UK's REGULATORY CONSIDERATION OF PARTIAL FAILURES IN HIGH ENERGY COMPONENTS – A MULTI-DISCIPLINE VIEW

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

[1] Principal Inspector, Office for Nuclear Regulation, UK (anastasios.alexiou@onr.gov.uk)
[2] Inspector, Office for Nuclear Regulation, UK (leslie.nyogeri@onr.gov.uk)
[3] Retired Principal Inspector, UK

ABSTRACT

Partial failure concepts such as Leak Before Break (LBB) and Diameter (D) x Thickness (t) of Pipe / 4 (Dt/4) have been applied in many countries in the design of reactor plant. These approaches are used to exclude the analysis of dynamic effects following a full-bore pipe rupture (such as pipe whip, jet impingement, flooding, and associated combinations). The absence of such analysis can result in protective measures such as pipe whip restraints and jet impingement shielding not being installed in key locations. This paper presents ONR's multi-discipline (internal hazards and structural integrity) regulatory expectations related to the consideration and application of partial failure concepts (such as LBB) for high energy components. The paper discusses consequences analysis and the challenges presented by the adoption of these concepts in the safety classification of Structures, Systems and Components (SSCs) and when looking to demonstrate that the associated plant risks are As Low As Reasonably Practicable (ALARP).

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 ONR's regulatory approach is that licensees are responsible for the safe build, operation, and decommissioning of their nuclear sites demonstrating that the risks are reduced So Far As Is Reasonably Practicable (SFAIRP) or ALARP.

The UK's regulatory framework is predominantly goal setting. This approach enables licensees to be innovative in their approach to demonstrate the required high level of nuclear safety expected by the UK regulatory regime. This can be mostly achieved through adoption of Relevant Good Practices (RGP), but this does not preclude adoption of other methods, to adequately reduce relevant risks. 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 its Safety Assessment Principles 2014 (SAPs) (ONR SAPs 2020) and associated Technical Assessment Guides (TAGs) (ONR TAGs 2023) – all of which are published and are freely available on the internet. It should be noted that the ONR SAPs are considered holistically for all ONR assessments.

In line with the international consensus, such as the International Atomic Energy Agency (IAEA) Specific Safety Guide on Protection Against Internal Hazards in the Design of Nuclear Power Plants No. SSG-64 (IAEA 2021), and Western European Nuclear Regulators Association (WENRA) Safety Reference Levels for Existing Reactors 2020 (WENRA 2021), the application of defence in depth is a fundamental element of demonstrating nuclear safety risks are ALARP. The application of defence in depth in this

context means that 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. Defence in depth should prevent faults, or if prevention fails should ensure detection limits the potential consequences and stop escalation.

This paper presents ONR's multi-discipline (internal hazards and structural integrity) regulatory expectations relating to the consideration of partial failures in high energy components within a nuclear safety case context.

APPLICATION OF PARTIAL FAILURES IN THE DESIGN OF HIGH ENERGY COMPONENTS IN REGULATORY REGIMES OUTSIDE UK

A partial failure concept, such as LBB argument is aimed at demonstrating with a high degree of confidence that leakage from a through wall crack in a pressurised vessel or pipe can either be detected prior to the crack attaining a critical size (or limiting size) or the crack will not exceed a specific size. In broad terms the crack must be stable and there must be adequate time to detect leakage to provide forewarning against the development of an unstable crack.

In general, partial failure concepts are primarily aimed at the assessment of discrete defects, either postulated or known, for which breakthrough would occur in a ductile manner. In principle, the procedures may be used when the ligament beneath the defect fails in a brittle manner.

The development of a partial failure argument such as LBB is dependent on several assumptions covering the development and stability of the defect (fracture mechanics), the prediction of the leak rate and its detection. In addition, the leak detection claims will be dependent on the location and the capabilities of the leak detection system to demonstrate that adequate forewarning of failure can be justified.

