Transactions, SMiRT-25
Charlotte, NC, USA, August 4-9, 2019
Division VI

UK's REGULATORY SAFETY ASSESSMENT OF NUCLEAR PLANTS PRESSURE PART FAILURE – A MULTI-DISCIPLINE VIEW

Anastasios Alexiou[1], Jim Caul[2], Leslie Smith[3], Diego Lisbona[4]

[1]Principal Inspector, Office for Nuclear Regulation, UK (anastasios.alexiou@onr.gov.uk).
[2]Principal Inspector, Office for Nuclear Regulation, UK (jim.caul@onr.gov.uk).
[3]Principal Inspector, Office for Nuclear Regulation, UK (leslie.smith@onr.gov.uk).
[4]Inspector, Office for Nuclear Regulation, UK (diego.lisbona@onr.gov.uk).

ABSTRACT

Recent ONR experience in safety case assessment has shown the importance of coordinated, multi-disciplinary approaches in the development of resilient designs against Pressure Part Failure (PPF) and their subsequent assessment. In this paper, ONR's structural integrity, internal hazards and civil engineering specialists provide a regulatory perspective on this topic by outlining ONR's expectations and by discussing some key challenges relating to the assessment of PPF. The paper focuses on the methods used for the assessment and characterisation of PPF including classification, quantification of loads and barrier design substantiation in the context of nuclear new build designs which have recently undergone Generic Design Assessment (GDA) in the UK.

INTRODUCTION

The Office for Nuclear Regulation (ONR) is the United Kingdom's (UK) independent regulator of nuclear safety and security. A key requirement of UK law and the ONR regulatory approach is that licensees build, operate and decommission nuclear sites ensuring that risks are reduced "So Far As Is Reasonably Practicable" (SFAIRP) which is viewed as the same as "As Low As Reasonably Practicable" (ALARP) for the purposes of this paper.

The UK generally operates a goal-setting regime rather than the more prescriptive standards based regulatory regimes. ONR's goal setting approach allows licensees (and Requesting Parties (RPs) in the GDA) to be innovative and achieve the required high level of nuclear safety by adopting practices that meet its particular circumstances. It also encourages continuous improvement and the adoption of Relevant Good Practice (RGP). RGP are those standards for controlling the risk judged and recognised by ONR as satisfying the law, when applied appropriately. ONR's regulatory expectations are outlined within the Safety Assessment Principles (ONR SAPs 2014) and associated Technical Assessment Guides (ONR TAGs 2019) – all of which are published and are freely available on the internet. The ONR's enabling approach to regulation involves a constructive approach with duty holders and other stakeholders to enable effective delivery against clear and prioritised safety and security outcomes.

This paper presents ONR's multi-discipline (structural integrity, internal hazards and civil engineering) regulatory expectations relating to evaluating the effects of PPF e.g. failure of vessels and high energy pipework in the context of nuclear new build installations, which have recently undergone GDA in the UK. For each technical discipline, key aspects relating to meeting UK expectations are described. In addition, some significant challenges for the RPs in GDA are outlined and we described how they were overcome. This includes the importance of the application of an integrated approach at an early stage in the design to ensure coherency in the safety case and in its assessment.

DEFENCE IN DEPTH

In line with the international consensus, an appropriate strategy for achieving the overall safety objective includes the concept of defence in depth. This should provide a series of independent barriers aimed at preventing faults in the first instance, and ensuring appropriate protection from or mitigation of the consequences in the event that prevention fails. The aim is to gain confidence in the robustness of the overall design (SAP EKP.3, ONR SAPs 2014).

In the UK, the adequacy of the defence in depth provision in the area of PPF is based on the consideration of the direct and indirect consequences of postulated gross failures on the delivery of nuclear safety functions. Direct effects include the failure of a division/train of the system associated with the failure, whilst indirect effects include, pipe whip, jet impact, missile impact, flooding, pressurisation, blast impact and environmental effects. This usually involves a multi-discipline approach which includes consideration of the pressure boundary integrity (structural integrity), assessment of the direct consequences (fault analysis) and the indirect consequences (internal hazards and civil engineering).

For PPF where gross failure is not discounted a defence in depth approach should be adopted based on a robust consideration of the consequences of failure. The safety case should demonstrate how the defence in depth philosophy has been applied and should also identify any appropriate control measures. Consideration should be given to prevent the hazard occurring, limit the severity of the hazard should it occur, and limit the consequence of the hazard should it occur and be severe. To prevent the hazard occurring all reasonable practicable means commensurate with relevant good engineering practice should be adopted in the design and layout of the plant, and through the use of Systems, Structures, and Components (SSCs) of appropriate capacity and capability.

ONR expects the RPs to consider the unmitigated consequences from hazard scenarios/ faults, and to use these to define the appropriate engineering provisions. SSCs should be defined and classified according to their significance in ensuring nuclear safety.

