Transactions, **SMiRT-26**
Berlin/Potsdam, Germany, July 10-15, 2022
Division 06

UK's REGULATORY SAFETY ASSESSMENT OF NUCLEAR PLANTS HIGHEST RELIABILTY COMPONENTS – A MULTI-DISCIPLINE VIEW

Anastasios Alexiou[1], Jim Caul[2], Leslie Nyogeri[3]

[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]Inspector, Office for Nuclear Regulation, UK (leslie.nyogeri@onr.gov.uk).

ABSTRACT

ONR has previously shared its assessment approach in the area of Pressure Part Failure (PPF) from high energy lines where demonstration of defence in depth provisions requires consideration of the direct and indirect consequences of postulated gross failures of high energy components. This paper describes a multi-discipline approach in the assessment of firstly the quantification of the indirect consequences of pressure boundary components to inform the classification or otherwise of highest reliability components and secondly the assessment of the quantification of the potential threat posed by internal hazards to those components that have been classified as highest reliability components.

INTRODUCTION

The Office for Nuclear Regulation (ONR) is the United Kingdom's (UK) independent regulator of nuclear safety, nuclear site health and safety, nuclear security, nuclear safeguards and safety of transport of nuclear and radioactive materials. A key requirement of UK law and the ONR regulatory approach is that licensees design, build, operate and decommission nuclear sites to ensure 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.

To regulate nuclear safety, the UK generally operates a goal-setting regime rather than the more prescriptive standards-based regime. ONR's goal setting approach allows licensees (and Requesting Parties (RPs) in the GDA process) to be innovative and achieve the required high level of nuclear safety by adopting practices that meet its circumstance. 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 2021 – all of which are published and are freely available on the internet. The ONR's enabling approach to regulation encourages open and constructive dialogue with duty holders and other stakeholders towards effective delivery against clear and prioritised safety and security outcomes.

This paper presents a structured approach in line with ONRs regulatory expectations for the assessment of those systems structures and components (SSCs) that a licensee or duty holder assigns as highest reliability components and includes the consideration of the internal hazards impact on them.

GENERAL SAFETY CASE EXPECTATIONS

Inherently Safe Design

In the first instance the underpinning safety aim for any nuclear facility should be an inherently safe design, where the design avoids radiological hazards rather than controlling them (SAP EKP.1, ONR SAPs 2014). However, where an inherently safe design is not achievable, the design needs to demonstrate that it is tolerant to faults and hazards, such that if a fault/ hazard occurred the design is able to reach a safe state and the risk to nuclear safety is ALARP (SAP EKP.2, ONR SAPs 2014).

To achieve the demonstration of a fault/ hazard tolerant plant, ONR expects a safety case to consider the unmitigated consequences from faults/ hazards scenarios, and to use these to define the appropriate engineering provisions. SSCs should be defined and classified according to their significance in ensuring nuclear safety.

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 to prevent faults occurring in the first instance, and if a fault occurs ensuring appropriate protection or mitigation measures are in place to ensure the risk is ALARP. The aim is to gain confidence in the robustness of the overall design (SAP EKP.3, ONR SAPs 2014). The highest level of protection with respect to defence in depth principle is through the optimisation of the design and layout.

Layout

ONR expects that the design and layout of the site, its facilities (including the enclosed plant), support facilities and services should be such that the effects of faults and internal hazards are minimised. This includes minimising the direct effects of internal hazards on SSCs and minimising any interactions between a failed SSC and other SSCs. The purpose of this is to demonstrate that the overall layout of the plant and equipment is optimised to eliminate or minimise (if elimination is not practicable) the impact of internal hazards (SAP ELO.4, ONR SAPs 2014). This can be achieved through conservative design, construction, maintenance, and operation in accordance with appropriate safety margins, engineering practices and quality levels.

Safety Functions and Measures

Where limitations of layout are identified and additional defence in depth measures are required to minimise the impact of faults/ internal hazards a safety function is identified. A safety function is a duty that is required in the interests of nuclear safety either during normal operation or following a fault or hazard (including internal hazards). These functions are categorised on their significance to nuclear safety based on consequences of failure to deliver the function, likelihood of calling upon the function and the extent to which the function is required to prevent, protect or mitigate (SAP ECS.1, ONR SAPs 2014).