Partial failure assessment and application may not be tenable if the pipe or vessel is prone to active degradation mechanisms that result in a defect or defects (multiple defects rather than isolated defects), which differ from those assumed and in particular those that may lead to very long surface defects e.g. creep, erosion, corrosion or excessive fatigue (NS-TAST-GD-016, ONR TAGs 2023).

The most applied partial failure concept is the LBB approach defined in the United States (US) Nuclear Regulatory Commission (NRC) NUREG-1061 Volume 3 (US NRC NUREG-1061 1984), and US NRC NUREG-0800 Standard Review Plan 3.6.3 (US NRC NUREG-0800 1987). However, it should be noted that there can be differences in the LBB procedures adopted in different countries. The key differences relate to how the surface defect is characterised (location, size and shape), the defect growth assessment, leak rate calculations and the calculation of the critical (limiting) defect size.

ONR's REGULATORY POSITION ON PARTIAL FAILURES IN THE DESIGN OF HIGH ENERGY COMPONENTS

ONR's assessment of high energy component failure involves benchmarking the safety case analysis against RGP. ONR seeks to undertake proportionate assessments through targeting those SSCs for which gross failure presents the greatest nuclear safety risks as defined by their safety function category and safety classification.

ONR expects that the plant layout for the siting of high energy components (for pipes with ≥ 2 MPa or $\geq 100^{o}$C (IAEA 2021)) is optimised such that it eliminates or minimises the impact of internal hazards from a high energy component, or to a high energy component, that could result in the loss of SSCs delivering nuclear safety functions.

To understand the UK regulatory position on the assessment of high energy components and the role of partial failures in consequences analysis in safety cases, the UK expectations for demonstration of defence in depth and pressure boundary integrity need to be considered. These subsequently inform the safety classification of SSCs and the expectations for the structural integrity safety case.

There are some key requirements and challenges associated with substantiating partial failure behaviour and its potential role in a safety case development and these are discussed in the following sections.

ALARP Demonstration

Demonstration that the risks are ALARP requires the duty holder to carry out hazard and risk analysis, to identify and implement measures that demonstrate either that the hazard has been eliminated or that the risks have been sufficiently reduced. ALARP demonstration is underpinned by optioneering studies, which are intended to identify candidate measures that could be implemented as well as the assessment of risk reduction that would be achieved if the measures are implemented. Compliance with the law requires that all such design options and measures should be implemented unless their costs in terms of time, trouble, and money are demonstrably grossly disproportionate in relation to the risk averted.

The demonstration that the nuclear safety risk for a given design is ALARP has proven to be a challenging concept to Requesting Parties in the UK Generic Design Assessment (GDA) process who are more familiar with prescriptive regulatory regimes applying partial failure concepts for high energy pipes. A particular challenge often seen is balancing the competing needs of various relevant disciplines with inherent limitations in the plant layout. For example, optimising plant layout to eliminate a hazard such as pipe whip may not be practical if the system presenting the hazard is needed to perform a specific safety function in that specific location. In this instance, mitigation measures such as barriers would need to be considered to reduce the pipe whip loadings and protect other SSCs. Another typical example is when space limitations within the plant limits the ability to fit mitigation measures such as pipe whip restraints, shielding or reinforced barriers. In these instances, layout modifications and pipe rerouting may need to be considered to demonstrate risks are ALARP. For mature designs, incorporating such modifications can be challenging, but in many instances achievable.

ALARP demonstration for high energy components requires a multi-discipline team effort. This should include input from internal hazards and structural integrity to ensuring the plant layout is optimised for the level of challenge presented by hazards including combined loads of internal hazards, Alexiou et al. (2019).

ONR's regulatory benchmark for new designs needs to reflect current standards informed by relevant good practice and experience. In GDA, the consequences assessment of high integrity components pressure part failure has been based on gross failure. This included the AP1000® design (ONR Internal Hazards Close-out of GDA Issue Assessment Report 2017), UK ABWR design (ONR Step 4 Assessment Reports 2017) and the UK HPR100 design (ONR Step 4 Assessment Reports 2022).