EXPECTATIONS AND CHALLENGES FROM A STRUCTURAL INTEGRITY PERSPECTIVE

In ONR, the structural integrity discipline primarily considers the confinement safety function associated with pressure boundary components. Accordingly, the majority of the safety significant and/or life limiting SSCs fall within the remit of the structural integrity discipline e.g. reactor pressure vessel, pressuriser, steam generators, reactor primary pump casings and primary and secondary pipework. ONR's structural integrity discipline also encompasses a number of technical areas including metallurgy, material properties and testing, ageing and degradation mechanisms, welding engineering, stress analysis, fracture mechanics and Non Destructive Testing (NDT). For structural integrity, key SAPs include those covering the integrity of metal structures and components; EMC.1 to EMC.34 (ONR SAPs 2014). The SAPs are underpinned by a suite of supporting TAGs which for structural integrity is NS-TAST-GD- 016 (ONR TAGs 2019).

The starting point for structural integrity assessment is the question: "What are the consequences posed by failure?" For example gross failure of a pressure boundary component could lead directly to release of radioactivity from the failed component, and/or the event could be an internal hazard that threatens the integrity of other components.

The principal means of identifying the level of structural integrity demonstration is by consideration of the consequences (direct and indirect) of postulated gross failures. Note that gross failure rather than partial failure is usually the limiting condition and in common with other disciplines is aligned to the achievement of defence in depth in the plant design. The assessment looks for measures taken to underpin structural integrity of a component that are consistent with the consequences of failure.

A robust consequence case is expected in situations where gross failure cannot be discounted. In these situations, the level of defence in depth in the design, in terms of the delivery of the safety functions, informs the plant class of the SSCs and subsequently the selection of appropriate codes and standards. Therefore, compliance with recognised codes and standards may form the primary means of establishing the structural integrity provisions. This notwithstanding, to comply with the need to reduce risks to ALARP, meeting the requirements of recognised design codes and standards may need to be supplemented, if reasonably practicable, e.g. the additional manufacturing controls, inspection and surveillance activities or additional measures to either improve access for inspection or design for "inspectability".

When the estimated likelihood of gross failure needs to be very low or the safety case claims gross failures can be discounted, ONR expects the RP to invoke a highest reliability claim for the SSC. In this situation usually no engineered means of preventing or protecting against the consequences of a postulated gross failure is offered, and so the safety case rests on avoiding the occurrence of the initiating event. Whenever possible, highest reliability claims should be avoided. This is because a case to discount gross failure is an onerous route to a safety case. Notably, the low failure frequency expected goes beyond what may be inferred from the actuarial statistics relevant to the gross failure of pressure vessels and piping designed and constructed to high standards.

These expectations may result in differences with international practices, where Leak Before Break (LBB) or partial failure type claims (e.g. Diameter x Thickness of Pipe / 4 (Dt/4)) are invoked. LBB arguments rely on several assumptions: adequacy of material properties, adequacy of leak detection, defect size, development and stability, time to take mitigating action, and the absence of certain degradation mechanisms e.g. stress corrosion cracking. Therefore, whilst LBB may occur in practice, because of the range of assumptions and uncertainties, it is questionable whether it can be demonstrated reliably to underpin plant design. ONR recognises that LBB type arguments add value, but to meet the need for robust consequence arguments it considers that the primary arguments in a structural integrity case should be founded on sound engineering provision, with LBB providing a secondary argument. This view reflects the need to prevent failure through sound engineering provision and with in-service inspection providing the principal means of providing forewarning of failure and managing potential through-life degradation i.e. the *'known knowns'*, the *'known unknowns'* and the *'unknown unknowns'*.

With regard to partial failure used in some countries, for example the Dt/4 approach, ONR considers that this approach may not represent the failure mode of failure and that the subsequent consequences may not represent the worst case unmitigated scenario for the internal hazards consequences analysis (e.g. internal flooding, pipe whip and combined consequences), which in turn feeds into the classification of the safety measures put in place.

In addition, ONR recognises that the application of "break preclusion" or "no break zone" concepts may include some additional provisions above normal practice to support higher levels of integrity. However, to meet ONR expectation for highest reliability these additional provisions may need to be supplemented with further measures.

Highest Reliability

For metal pressure boundary components operating below the creep temperature region, the main potential failure modes are:

- Rupture of the pressure boundary wall due to a combination of thickness and material i.e. strength not being sufficient to meet the loading demand;
- Failure by propagation of a crack-like defect.

Pressure vessel and piping design codes have for many years dealt with the first failure mode above. Pressure vessel and piping design codes also deal to an extent with the second failure mode above. However, it is this second failure mode that receives close attention in assessment of those structures and components where the RP discounts gross failure.

To underpin a highest reliability claim, ONR expects a demonstration of integrity based on sound engineering provision with measures over and above normal practice defined in nuclear codes and standards. Typically these additional measures include but are not limited to:

- The use of proven materials and manufacturing processes.
- Direct fracture toughness testing of representative materials in manufacture and where appropriate through-life via a material surveillance strategy e.g. irradiation embrittlement.
- Fracture analyses (defect tolerance assessment) with a margin between the limiting defect size and defects that could be present in the component accounting for in-service growth (avoidance of fracture demonstration)
- Design for access and inspectability.
- High reliability (qualified) NDT performed during manufacture and prior to (and during) service integrated with Defect Tolerance Assessment (DTA) to show tolerance to defects that may be present.
- Enhanced quality assurance/control measures; provision for an "intelligent customer capability" along with the development of arrangements for third party independent surveillance of design and manufacturing activities.

