Office for Nuclear Regulation

New Nuclear Power Plants: Generic Design Assessment Technical Guidance

ONR-GDA-GD-007 Revision 0
May 2019

Any enquiries regarding this publication should be sent to us at onr@onr.gov.uk

This publication is available at www.onr.gov.uk

ABBREVIATIONS

AC	Alternating Current
ACOP	Approved Code of Practice
ALARP	As Low as Reasonably Practicable
BAT	Best Available Techniques
BEIS	The Department for Business, Energy and Industrial Strategy
C&I	Control and Instrumentation
CDF	Core Damage Frequency
CDM 2015	Construction, Design and Management Regulations 2015
DAC	Design Acceptance Confirmation
DBA	Design Basis Analysis
DBT	Design Basis Threat
DC	Direct Current
DRP	Design Reference Point
EA	The Environment Agency
EIMT	Examination, Inspection, Maintenance and Testing
FMEA	Failure Modes and Effect Analysis
FOAK	First of a Kind
GB	Great Britain
GDA	Generic Design Assessment
GDF	Geological Disposal Facility
GSE	Generic Site Envelope
GSR	Generic Security Report
HAW	Higher Activity Radioactive Wastes
HAZOP	Hazard and Operability Study
HBSC	Human Based Safety Claim
HF	Human Factors
HFE	Human Failure Event
HFI	Human Factors Integration
HRA	Human Reliability Analysis
HVAC	Heating, Ventilation and Air Conditioning
IAEA	International Atomic Energy Agency
ICBM	Independent Confidence Building Measure
IEC	International Electrotechnical Commission
LOCA	Loss of Coolant Accident
LRF	Large Release Frequency
MDSL	Master Document Submission List

MSQA	Management System and Quality Assurance
NIA65	Nuclear Installations Act 1965
NLR	Nuclear Liabilities Regulation
NPP	Nuclear Power Plant
NRW	Natural Resources Wales
ONR	Office for Nuclear Regulation
OPEX	Operating Experience
PCSR	Pre-Construction Safety Report
PE	Production Excellence
PL	Professional Lead
PSA	Probabilistic Safety Analysis
PSR	Preliminary Safety Report
RGP	Relevant Good Practice
RI	Regulatory Issue
RO	Regulatory Observation
RP	Requesting Party
RQ	Regulatory Query
SAA	Severe Accident Analysis
SAPs	Safety Assessment Principles
SFIS	Spent Fuel Interim Storage
SNI	Sensitive Nuclear Information
SQEP	Suitably Qualified and Experienced Personnel
SyAPs	Security Assessment Principles
SSCs	Structures, Systems, and Components
TAGs	Technical Assessment Guides
TIGs	Technical Inspection Guides
TOR	The Tolerability of Risk from Nuclear Power Stations
TSC	Technical Support Contractor
WENRA	Western European Nuclear Regulators Association

TABLE OF CONTENTS

Office for Nuclear Regulation

Introduction

1 INTRODUCTION

1.1 THE PURPOSE OF THIS GUIDANCE

1. This document provides technical guidance to support the Office for Nuclear Regulation's (ONR) Generic Design Assessment (GDA) process for the safety, security and safeguards assessment of new Nuclear Power Plants (NPP) proposed for construction and operation in Great Britain (GB). This process will be applied where ONR is asked to assess a proposed design in advance, or in parallel to an application for a nuclear site licence.

2. ONR's inspectors use the Safety Assessment Principles (SAPs) for Nuclear Facilities [1], together with the supporting Technical Assessment Guides (TAGs) [2], to guide regulatory decision making. This will involve the use of the Inspector's professional regulatory judgement, within the framework of ONR's assessment process. This document supports the SAPs and TAGs and contains additional guidance to advise and inform ONR staff in exercising their regulatory judgement when undertaking an assessment as part of a GDA.

3. This document may also be of use to those organisations who undertake a GDA, known as the Requesting Party (RP), in explaining ONR's approach and expectations in a number of Technical Assessment Topics and highlighting lessons learned for each of these during completed GDAs.

4. This document was informed by the learning from the full-scope GDAs undertaken to date and is applicable to ongoing and future GDAs. It will be a "living document" and will be updated in order to take into account changes to relevant good practice (RGP) and lessons learned from future GDAs.

1.2 SCOPE

5. This document is a supplement to ONR's 'Guidance to Requesting Parties' [3], which describes the GDA process, and provides additional technical guidance across a number of topics. ONR has considerable experience in conducting GDAs, and this guidance has been developed to reflect this.

6. The scope of this guidance document is to provide clarity regarding ONR's expectations for:

   - Generic technical matters (As Low As Reasonably Practicable (ALARP), categorisation and classification, the generic site envelope, etc.) which are common to all aspects of ONR's assessment during GDA.
   - The nuclear safety case.
   - Topic areas within nuclear safety.
   - Conventional safety and fire safety.
   - Nuclear security.
   - Nuclear safeguards.