Safety functions (both for normal operation and in fault/ hazard scenarios), are delivered by SSCs. The SSCs delivering the various safety functions are classified based on the category of the safety function being delivered, likelihood that the item will be called upon, potential for failure to initiate a fault and demand to perform its function (SAP ECS.2, ONR SAPs 2014) and the radiological consequences from the associated faults/ hazards. The classification of SSCs therefore reflects the consequence (direct and indirect) of postulated gross failure. This involves a multi-disciple approach including structural integrity (metallic SSCs), fault studies (direct consequences) and internal hazards/ civil engineering (indirect consequences).

STRUCTURAL INTEGRITY PERSPECTIVE

In ONR, the structural integrity discipline primarily considers metallic SSCs, which includes 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 and includes components such as the reactor pressure vessel, pressuriser, steam generators, reactor primary pump casings and primary and secondary pipework. These types of SSCs have the highest safety functional requirements assigned, because their failure would significantly impact nuclear safety. It is ONR's expectation that the design of the plant is demonstrated to be tolerant as far as is reasonably practicable to the failure of such SSCs. For structural integrity, key SAPs include EMC.1 to EMC.3 (highest reliability) and EMC. 4 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).

When the estimated likelihood of gross failure needs to be very low or the safety case claims gross failures can be discounted, the RP or licensee may invoke a highest reliability claim for the SSC. In this situation usually the consequences of gross failure are unacceptable, and it is not reasonably practicable to provide an engineered means of preventing or protecting against the consequences of the postulated gross failure. The safety case rests on the structural integrity case and the inference of a low initiating event frequency. 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 (SAP EMC.1 to SAP EMC.3, ONR SAPs 2014), with the expectation of measures beyond normal practice i.e. above compliance with recognised nuclear codes and standards. These additional measures are informed by precents in the UK including 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). The designation of a highest reliability components should therefore be by exception and assessed on a case-by-case basis.

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. The concept of a highest reliability claim is well-established in the UK and is akin to the IAEA concept of practical elimination (IAEA 2016).

ONR recognises that the application of concepts such "break preclusion" or "no break zone" may include some additional provisions above normal practice to support higher levels of integrity demonstration. However, to meet ONR expectation for highest reliability these additional provisions may need to be supplemented with further measures based on sound engineering provision with measures over and above normal practice defined in nuclear codes and standards, Alexiou et al. (2019).

Away from these exceptional cases where a highest reliability claim is needed, ONR expects a robust consequence case to be provided as the potential for gross failure is not being 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. Importantly, compliance with recognised codes and standards may form the primary means of establishing the structural integrity provisions. This notwithstanding, and in accordance with UK law, 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. with additional manufacturing controls, inspection and surveillance activities or additional measures to either improve access for inspection or design for "inspectability".

Selection of Codes and Standards

ONR expects that the safety case identifies the role and importance (safety functions) of SSCs 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). Therefore, SSCs important to safety should be designed, manufactured, constructed to the appropriate standards. The GDA process has considered multiple codes and standards from around the world supporting the various reactor designs, but it is the RP's responsibility for the selection of appropriate codes and standards.

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 (as described above) affords the flexibility to assess a wide range of reactor designs, but the output is dependent on the assumptions used e.g. leak before break (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. For GDA, RPs 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 for GDA the RP must propose codes and standards for the design, construction and inspection of SSCs 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)).

During GDA, ONR further developed its collaborating working between structural integrity, fault studies and internal hazards, in two key areas. Firstly, it was recognised that a key element of the assessment of the RP's highest reliability claims was to gain evidence that the RP's designation of a highest reliability claim is justified, and secondly it is important to establish that the RP has demonstrated adequate protection from faults/ internal hazards, that if realised, could undermine the highest reliability claim. These areas are discussed further under multi-discipline considerations below.

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.

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 2021).

ONR's assessment of a design against PPF of high energy systems and components ($\geq$ 2 MPa or $\geq$ 100^{o}C (IAEA 2021)) and in particular the characterisation of the indirect effects of high energy pipe failure 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) have been described previously, Alexiou et al. (2019).

ONR's internal hazards assessment of highest reliability components is focused on two areas: 1) the assessment of the indirect consequences of SSCs to aid their classification as highest reliability components or otherwise and 2) the impact of internal hazards consequences on those SSCs classified as highest reliability component.

