.

122 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

123 Expectations for management of component ageing and degradation are set down in SAPs EAD.1 to 5. Both IAEA and WENRA 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.

124 The inspector should verify that monitoring, testing, sampling and inspection activities are provided to assess ageing effects and to identify unexpected behaviour or degradation during service.

125 Good practice for fuel is that regular inspection of fuel should take place when it is discharged from reactor and that this should be informed by operational experience and the importance of the component to safety. WERNA reference levels require that this information be securely stored and systematically ordered so as to preserve knowledge. Useful advice in judging good practice is found in Ref. 8.

126 Topics of interest include:

- Irradiation growth and creep;
- Fatigue;
- Corrosion; and
- Fretting damage.

127 See Section 5.3 above.

128 Periodic non-destructive examination of fuel is expected to confirm:

- Safety case assumptions and safety margins;
- Fuel microstructure;
- Isotopic compositions and irradiations.

129 Particular focus should be given to the performance of novel features and of components operating outside the normal experience.

130 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. In particular, distortion of the fuel assemblies (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

131 The inspector should verify that limits placed on key core design parameters are appropriate to providing sufficient safety margin to accommodate anticipated faults. This requirement places active constraints on core design.

132 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 positive.

133 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.

134 In some core designs, the inability to demonstrate adequate dynamic response may be a sufficient reason to refuse a license.

135 Ref. 5 advises that the following parameters which describe the kinetic response of the core are significant:

- The temperature coefficient of reactivity for the fuel,
- The temperature coefficient of reactivity for the coolant,
- The temperature coefficient of reactivity for the moderator,
- The coolant density coefficient of reactivity,
- The delayed neutron fraction,
- The prompt neutron lifetime,
- The effects of power redistribution on reactivity (e.g. the xenon efficiency and the moderator density).

136 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 local power density to enable structural integrity limits to be met.
- 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 anticipated faults.

137 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). Consideration should be given to the resilience of the system to one or more of the shutdown assemblies failing to insert. IAEA standards require that at least one of these two 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. 5 gives details of measures that can be taken to ensure suitable reliability. These are reproduced in Appendix 2.

6. REFERENCES

1) Safety Assessment Principles for Nuclear Facilities. 2014 Edition Revision 0. ONR. November 2014. 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) 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
5) Design of the Reactor Core for Nuclear Power Plant, IAEA Safety Guide, NS-G-1.12, IAEA Vienna 2005.
6) Safety of Nuclear Power Plants: Design, Specific Safety Requirements, IAEA Standards Series No. SSR-2/1 Rev. 1, IAEA, Vienna (2016).
7) Core Management and Fuel Handling for Nuclear Power Plants, IAEA Safety Guide No. NS-G-2.5, IAEA, Vienna (2002).
8) 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
DBA	Design Basis Analysis
DNB	Departure from Nucleate Boiling
IAEA	International Atomic Energy Agency
LWR	Light-water Reactor
ONR	Office for Nuclear Regulation
PWR	Pressurised-water Reactor
PSR	Periodic Safety Review
SAP	Safety Assessment Principle(s)
SSC	Structures, Systems and Components
TAG	Technical Assessment Guide(s)
WENRA	Western European Nuclear Regulators' Association

Table 1: Relevant WENRA Reference Levels		
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

8. APPENDICES

APPENDIX 1: Safety Functions for Reactors.

A review of various reactor designs shows that current design safety requirements can be met by having structures, systems or components that perform the following safety functions:

(1) to prevent unacceptable reactivity transients;
(2) to maintain the reactor in a safe shutdown condition after all shutdown actions;
(3) to shut down the reactor as necessary to prevent anticipated operational occurrences from leading to design basis accidents and to shut down the reactor to mitigate the consequences of design basis accidents;
(4) to maintain sufficient reactor coolant inventory for core cooling in and after accident conditions not involving the failure of the reactor coolant pressure boundary;
(5) to maintain sufficient reactor coolant inventory for core cooling in and after all PIEs considered in the design basis;
(6) to remove heat from the core after a failure of the reactor coolant pressure boundary in order to limit fuel damage;
(7) to remove residual heat in appropriate operational states and accident conditions with the reactor coolant pressure boundary intact;
(8) to transfer heat from other safety systems to the ultimate heat sink;
(9) to ensure necessary services (such as electrical, pneumatic, hydraulic power supplies, lubrication) as a support function for a safety system;
(10) to maintain acceptable integrity of the cladding of the fuel in the reactor core;
(11) to maintain the integrity of the reactor coolant pressure boundary;
(12) to limit the release of radioactive material from the reactor containment in accident conditions and conditions following an accident;
(13) to limit the radiation exposure of the public and site personnel in and following design basis accidents and selected severe accidents that release radioactive materials from sources outside the reactor containment;
(14) to limit the discharge or release of radioactive waste and airborne radioactive materials to below prescribed limits in all operational states;
(15) to maintain control of environmental conditions within the plant for the operation of safety systems and for habitability for personnel necessary to allow performance of operations important to safety;
(16) to maintain control of radioactive releases from irradiated fuel transported or stored outside the reactor coolant system, but within the site, in all operational states;
(17) to remove decay heat from irradiated fuel stored outside the reactor coolant system, but within the site;
(18) to maintain sufficient subcriticality of fuel stored outside the reactor coolant system but within the site;
(19) to prevent the failure or limit the consequences of failure of a structure, system or component whose failure would cause the impairment of a safety function.

APPENDIX 2: Shutdown System Reliability Requirements from Ref. 5

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

(a) Adopting systems that are as simple as possible.
(b) Using a fail-safe design as far as practicable.
(c) Giving consideration to the possible modes of failure and adopting redundancy in the activation of shutdown systems (e.g. sensors or actuation devices). Provision for diversity may be made, for example, by using two different physical trip parameters for each accident as far as practicable.
(d) 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.
(e) Ensuring easy entry of the means of shutdown into the core, with account taken of the in-core environmental effects of operational states and accident conditions within the design basis.
(f) Designing to facilitate maintenance, in-service inspection and operational testability.
(g) Providing means for performing comprehensive testing during commissioning and outages for maintenance.
(h) Testing of the actuation process (or of partial rod insertion, if feasible) during operation.
(i) Selecting equipment of proven design.

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