Safety Classification

ONR expects that the safety case identifies the role and importance (safety functions) of SSCs in maintaining nuclear safety, which leads to its classification and demonstration of the measures that will be taken to assure its structural integrity through-life (SAPs ECS.1 to ECS.3, ONR SAPs 2020). Further guidance on SSCs classification and categorisation can be found in ONR guidance NS-TAST-GD- 094 (ONR TAGs 2023).

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.

ONR's expectation is that the categorisation of safety functions and classification of SSCs is based on considering the worst-case (direct and indirect) consequences of postulated gross failure. The use of partial failure concepts such as LBB to effectively discount gross failure or reduce the safety classification of SSCs is inconsistent with the achievement of these expectations and is not in line with UK expectations. This is because the use of partial failure doesn't account for gross failure induced by catastrophic failure and therefore the approach doesn't incorporate the potential worst-case consequences. The associated worst-case consequences may result in an unacceptable loss of safety functions (e.g. due to flooding, pipe whip, missiles or combinations of them) or undermine the structural integrity of highest reliability SSCs (SAPs EMC.1 to EMC.3, ONR SAPs 2020). Similarly, ONR considers that the Dt/4 approach may not represent the failure mode of failure and that the subsequent consequences may not represent the worst-case unmitigated scenario such as internal flooding, pipe whip and combined consequences which in turn feeds into the classification of the SSCs.

Classification of SSCs is usually a multi-disciple approach and includes structural integrity (metallic SSCs), fault studies (direct consequences) and internal hazards/ civil engineering (indirect consequences).

Structural Integrity Considerations

The structural integrity discipline primarily considers metallic SSCs and typically 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 result in significant nuclear safety consequences. 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.34 (ONR SAPs 2020). The SAPs are underpinned by a suite of supporting TAGs which for structural integrity is NS-TAST-GD- 016 (ONR TAGs 2023).

ONR expects the principal means of identifying the level of structural integrity demonstration is by consideration of the consequences of failure, both direct and indirect. 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. 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 choice of relevant codes and standards. Notwithstanding the need to reduce risks to ALARP, compliance with recognised codes and standards may form the primary means of achieving the required structural integrity provisions.

When the consequence of gross failure is unacceptable, and it has been demonstrated by the duty holder 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 will have to rest on the structural integrity case that claims highest reliability and the inference of a low initiating event frequency. Whenever reasonably practicable, highest reliability claims should be avoided. This is because a case to discount gross failure is an onerous route to a safety case (SAPs EMC.1 to EMC.3, ONR SAPs 2020), with the expectation of measures beyond normal practice i.e. above compliance with recognised nuclear codes and standards. The designation of a component failure beyond design basis analysis should

therefore be by exception and assessed on a case-by-case basis NS-TAST-GD- 016 (ONR TAGs 2023) and Alexiou et al. (2022).

When highest reliability claims are made, the case for the components should be based on a robust demonstration of conceptual defence in depth and if highest reliability (practical elimination) is invoked then additional measures above design code compliance are expected. ONR expects an avoidance of fracture demonstration which is informed by precedent following 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). More recently, this precedent has been used to support nuclear safety cases for multiple gigawatt-scale nuclear plant designs that have completed the UK's GDA process, ahead of nuclear site licensing. Through this process, the GDA Requesting Parties submitted sufficient evidence to demonstrate avoidance of fracture for the most challenging (bounding) weld locations or structural features of an SSC on nuclear plant. This has provided confidence that risks associated with gross failure of the most safety significant metallic components of these plants, sampled within the GDA, are reduced ALARP.

ONR expects that primary arguments in a structural integrity case should be founded on sound engineering provision alongside conservative consequence analysis, with LBB mainly used as a defence in depth argument rather than as a primary 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'. These expectations may result in differences with international practices, where LBB or other partial failure type claims (e.g. Dt/4) are invoked.