This paper focuses on the assessment of ONR's expectations on evaluating the impact of internal hazards on highest reliability components presented as a set of expectations based on experiences gained through various GDA assessments. In general, it is ONR's expectation that internal hazard sources are identified, SSCs are identified, hazard consequence analysis is undertaken and safety measures are identified and substantiated. The main goal from an internal hazards safety case perspective is to avoid highest reliability claims, where possible. However, if these are invoked by the RP, then it is important to gain sufficient evidence that the integrity of highest reliability components can be maintained given an internal hazard event (i.e. avoidance of unacceptable consequences). The following expectations should be considered.

Optimisation of Layout

Where the RP's safety case analysis and evaluation has identified a highest reliability SSC, it is ONR's expectation that the design of the plant's layout should be optimised to eliminate hazards that can impact on the highest reliability components as far as is reasonably practicable. Where elimination cannot be achieved, suitable measures should be put in place to protect the highest reliability component. Priority should be given to passive measures, or if not practicable, engineered measures that do not rely on active systems/ intervention over other measures that require manual initiation or administrative measures. That hierarchy should however not be interpreted to mean that the provision of an item towards the top of the hierarchy (more passive) precludes provision of other items where they can contribute to defence in depth. In instances, where full protection from internal hazard effects cannot be achieved, the integrity of the highest reliability component should be demonstrated, noting that functionality of the highest reliability component maybe lost. The main consideration in this approach is avoidance of unacceptable consequences.

Hazard Identification

It is ONR's expectation that a safety case demonstrates that the risk to nuclear safety associated with internal hazards during normal operation and under potential faults and relevant accident conditions have been reduced ALARP. To achieve this, it is expected that a systematic identification of internal hazards (SAP EHA. 1, EHA.19 and EHA.3, ONR SAPs 2014) and their combinations is undertaken that may have hazardous consequences particularly for highest reliability components.

It is also ONR's expectation that the safety case should demonstrate that in this instance the necessary level of integrity has been achieved for the most demanding safety case situations (SAP EMC. 3, ONR SAPS 2014). Therefore, from the internal hazards perspective, the worst-case hazard load scenario should be considered within the safety case.

Segregation

Where hazard loads cannot be eliminated through design, suitable measures should be put in place to demonstrate that the effects of hazards (individually and in combination) are minimised through adequate segregation delivered either by passive barriers or spatially such that the highest reliability component integrity can be substantiated.

ONR expects nuclear plants to show hazard resilience by means of layout optimisation and segregation of redundant and diverse safety systems by passive barriers (SAPs EDR.2, ESS.18 and ELO.4, ONR SAPs 2014). Approaches based entirely on separation by distance or heavily reliant on SSC 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 safety functions, 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.

Such challenges have been addressed in previous GDAs with adopted measures including plant modification such as reorientation of valves and pipework, restraints and the introduction of bespoke passive barriers to minimise or eliminate the consequences.

Hazard Analysis

There are two key aspects to internal hazards analysis when dealing with highest reliability components.

The first aspect relates to the determination of the indirect consequences to inform the component classification. It is ONR's expectation that the analysis to determine the consequences in this context follows a conservative approach to determine the load tolerance of the components.

The second aspect relates on the impact of internal hazards loads on a component which the RP has classified as a highest reliability. This still requires a conservative approach to determine the internal hazard loads, from other internal hazards sources, to demonstrate that the highest reliability components are not compromised. However, in this instance the objective is to demonstrate the absence of unacceptable consequences. In broad terms this is the demonstration that the component integrity is maintained (e.g. pressure boundary).

It is recognised that many codes and standards applied in the demonstration of highest reliability components may not encompass the consideration of all potential internal hazard loads. This is because the structural integrity claim is inherently founded on the design code provisions for design, manufacturing and inspection. Due to the complexity and variability in internal hazard loads it is not practicable to include them into the various codes and standards. Notwithstanding this, many codes include various additional factors of safety that, if subject to an internal hazard load, the component could have adequate withstand and safety margins. However, the suitability of such approaches needs to be justified by the RP in their safety case.