Taken together these measures provide "conceptual" defence in depth. These expectations derived in part from precedents, in particular, the recommendations of the Light Water Reactor Study Group circa 1978 and 1982 (United Kingdom Atomic Energy Authority 1982) and the conclusions of the Sizewell B public inquiry relating to the integrity of PWR vessels (Sizewell B Public Inquiry 1987). Indeed, they address public concerns raised during the introduction of civil Pressurized Water Reactor (PWR) technology to the UK and cover measures to infer a lower failure frequency for pressure vessels built to high standards. The measures include fracture analyses (DTA) using an elastic-plastic approach beyond for example the fracture assessment used in established design codes along with qualified inspections to detect defects of structural concern with high reliability.

The following examples cover some key challenges from a structural integrity perspective. This is not an exhaustive listing rather; the examples serve to illustrate some common difficulties encountered in structural integrity assessment of new reactor designs.

Selection of Codes & Standards

ONR's expects that the safety case identifies the role and importance (safety functions) of SSC in maintaining nuclear safety, which leads to classification and subsequently the measures that will be taken to assure structural integrity through-life (SAPs ECS.1 to ECS.3, ONR SAP 2014). Thus SSCs important to safety should be designed, manufactured, constructed to the appropriate standards. The RP is responsible for the selection of appropriate codes and standards.

Nuclear pressure vessel design and construction codes such as ASME III (The American Society of Mechanical Engineers) and RCC-M (2007) (French Association for Design, Construction and In-Service Inspection Rules for Nuclear Island Components) set out a range of requirements (design construction and in-service inspection) graded in accordance with the level of assurance required: e.g. Class1/M1 (Highest level); Class 2/M2 (Intermediate level); and Class 3/M3 (Lowest level).

ONR experience is informed by Sizewell B, with SSC classification based upon the guidance with prescribed SSC classifications e.g. ANSI 18.2 (1973) (American National Standards Institute) and ANSI/ANS 51.1 (1983) (American National Standard). The current approach in the US is defined in the Nuclear Regulatory Commission (NRC) Guide 1.26 (2017), which provides component classification using the function to define the required quality level, which then inform the nuclear pressure vessel class. The SSC classification methodology may be different in other regulatory regimes. For example, for the EPR the safety class is based on both function and the operating conditions/barrier role. Using this methodology there is the potential for safety class 1 and 2 components to be designed and manufactured to a lower level of quality assurance than would be expected from existing UK experience. This may or may not be appropriate.

The salient point is that the basis for the safety class and design code provisions needs to be established in the safety case. A classification scheme based on the delivery of safety functional requirements affords the flexibility to assess a wide-range of reactor designs, but the output is dependent on the assumptions used e.g. LBB versus gross failure. Alternatively, the rationale for the SSC safety class needs to be justified, in particular, if a change in the SSC safety class (and hence code class) is proposed, it needs to be established whether the proposed change is founded on a justified change in the safety functional requirements or is an artefact of the safety classification methodology. RP's have responded to this challenge by either justifying their proposed code and construction class designations or raising the design and construction codes designations.

Whilst compliance with recognised codes and standards usually forms the primary means of establishing the structural integrity provisions, ONR does not prescribe codes and standards and so the RP must propose codes and standards for the design, construction and inspection of SSC. This is a challenge for a non-prescriptive regulator. If, in the opinion of ONR, the proposed codes and standards are considered as RGP, ONR will focus the assessment on the application of those standards. However, if the RP proposes codes and standards that are not familiar to ONR or if novel or internal company methods are adopted then, ONR will focus on both the basis of the approach and its application. This does not mean that there are difficulties with the proposed codes and standards, but ONR needs to have confidence in the proposed provisions. The aim is to establish that the proposed codes and standards provide structural integrity provisions which are consistent with RGP. This approach offers flexibility and a means to establish the suitability of the proposed codes and standards for a wide range of reactor designs. In some cases, ONR has undertaken broad comparisons of code and standards against relevant RGP to establish the suitability of the duty holder's proposals (e.g. during GDA for the UK EPR™ design, (ONR Technical Assessment Reports 2011)).

ONR also expects the intelligent application of codes and standards. Specifically, prior to applying a code or standard, the RP should identify the failure mechanisms of concern and show how these are addressed in the chosen code or standard.

Avoidance of Fracture Demonstration

ONR SAP EMC.1 includes the expectation that the safety case is robust and the corresponding assessment suitably demanding, in order to properly inform engineering judgement that:

- The metal component or structure is defect-free as possible;
- The metal component or structure is tolerant of defects.

For GDA these expectations are achieved through the RP demonstrating confidence in the achievement of adequate material properties and quality during manufacture. In addition, an approach based on an "avoidance of fracture" demonstration was developed to show defect tolerance for highest reliability structures and components. This approach integrates defect tolerance calculations for limiting defect sizes, predictions of fatigue crack growth, with qualified inspections (examination) and conservative material properties confirmed through planned direct fracture toughness testing, see Figure 1 below.