7. The environmental aspects of the generic design are assessed by the environment agencies (the Environment Agency (EA) and Natural Resources Wales (NRW)) with which ONR works closely in GDA. There is separate guidance 621.[4][4] which provides an overview of the processes followed by both regulators and how those processes are integrated. The EA and NRW have also published separate guidance to RPs on its GDA process [5].

1.3 BACKGROUND

8. ONR is the independent regulator of safety and security at nuclear licensed sites in GB. It also regulates radioactive materials transport and ensures that nuclear safeguards obligations for the UK are met. ONR's mission is to provide efficient and effective regulation of the nuclear industry, holding it to account on behalf of the public.

9. In 2018, ONR conducted a lessons learned review of the previous GDAs undertaken. One of the findings that emerged from the review was that there should be guidance providing additional discipline level information regarding the scope, expectations and approach to GDA, along with lessons learned from previous GDAs.

10. ONR is in a position to build upon the experience gained from previous GDAs, and this guidance has been developed to reflect this and provide further advice to prospective RPs over expectations. A number of related matters highlighted by the review have been addressed effectively by making these guidance improvements.

1.4 ONR's REGULATORY APPROACH

11. The GDA process may be applied when ONR is asked to assess the safety case for a new reactor technology in advance of an application for a nuclear site licence being made. It is part of an overall process that ONR undertakes to regulate the design, construction and operation of any nuclear installation in GB for which a nuclear site licence is required under the Nuclear Installations Act 1965 (NIA65). For an overview of ONR's regulatory approach, the nuclear regulatory regime and the processes for licensing nuclear sites, see the document "Licensing Nuclear Installations" [6].

Office for Nuclear Regulation

Generic Technical Guidance

2 GENERIC TECHNICAL GUIDANCE

12. This section presents technical guidance on those generic matters that affect most, if not all, technical assessment topics within GDA. While each of these matters is important to each technical assessment topic, and forms part of their individual assessments, they are of such importance to a GDA that they must be addressed in a consistent and holistic manner by both ONR and the RP. These matters are also where additional guidance has been needed during completed GDAs.

2.1 ALARP

13. The requirement for duty holders to demonstrate that risks have been reduced ALARP is fundamental to UK health and safety legislation, and applies to the design, construction and operation of NPPs. It is therefore an essential objective for RPs' GDA nuclear safety submissions to demonstrate ALARP (although it is not applicable to nuclear security submissions).

14. ONR inspectors during GDA will, as necessary, make judgements on the adequacy and credibility of the claims, arguments and evidence (to demonstrate ALARP) provided for assessment, but it is the RP that puts forward its case, justifies the adequacy of the extant design in a series of submissions to ONR, and initiates further design changes as necessary to comply with requirements (for example, modern codes and standards, RGP and ONR's regulatory expectations).

15. ONR's judgment will be based on extant ONR guidance including:

- ONR's SAPs.
- ONR's TAG on ALARP (NS-TAST-GD-005).
- Risk informed regulatory decision making. (http://www.onr.org.uk/documents/2017/risk-informed-regulatory-decision-making.pdf)

16. These documents provide links to additional references that the RP may find useful. An overseas RP unfamiliar with the concept and application of the ALARP principle may also want to consider contracting GB-based capability to inform its approach.

17. Demonstration of ALARP in GDA will require the RP to evaluate the risks and to consider whether it would be reasonably practicable to implement further safety measures beyond their extant design or initial proposals for design improvement. In many areas of the safety case, this will not be done through an explicit comparison of costs and benefits but rather by applying established RGP and standards. The developers of RGP and standards should have included ALARP considerations (in the case of international guidance, perhaps not explicitly) so in many cases meeting them is sufficient. In other cases, either where standards and RGP are less evident or not fully applicable, the onus is on the RP to implement measures to the point where the costs of any additional measures (in terms of money, time or trouble – the sacrifice) would be grossly disproportionate to the further risk reduction that would be achieved (the safety benefit).

18. The demonstration of ALARP is not a one-off task or a discrete piece of work for GDA. It needs to be undertaken in every topic area, applied throughout the reactor design and embedded throughout the supplied safety case. As a result, it should be an early discussion item between ONR and the RP and its development should be kept under review throughout GDA.

19. While the principles of ALARP are consistent, how the RP demonstrates that RGP has been followed and that that further risk reductions may be grossly disproportionate to achieve can vary from topic area to topic area:

- In many engineering disciplines, identifying appropriate design codes and standards represent RGP, and then showing that they have been followed in the design will be very important.
- Similarly in analysis disciplines, it will be necessary to clearly identify methods and techniques that represent RGP for that topic area, and show that they have been followed.
- The RP needs to have clearly established principles and criteria for both engineering and analysis areas that allow for identified RGP to be followed, and to judge that appropriate outcomes have been achieved.
- The RP needs to have clearly established procedures for new and ongoing design work which include a requirement to consider of a number of options to identify which is the reasonably practicable option (or collection of options) that give the best safety benefit, and make this consideration transparent.