Safety Measures

ONR's expectation is that the safety case demonstrates that appropriate engineering provisions are implemented to minimize the risk of internal hazards to highest reliability components. These measures should be appropriate substantiated.

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

ONR's expectations and RP's challenges in the design of multi-hazard barriers concrete barrier have been described in Alexiou et al. (2019). This involves, careful multi-disciplinary development of the plant layout, assumptions, and definition of the relevant hazards. In particular, loads from the indirect effects of pressure part failure 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. The design analysis may be complex and involve advanced or bespoke methods of modelling and calculation requiring special verification and validation.

Engineering design codes and standards such as ACI 349 specify load combinations, load factors and acceptance criteria for use in the design of concrete barriers (American Concrete Institute 2014). 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.

MULTI-DISCIPLINE CONSIDERATION

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 internal hazards there are many challenges that are common to all structural integrity, internal hazards and civil engineering 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 internal hazard analysis, identifying and implementing safety measures that demonstrate either that the internal hazard has been eliminated or that the risks have been sufficiently reduced. An ALARP demonstration also requires optioneering studies, which identify further measures that could be implemented and the level of risk reduction that would be achieved.

As described above, the classification of highest relativity components has two aspects. Firstly, the determination of the indirect and direct consequences following a component failure. For this aspect, a multi-discipline team comprising structural integrity, fault studies, internal hazards and civil engineering need to be established to assess the RP's consequence analyses and their consideration of whether it is reasonably practicable to avoid a highest reliability claim. Furthermore, if a highest reliability claim was invoked by the RP, there is an expectation to consider whether any further mitigating measures could be taken to reduce risk. The multi-discipline team effort with input from internal hazards, structural integrity and civil engineering is critical to ensure that the SSC classification is justified. It is important to note that whilst it may be deemed reasonably practicable to provide additional measures to provide protection or limit the consequences for specific consequences, the overall ALARP judgement takes cognisance of the holistic position i.e. the collective measures required to avoid the highest reliability claim.

The second aspect is to demonstrate the highest reliability component is adequately protected from internal hazards which also requires a multi-discipline approach as above to demonstrate the risks are ALARP involving structural integrity, internal hazards and civil engineering disciplines to mention a few.

Compliance with the law requires all design options and measures to be implemented unless their costs in terms of time, trouble, and money are 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 in-direct) analyses inform the structural integrity classification.

ONR's assessment involves benchmarking against RGP with the rigour in the safety case and in ONR's assessment proportionate to the safety function 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. A particular challenge often includes balancing the competing needs of various relevant disciplines demonstrating the integrity of highest reliability SSCs, 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.

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 safety functions 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.

The safety justification presenting the classification of highest reliability component should present a holistic and balanced position of the competing factors. This should be founded on a multi-disciplinary approach to understand the design tolerance to faults and internal hazards.

Experience indicates 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.

Disciplines need to work together to ensure consistency in the development of the safety case and in its subsequent assessment. If the classification of an SSC changes, then all disciplines need to be informed so that the implications can be assessed. For example, an 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's regulation of nuclear safety generally 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.

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

The paper focuses firstly on the assessment of the indirect consequences of SSCs to aid assessment of the RP's justification of their classification as highest reliability components or otherwise and secondly on the impact of internal hazards consequences on those SSCs classified by the RP as highest reliability components.

The paper describes the significant technical challenges to assess an RP's classification of an SSC as a highest reliability component which should be determined on a case-by-case basis. Where the RP's safety case has to make a highest reliability claim it is ONR's expectation that this component is adequately protected from the internal hazards consequences.

The importance of early multi-discipline assessment is highlighted for the assessment of 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

Anastasios Alexiou, Jim Caul, Diego Lisbona, and Leslie Smith (2019). "UK's Regulatory Safety Assessment of Nuclear Plants Pressure Part Failure – A Multi-Discipline View". SMiRT 25, Charlotte, NC, USA.

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

International Atomic Energy Agency (2016). "Safety of Nuclear Power Plants: Design". *IAEA Safety Standards, Specific Safety Requirements SSR-2/1*.

International Atomic Energy Agency (2021). "Protection Against Internal Hazards in the Design of Nuclear Power Plants, Specific Safety Guide". *IAEA Safety Standards Series No. SSG-64*.

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

Office for Nuclear Regulation (2021). "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.

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

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.