A "margin" can be expressed as the ratio of the limiting defect size, corrected for fatigue crack growth, to the size of defect that can be found with high confidence by NDT. Typically, based on custom and practice, a margin of 2 is used. Code-based inspections may not deliver the high confidence required in the NDT to detect defects of structural concerns and consequently additional measures are applied. These measures include qualifying the procedures, equipment and personnel to confirm the inherent capability of the NDT system to detect and reject defects of structural concern. In this context, the inspections are considered to be "objective based" where the aim of the qualification is to demonstrate that the NDT system has high performance against defects that have predefined sizes (determined from DTA) and predefined characteristics (location, orientation and roughness). Additional quality measures such as repeat inspections and enhanced witnessing are also applied during the site application to enhance the confidence in the NDT.

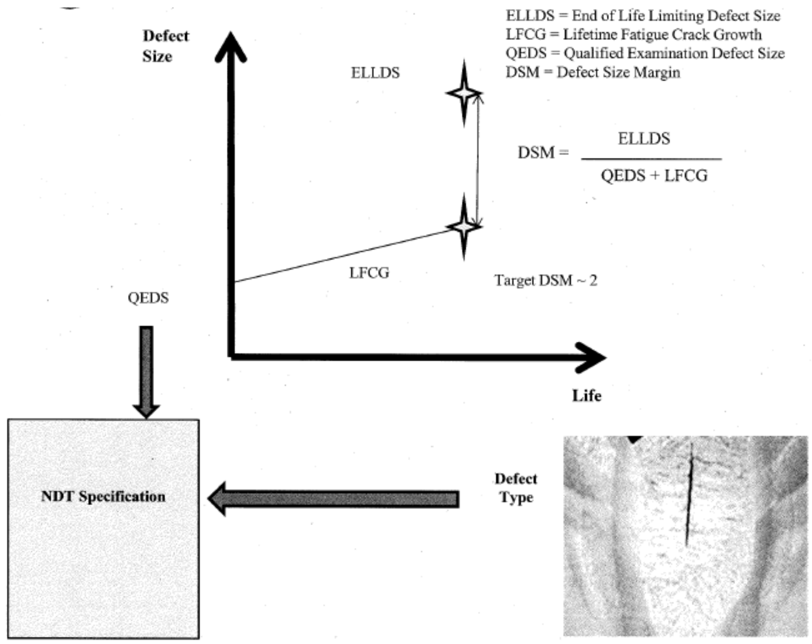

Figure 1. Avoidance of Fracture Demonstration.

An essential aspect is to ensure that, as far as is reasonably practicable, the components are designed to promote the reliable NDT. For example, where ultrasonic inspection is the NDT method, it is expected that materials are suitably transparent to ultrasound and that there is sufficient straight section to scan probes. In the UK, reactor designers have modified features of the reference design to improve inspectability to meet these expectations.

ONR expects evidence-based safety cases which are presented in a usable form for the future licensee. The presentation of adequate evidence is particularly important for the structural integrity case when the RP needs to develop a case for “highest reliability”. The development of a structural integrity case for highest reliability components and structures is relatively straightforward for UK based licensees who are well aware of precedent and expectations, but this presents quite a challenge for non-UK based RPs. RPs have addressed this challenge by presenting their safety cases, typically with a claims, argument, and evidence structure.

Overall, ONR expects conservative defect assessment calculations, but equally there should be reasonable demands placed on inspection, qualification and achievement of material properties. A balanced demonstration of defect tolerance is therefore sought. RPs have overcome these challenges by developing new approaches, validating their methods and by exercising sound engineering judgement to ensure that avoidance fracture demonstration is both conservative and achievable in practice. In general, RPs have adapted well to these challenges and their progression has often benefited from the support of UK expertise notably in the areas of defect assessment and the development of part technical justifications to support confidence in the achievement of inspection qualification for GDA.

Whilst the primary aim of a highest reliability claim is to either discount gross failure or infer a very low failure frequency for the structure or component, the additional measures have proven valuable in addressing emergent problems e.g. high reliability NDT undertaken for Sizewell B provided good evidence to show the absence of hydrogen flakes identified in Doel 3/Tihange 2.

EXPECTATIONS AND CHALLENGES FROM AN INTERNAL HAZARDS PERSPECTIVE

Internal hazards are those hazards to plant, structures and personnel which originate within the site boundary but are external to the process in the case of nuclear chemical plant or primary circuit in the case of power reactors.

This paper is focusing on the PPF aspect of high energy systems and components (≥ 2 MPa or ≥ 100^{o}C (IAEA 2004)) that could result in both dynamic (such as pipe whip, jet impingement, spray, flooding, steam release, missiles) and environmental effects (such as temperature and pressure effect).

ONR's expectation in internal hazards are outlined in the "External and Internal Hazards" SAPs series EHA (ONR SAPs 2014). SAPs are considered holistically for all ONR assessments including in internal hazards. ONR's specific TAG for internal hazards is NS-TAST-GD- 014 (ONR TAGs 2019). ONR's assessment of a design against PPF and in particular the characterisation of the indirect effects of high energy pipe failure focuses on the following distinct steps:

Identification of Sources

In a typical nuclear power plant there are numerous locations where high energy components exist inside and outside containment. ONR expects a systematic identification of all high energy pipes followed by appropriate screening out of scenarios that make no contribution to the overall risk and therefore focusing on those that may have hazardous consequences to the buildings structures and SSCs delivering Fundamental Safety Functions (FSFs) (SAPs EHA.1 and EHA.19, ONR SAPs 2014). The identification should also include moderate energy lines with temperature and pressure energies close to the threshold of high energy lines (cliff-edge effects) and with consideration of all potential pipe to pipe interactions.