Furthermore, to apply a partial failure argument ONR expects the degradation mechanisms of the components should be evaluated in the safety case. However, the variability of such degradation mechanisms, especially if initiated by a hazard load, will be challenging to substantiate. For example, the LBB approach is difficult to apply to piping or SSCs that can fail in service from unanticipated loads or active degradation mechanisms e.g. water hammer, creep, erosion, corrosion or excessive fatigue. Such effects would result in defect or loading conditions different from those postulated during the initial LBB assessment and as a result invalidate the LBB argument. In addition, if a component is challenged by a significant hazard loading, such as blast, missile or pipe whip or combination of them, it requires quantification and design substantiation. This has proven challenging especially for combined consequential hazard loads.

Internal Hazards Considerations

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 expectations for the analysis of internal hazards are outlined within the "External and Internal Hazards" SAPs series EHA (ONR SAPs 2020). Detailed guidance regarding ONR's internal hazard expectations can be found within ONR's specific TAG for internal hazards NS-TAST-GD-014 (ONR TAGs 2023).

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 and their combinations is undertaken to determine their consequences and identify appropriate safety measures to eliminate/mitigate them (SAPs EHA.1, EHA.3 and EHA.19, ONR SAPs 2020).

For internal hazards, it is expected that all SSCs are assessed within the design basis. ONR expects that conservative deterministic analysis is undertaken to define the bounding hazard loads, based upon the postulated worst-case failure scenario. ONR also expects that the analysis of the bounding scenario is adequately justified to demonstrate that the bounding hazard loads are truly bounding. The consideration of gross failure should be applied to all relevant SSCs (such as low and medium energy pipework) as these may present bounding loads such as flooding.

Whilst the gross failure (rupture) of pressure vessels and piping built to high standards can be considered a rare event (Health and Safety Executive 2017), such failures do occur and the failure rate though low is non-zero. In addition, a recent internal ONR review of the IAEA Incident Reporting System database of pipe degradation, leaks and breaks (rupture) events for Pressurised Water Reactors (PWR) and Boiling Water Reactors (BWR) primary circuits for the period 2008 - 2022 confirmed that although pipe break events are rare, the consequences of such events were significant. These events were all caused by high cycle fatigue and showed no forewarning of failure.

For high energy components, ONR expects the internal hazard analysis to focus on identifying all potential indirect consequences that can credibly occur. Such consequences include individual hazards (such as pipe whip, jet impact, missiles and pressurisation), combined hazards (such as flooding, pipe whip and pressurisation on a barrier) and consequential hazards (such as failure of other SSCs). As stated above, ONR expects that all associated hazards are identified, loadings derived, and consequences assessed based on a worst-case unmitigated basis. Suitable safety measures should be identified and substantiated. The following should be considered in the development of a robust internal hazard safety case.

The starting point in the analysis of high energy components is to analyse the worst-case unmitigated consequences of the gross failure of that component. This approach is in line with international guidance (IAEA 2021), and informs the tolerability of the plant design against the associated hazard conditions and associated consequences. This in turn then informs the safety classification of the SSCs as well as any other safety measures required to mitigate the effects of the hazard to ensure the delivery of the nuclear safety functions.

ONR recognises that in some instances a components reliability can be adequately substantiated (based on structural integrity claims) such that its failure can be considered as a beyond design basis event. For beyond design basis events, a demonstration that there are no cliff edge effects, after appropriate sensitivity analysis, is required to demonstrate that the plant can still tolerate failure and that the nuclear safety risks are ALARP (SAP EHA.18, ONR SAPs 2020). This is aligned with IAEA (IAEA 2021) and WENRA (WENRA 2021) guidance. A notable exception to this is when a component has an incredibility of failure claim made, in this instance the internal hazards consequences are not considered as part of the safety case demonstration due to the structural integrity claims.