The identification of credible bounding scenarios has proven very challenging to a number of RPs due to the large number of potential scenarios and the complexity involved. In GDA, the RPs managed to overcome these difficulties by developing specific robust criteria of selection of bounding scenarios and room by room application of these criteria. Furthermore, appropriate justification of those scenarios excluded was provided.

Identification of Structures, Systems and Components

A key aim of nuclear plant safety cases is demonstrating that SSCs important to safety are protected from the effects of internal hazards and that there is sufficient redundancy, diversity and segregation of SSCs to continue to deliver the FSFs in all operational states and hazard conditions. PPF of high energy lines has the potential to challenge the SSCs delivering FSFs, which prevent detrimental nuclear safety effects such as radiological releases. During this step of the analysis all SSCs that could be potentially affected by the high energy lines failure should be identified (SAP EHA.5, ONR SAPs 2014).

Characterisation of Consequences

During this step all dynamic and environmental consequences associated with the PPF of high energy lines should be characterised using suitable tools and methods. The guidance available in ANSI/ANS 58.2 (1988) (withdrawn) has been widely used internationally to quantify the dynamic effects such as pipe whip and jet impact.

ONR's regulatory approach seeks to obtain confidence that the risk of the unmitigated worst case scenario (e.g. assuming the worst plant state and hinge location, no restraints, longest length or unrestrained pipe or sweeping angle) is reduced ALARP. In demonstrating ALARP, ONR considers that the analysis undertaken based on ANSI/ANS 58.2 (1988) standard should be supplemented by additional analyses, including sensitivity studies relating to key assumptions, addressing the following topics:

- The assumed break size should be based on guillotine failure (gross failure). The expectation is that the safety case should demonstrate that the design can accommodate the consequences of gross failure, or otherwise that the pipework or components are classified as highest reliability.

- The assumed break location should include all potential break locations to derive a bounding case. Break locations should include terminal ends, intermediate locations due to high stress areas or welding locations as well as locations where a high energy line is in close proximity to SSCs delivering the FSFs or highest reliability components.
- All high energy systems should be considered including those which temporarily operate in high energy modes (i.e. low utilisation lines).
- Domino effect; pipe to pipe interaction.

ONR expects that all dynamic and environmental effects (e.g. pipe whip, jet impact, missiles, steam release, flooding and pressurisation) and their impact on nuclear safety significant plant should be studied individually and in combination.

The above expectations have been very challenging to a number of RPs entering GDA for a number of reasons including the design of the plant excluded a number of systems from gross failure (such as main steam and feed water systems) or that the layout was not fully optimised against internal hazards, or that the analysis was not based on true pipework layout or room dimensions. An area of particular challenge was the quantification of the combined consequential effects of high energy pipe failure and the requisite substantiation of barriers, and these are discussed in the sections below.

The effects of the consequences are commonly modelled utilising analytical computer models (from simplified empirical equations to complex computational fluid dynamic model) to predict the local and global effects. The predicted loads are sensitive to the granularity of the model used and therefore it is important to understand the basis of the model, any underlying data used, the history of its development, and evidence of appropriate verification and validation (SAPs AV.2 to AV.6, ONR SAPS 2014). Nevertheless, the timing of each consequential effect (e.g. pipe whip, jet impact, flooding and pressurisation) may play a part in the engineering substantiation of multi-hazard barriers. Any assumptions on timing and duration should be based on robust consequence assessment, the layout of the plant in question, and the qualification and proven performance of the SSCs under the conditions of the hazard. For example, for a steam release scenario the time to isolation should be based on valve performance characteristics and the time to peak compartment pressure, if used, should be based on analytical pressure relief calculations relevant to the compartments in question.

In addition, the analysis should also take into consideration any deterioration or damage to safety related SSCs after being subjected to each of the various consequences and determine how its performance and subsequent withstand is affected. For example, a structure that has been subject to a pipe whip could have reduced withstand as a result of damage. If this structure was then subjected to pressurisation due to steam release or due to a hydrostatic load due to flooding it could ultimately result in a failure of the structure. Therefore, for a combined load event it is the net effect of the consequences that could result in a failure of a system or structure, even if individual withstands can be demonstrated.

In recent GDAs, RPs successfully managed to overcome the above challenges by undertaking additional analysis including sensitivity analysis for a number of key systems that were excluded from gross failure consequences analysis.

Identification of Safety Measures

ONR's experience of assessing safety cases from differing nuclear power plant designs suggest that it is often easier to make compelling safety cases if designers are "hazard aware" at the early concept stage of a design (i.e. adopting inherently safe design options). This can lead to a simpler and more robust set of "hazard informed" layout decisions, with improved alignment between the rooms in differing floors, with simpler near-monolithic primary hazard barriers, and with a reduced number of penetrations though primary hazard barriers. Many designs, however, appear to have internal hazards considered as an afterthought and although acceptable safety cases can be constructed these may be more complex, and potentially less robust. Limiting the consequences of PPF can be, therefore, ensured by good plant layout principles, from the outset of the design (inherent safe design), and by protecting the plant from the hazard loadings. The latter should be generally achieved by the provision of robust passive barriers which withstand the maximum credible loadings and segregate safety systems that allow the continued delivery of FSFs. ONR, therefore, expects nuclear plants to show hazard resilience by means of layout optimisation and segregation of redundant and diverse safety systems (SAPs EDR.2, ESS.18 and ELO.4, ONR SAPs 2014). Approaches based entirely on separation by distance or heavily reliant on SSCs qualification may be challenging to substantiate in the absence of suitable segregation. This is particularly true for areas inside the containment where full segregation of SSCs delivering the FSFs by barriers is not feasible. In such cases a safety case could still be made utilising multi-leg claims and arguments and by taking credit of geometry and partial protection including partial barriers.

With respect to pipe whip, the extent of whipping can be reduced or eliminated by appropriate restraint design, which should be substantiated against the forces exerted. Other safety measures may include jet shield, blow out panels and/ or isolation valves to mention but a few. All safety measures should be supported by adequate design substantiation.

Substantiation of Safety Measures

A key safety measure against PPF in many nuclear power plant designs is the provision of reinforced concrete barriers (including penetrations), which are designed against a number of internal hazards (i.e. multi-hazard barriers). Substantiation of concrete barriers is covered in the next section.

Substantiation of other safety measures claimed in PPF and in particular on high energy pipes failure such as restraints, jet shields and blow out panels should be provided proportionate to the function of the safety category that they provide and classification assigned. This will require appropriate coordination with other disciplines such as mechanical engineering and civil engineering.

EXPECTATIONS AND CHALLENGES FROM A CIVIL ENGINEERING PERSPECTIVE

In order to ensure robust design of civil engineering structures as barriers to protect SSCs from multi-hazard threats and contribute to defence in depth, careful multi-disciplinary development of the plant layout, assumptions, and definition of the relevant hazards and their incidence is required. The analysis may be complex and involve advanced or bespoke methods of modelling and calculation requiring special verification and validation.

ONR’s civil engineering expectations on the robustness of structural barriers are outlined in the “Civil Engineering” SAPs series ECE and in particular in ECE1 and ECE.6 (ONR SAPs 2014). The applicable civil engineering TAG is NS-TAST-GD- 017 (ONR TAGs 2019).

Loads from the indirect effects of PPF can credibly combine, which could compromise the integrity of the multi-hazard barriers. ONR expects that initially, the utilization of multi-hazard barriers as a result of each individual hazard load and the residual withstand capacity should be determined analytically. This should, in turn, inform the analysis of the response of multi-hazard barriers to the combined consequential effects of PPF. As the hazard sequence is considered, it may be the case that partial or complete failure of the barriers (e.g. perforation or scabbing) are predicted when utilization is determined analytically. In these cases, ONR’s expectation is that reasonably practicable measures to prevent the failures are implemented in line with UK regulatory requirements to avoid undesirable secondary effects, and that delivery of FSFs is still achieved.

Where structural analyses have been carried out on civil structures to derive static and dynamic structural loadings for the design, the methods used should be adequately validated and the data verified. The data used in structural analysis should be selected or applied so that the analysis is demonstrably conservative. When selecting which model type to use for the analysis and the standards for design of nuclear structures the nuclear safety function category and classification and the seismic classification need to be considered. It is important that these are identified at an early stage in the design although they may be modified at later stages in the process should additional nuclear safety claims be identified as design development progresses.

There is an increased expectation that the industry adopts the use of 3D Finite Element Modelling to model structures. ONR expects that relevant procedures should be selected based on the required accuracy to demonstrate the design limits and unmitigated consequences of failure. 3D Finite Element Modelling more accurately estimates the design loads on a structure thus allowing a higher degree of confidence that the structural withstand is sufficient to deal with the threat the hazard poses. Simpler models are often suitable to provide the global response of structures and may be suitable for use in the design of simple structures or preliminary scoping.

It is of course appropriate to ensure that barrier withstand is proven for all potential barrier failure modes following consideration of all credible combined loads of the PPF. Where the safety function of a structure provides a principal role in ensuring nuclear safety, predicted failure modes should be gradual, ductile and, for slowly developing loads, detectable. The loadings assumed should take account of uncertainty in the underlying fault or hazard specification.

Engineering design codes and standards such as ACI 349 (2014) (American Concrete Institute) specify load combinations, load factors and acceptance criteria for use in the design of concrete barriers. These are generally applicable to nuclear power plant design but careful consideration of the appropriateness of these in the potentially complex scenarios that may arise due to combinations of hazards is required. The required safety functions and structural performance of the civil engineering structures under normal operating, fault and accident conditions should be specified and the required resilience should be quantified and specified. To preclude cliff-edge effects, margins to failure should extend beyond design basis fault (or hazard) loadings. Beyond design basis loading considerations should be included before the structural design is finalised. The combining of different codes and standards for a single aspect of a SSC should be avoided so far as is reasonably practicable. Where this cannot be avoided, the combining of the codes and standards should be justified and their mutual compatibility demonstrated.