The analysis of gross failure provides contingency for the unexpected and associated uncertainties within the analysis such as the magnitude, sequence and combination of loadings arising from internal hazards and minimises dependencies on complex and costly analysis to substantiate partial failure claims are fully bounding. Application of partial failure concepts such as LBB (or other partial failure arguments) in the absence of consideration of the worst-case consequences is unlikely to result in a design that is robust against a gross failure, as consideration of the worst-case consequences following a gross failure has not been assessed, and thus may result in the unacceptable loss of safety functions, including loss of highest reliability components (SAPs EMC.1 to EMC.3, ONR SAPs 2020). Therefore, the use of partial failure concepts as the primary claim to argue and discount gross failure for a design basis analysis, without sufficient structural integrity substantiation is not consistent with ONR’s expectations.

A key component of a partial failure argument is the detection of failure. When leakage monitoring is claimed in the safety case to provide forewarning of significant failure the analysis should demonstrate that the means, frequency and response is consistent with the degradation mechanism (SAPs EMC.25 and EMC.26, ONR SAPs 2020). ONR expects that the safety case explains the leak detection system and its analysis accounts for the sensitivity, the reliability, the response time and availability of the leak detection system. The safety classification of the leak detection system should be commensurate with the potential consequences and should be substantiated to this level. In addition, there is a need for periodic testing and calibration of leak detection equipment.

CONCLUSION

The assessment of pressurised system failures should be aimed at demonstrating resilience against the most challenging failure modes and consequences. In this context, gross failures often results in the most onerous hazard loads on SSCs and should be considered as part of the safety case and design development. There are differences in the regulatory approach across countries regarding the application of gross failure and partial failure concepts in a nuclear safety case. These differences primarily arise from the underlying assumptions and whether credibility is given to crack stability providing sufficient time to detect leakage and isolate before gross failure.

Whilst ONR recognizes that partial failure type arguments could add value in a safety case, it is ONR's expectation that this is not the primary safety case argument.

The UK expectation is that high energy component failures are assessed taking consideration of worst-case consequences (direct and indirect) to demonstrate the tolerability of the plant to such failures. Where tolerability cannot be demonstrated, it is ONRs expectation that the risks are demonstrated to be ALARP.

A key element to demonstrate ALARP is the application of defence in depth along with applying robust structural integrity claims to underpin its classification and reliability. This approach results in taking a different emphasis on a partial failure argument in the safety cases, with the structural integrity case supported by in-service inspection providing the principal forewarning of failure safety case argument. Other means of plant monitoring (e.g. leak detection) providing a secondary argument. ONR considers partial failure is not a substitute for sound engineering practice to justify SSCs integrity and to demonstrate defence in depth in plant design.

ONR's multi-discipline assessment is key in the assessment of indirect consequences (internal hazard) to aid the classification of high energy components in the structural integrity case and the identification of robust safety measures including substantiation of them.

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.

Anastasios Alexiou, Jim Caul and Leslie Nyogeri (2022). "UK's Regulatory Safety Assessment of Nuclear Plants Highest Reliability Components – A Multi-Discipline View". SMiRT 26, Berlin/Potsdam, Germany.

Health and Safety Executive (2017). "Failure Rate and Event Data for Use within Risk Assessments".

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 (2020). “Safety Assessment Principles for Nuclear Facilities”, 2014 Edition, Revision 1. http://www.onr.org.uk/saps/.

Office for Nuclear Regulation (2023). “Technical Assessment Guides”. http://www.onr.org.uk/operational/tech_asst_guides/index.htm.

Office for Nuclear Regulation (2017). “Assessment Report - Close-out of GDA Issues for the AP1000 Reactor Internal Hazards GI-AP1000-IH-01 to IH-06”, ONR-NR-AR-16-020.

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

Office for Nuclear Regulation (2022). “Step 4 Assessment Reports UK HPR1000”. http://www.onr.org.uk/new-reactors/uk-HPR1000/reports.htm

U.S. Nuclear Regulatory Commission (1984). Piping Review Committee, “Evaluation of Potential for Pipe Break” NUREG-1061 Volume 3.

U.S. Nuclear Regulatory Commission (1987). “Standard Review Plan 3.6.3 Leak-before-Break Evaluation procedures” NUREG-0800.

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.

Western European Nuclear Regulators Association (2021). “Safety Reference Levels for Existing Reactors 2020”.