The combined impact of PPF on multi-hazard barriers has proved challenging for a number of RPs. This challenge relates to the assumptions used in the characterisation of the loads (e.g. break size, break locations, pipe to pipe interactions, exclusions of systems due to low utilization, combined consequential loads quantification) and the demonstration of adequate margins of safety. Therefore, care must be exercised when evaluating the hazard loads and in particular the loading/ magnitude of the combined consequences of PPF, the duration it is applied, and sequencing of the occurrence. In recent GDAs, the availability of SSCs delivering the FSF ensured by modifications to the designs such as improvement to layouts, strengthening of barriers and incorporation of additional restraints. Coordination with ONR specialists, structural integrity, internal hazards and civil engineering disciplines is essential.

MULTI-DISCIPLINE APPROACH

In the sections above the expectations and challenges within structural integrity, internal hazards and civil engineering disciplines in assessing the effects of PPF were outlined.

The emphasis in the assessment of new build is placed on reducing risk at the design stage; in particular, by influencing improvements, where appropriate, in the design provisions and by developing the RP’s understanding of ONR’s expectations to inform the development of their methods, if appropriate, to meet UK expectations. However, in the assessment of PPF there are many challenges that are common to all three disciplines including demonstration of ALARP and the achievement of coherency in the assessment.

ALARP Demonstration

Demonstration that the risks are ALARP generally involves designers and licensees' carrying out hazard and risk analysis, identifying and implementing measures that demonstrate either that the hazard has been eliminated or that the risks have been sufficiently reduced. ALARP demonstration also requires optioneering studies, which identify further measures that could be implemented and the level of risk reduction that would be achieved. Compliance with the law requires all such design options and measures to be implemented unless their costs in terms of time, trouble, and money are demonstrably grossly disproportionate in relation to the risk averted. The process involves balancing the benefits and detriments of implementing measures to reduce risk. These balances may be specific to a particular discipline, but could also include other technical disciplines e.g. for PPF the consequences (direct and indirect) analyses inform the structural integrity classification.

In most cases demonstrating risks are ALARP is not done through explicit comparisons of costs and benefits. ONR's assessment involves benchmarking against RGP with the rigour in the safety case and in ONR's assessment proportionate to the FSF category and safety classification of the SSCs. The demonstration that designs reduce risks ALARP has proven to be a challenging concept to RPs who are more familiar with prescriptive regulatory regimes (e.g. in France, US, Japan and China). ALARP demonstration in the area of PPF is a multi-discipline team effort where input from internal hazards, structural integrity and civil engineering (to mention but a few), is critical to ensure that the SSC design is appropriate to the level of challenge posed by the combined loads in PPF. Therefore, a particular challenge often includes balancing the competing needs of various relevant disciplines demonstrating the integrity of highest reliability SSC, the suitability of the layout and the location of reinforced barriers and penetrations (such as doors), and the adequacy of restraints and blow out panels.

To assist duty holders to meet their legal obligations, ONR provides advice and guidance. However, ultimately under UK law, duty holders are responsible for safety. In this respect, UK based technical support organisations who are more familiar with the UK regulatory regime and expectations may be able to provide sound advice to RPs.

Coherence in the Assessment

A further common challenge relates to ensuring coherency between the structural integrity case, consequences analyses and the reliabilities inferred from the categorisation of the FSFs and classification of SSCs (SAPs ECS.1 to ECS.5, ONR SAPs 2014).

To achieve coherency in the safety case and its assessment, the claims, arguments and evidence needs to be integrated across the technical disciplines. For example, a challenge for the substantiation of the withstand capability of barriers is to assess whether the sequence and timing of these demands on the barriers affect their integrity. This type of analysis is complex and may require input from a number of disciplines such as structural integrity, internal hazards and civil engineering.

Indeed from ONR's experience, it is clear that an integrated approach is necessary at an early stage in the assessment of the design of SSCs to ensure that the potentially conflicting requirements of nuclear safety, security, safeguards, fire and conventional safety are taken into account while ensuring that the measures adopted do not compromise one another. This approach may involve several iterations in order to develop the design and represents relevant good practice reflecting guidance and requirements in internationally recognised standards.

Existing safety cases for the reactor designs usually include consideration of the direct consequences through linkage to fault studies e.g. frequent, infrequent failure/design basis failure, but there can be challenges for the internal hazards assessment when gross failure had not previously been considered. This is because other regulatory regimes may allow a default assumption that pressure equipment designed to a nuclear design code will not fail in a catastrophic manner, which leads to plant designs based on partial rather than gross failures.

As an illustration, the integration of structural integrity claims with the internal hazards discipline has proved problematic across the UK EPR™ (ONR Technical Assessment Reports 2011), the AP1000® (ONR Technical Assessment Reports 2011) and the UK ABWR (ONR Assessment Reports 2017) GDAs. The issues here relate to assuring consistency in the assessment of the consequences of gross failure. These consequences include the direct consequences associated with the loss of the pressure boundary (e.g. loss of the safety functions), which tends to involve interactions with fault studies, Probabilistic Safety Analysis (PSA) and fuel and core. Whereas the indirect (or secondary) consequences involve internal hazard specialists as the concerns relate to the effects of flooding, pressurisation, pipe whip, jet impingement, missiles and environmental qualification, and civil engineering on the suitability of the multi-hazard barriers.

In conclusion, disciplines need to work together to ensure consistency in the development of the safety case and in its subsequent assessment. If the classification of a SSC changes then all disciplines need to be informed so that the implications can be assessed. For example, a SSC classified as highest reliability means that the direct and indirect consequences no longer warrant detailed consideration because the gross failure is discounted. In contrast a change in the classification from highest reliability to a non-highest reliability claim is significant because the consequences of a postulated failure now warrant consideration. Notably, the loads and conditions arising from the postulated failure of the SSC may be important to the delivery of the safety functions and the integrity of other highest reliability structures and components.

CONCLUSIONS

The UK regulatory regime follows a non-prescriptive approach. A key requirement of UK law and the ONR regulatory approach is that licensees build, operate and decommission nuclear sites ensuring that risks are reduced SFAIRP. Other key differences, compared to other regulatory regimes, include the expectations relating to the purpose of the safety case and the underlying assumptions to achieve defence in depth in the plant design e.g. the role of LBB.

In this paper, the UK approach has been illustrated through a regulatory perspective on the assessment of PPF, which has been informed by the collective experience of ONR's structural integrity, internal hazards and civil engineering specialists in assessing new build reactor designs during GDA.

ONR has some specific expectations relating to the structural integrity of metallic components and structures. Notably, although compliance with recognised codes and standards may form the primary means of establishing the structural integrity provisions, these may need to be supplemented to meet UK law i.e. to reduce risks SFAIRP or to meet expectations relating to the inference of highest reliability, which are informed by UK precedents.

From an internal hazards perspective, the consequences analysis for PPF of high energy lines along with the provision of robust safety measures has been proven challenging to a number of RPs during GDA due to the complexity of the direct and indirect consequences analyses. RPs have overcome this challenge through additional work to satisfy ONR's expectations, which in collaboration with civil engineering included identification and substantiation of safety measures such as restraints and barriers and changes to layout.

ONR's experience attests to the importance of early multi-disciplinary assessment of the classification, identification of bounding scenarios, consequences analyses and identification of robust safety measures including substantiation of them. It is essential that all technical disciplines communicate effectively to ensure coherency in the safety case and its assessment.

REFERENCES

American Concrete Institute (2014). “Code Requirements for Nuclear Safety Related Concrete Structures and Commentary”. *American Concrete Institute. ACI 349-13*.

American Nuclear Society (1988). “Design Basis for Protection of Light Water Nuclear Power Plants Against the Effects of Postulated Pipe Rupture”. *American National Standard*. *ANSI/ANS-58.2*.

American National Standards Institute (1973). “Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants”. *American National Standards Institute*. *ANSI N18.2*.

American Nuclear Society (1983). “Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants”. *American National Standard. ANSI/ANS 51.1*.

International Atomic Energy Agency (2004). “Protection against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants Safety Guide”. *IAEA Safety Standards Series NS-G-1.11*.

Office for Nuclear Regulation (2014). “Safety Assessment Principles for Nuclear Facilities”, Revision 0. http://www.onr.org.uk/saps/.

Office for Nuclear Regulation (2019). “Technical Assessment Guides”. http://www.onr.org.uk/operational/tech_asst_guides/index.htm.

Office for Nuclear Regulation (2011). “Step 4 Technical Assessment Reports EDF & AREVA UK EPR™ Reactor”. http://www.onr.org.uk/new-reactors/uk-epr/reports.htm.

Office for Nuclear Regulation (2011). “Step 4 Technical Assessment Reports, Westinghouse AP1000®” http://www.onr.org.uk/new-reactors/ap1000/index.htm.

Office for Nuclear Regulation (2017). “Step 4 Assessment Reports UK ABWR Reactor”. http://www.onr.org.uk/new-reactors/uk-abwr/reports.htm.

RCC-M (2007). “Design and Construction Rules for Mechanical Components of PWR Nuclear Islands”. Published by the French Association for Design, Construction and In-Service Inspection Rules for Nuclear Island Components – AFCEN. Paris.

Sizewell B Public Inquiry (1987). “Report by Sir Frank Layfield”. Volume One Part I, HMSO, ISBN 0 11 411575 3. London.

The American Society of Mechanical Engineers (ASME). “Boiler and Pressure Vessel Code Section III: Rules for Construction of Nuclear Facility Components”.

United Kingdom Atomic Energy Authority (1982). “An Assessment of the Integrity of PWR Pressure Vessels”. Summary Report. Second Report by a Study Group under the Chairmanship of Dr W. Marshall.

US Nuclear Regulatory Commission (2017). “Regulatory Guide 1.26: Quality Group Classifications and Standards for Water, Steam and Radioactive-Waste Containing Components of Nuclear Power Plants” Revision 5, Washington DC, USA.