20. Key and fundamental design choices should have been made by the RP before entering GDA, not necessarily taking explicit cognisance of the ALARP principle. There may also be many examples where aspects of the design are an evolution from NPPs which have been in operation for many years. The RP is not expected to repeat all of its design work and analysis during GDA following a new, ALARP informed methodology. However, it should be prepared to provide a narrative and justification for how significant design choices were made, what factors were taken into consideration, and how the final position is consistent with the ALARP principle.

21. If by following its processes for demonstrating ALARP, it identifies that it is reasonably practicable to do more, the RP should initiate the necessary analysis and / or design changes. It should not wait to be directed or instructed to make a change by ONR.

22. The RP should expect ONR to examine the adequacy of its arrangements for considering ALARP, challenge and advise on the sources of RGP followed, review in detail submissions in every topic area which demonstrate how the ALARP principle has been applied, and to comment and challenge on the validity of the final conclusion that it would be grossly disproportionate to do more.

23. ONR recognises, and the RP should be aware, that there is risk that blind adherence to standards or RGP in one area can have detrimental or unanticipated consequences in another area. A balanced outcome is required that takes into account, for example, the impact on both operational and fault conditions, risks to both workers and the public, long and short term considerations, the consequences of introducing additional complexity, etc. It should also look across all affected technical areas and seek advice as appropriate to ensure the right outcome is achieved that takes all relevant factors into account.

2.2 NUMERICAL TARGETS

24. The regulatory regime enforced by ONR is, in general, non-prescriptive and there are therefore few numerical legal requirements. The legal limits that do exist for nuclear safety are radiological. Unlike other regulators, ONR does not have specific limits or design requirements for an individual technology or reactor design. However, there does need to be a transparent framework against which ONR inspectors can make decisions on the adequacy of designs and the associated safety cases provided for them.

25. ONR's SAPs set out nine groups of numerical targets for use by ONR inspectors when considering whether radiological hazards are being adequately controlled and risks reduced to ALARP. These targets quantify ONR's risk policy and have been set to assist in making proportionate regulatory decisions and targeting resources to where the risks and hazards are greatest. More specifically, the targets are guides to inspectors to indicate where additional safety measures may need to be considered and to help judge whether risks are tolerable.

26. The origins and bases for these targets are explained in Annex 2 of the SAPs. Each of the nine numerical targets is expressed in terms of BSLs (Basic Safety Levels representing the upper tolerable risk level) and BSOs (Basic Safety Objectives representing the broadly acceptable risk level). It is ONR's policy that a new facility or activity should be demonstrated to at least meet the BSL while the BSOs form benchmarks that reflect modern safety standards and expectations.

27. The targets are all radiological but take different forms:

- Targets 1-3 are dose limits which apply in normal operation, applied to any person on the site, any group on the site, and any person off the site respectively.
- Target 4 provides dose targets for the effective dose received by any person from a design basis fault sequence. The targets are stepped or banded, based on the frequency of the fault considered.
- Targets 5 to 8 are risk targets. Targets 5 and 7 are set in terms of the overall (summated) risk impact to individuals from all the facilities on a site. Targets 6 and 8 are frequency based limits for doses to people on and off site respectively, banded by effective dose.
- Target 9 applies to societal risk, considering the total risk of 100 or more fatalities from an accident. It is therefore only relevant for severe accidents.

28. Apart from two limits associated with normal operation, the BSO/BSL framework does not in itself provide inspectors with a numerical algorithm or test for determining whether a GDA design is acceptable or not. However, it does help ONR inspectors to identify where additional or further regulatory attention may be required, and it provides appropriate context for any gaps or shortfalls against RGP.

29. It is important that the RP appreciates that numerical targets in the SAPs are meant to guide ONR's decision making. The RP may already have very similar targets or limits that it has applied to its design and considered in its safety case developed for other regulatory regimes. It would be a sensible course of action for the RP to benchmark its design and operational procedures against ONR's numerical targets to understand any gaps or differences in coverage or methodology, to facilitate meaningful interactions with the regulator.

30. It is also important that the RP recognises that simple compliance with numerical limits, whether those of ONR or the RP, is not in itself considered to be an adequate justification for not looking for further improvements. ALARP considerations may be such that the RP is justified in stopping before reaching the BSO but if it is reasonably practicable to provide a higher standard of safety then the RP should do so.

2.3 CATEGORISATION AND CLASSIFICATION

31. ONR has some high level expectations as set out in the SAPs and TAG NS-TAST-GD-094. These expectations are consistent with those set out in IAEA Safety Guide "Safety Classification of Structures, Systems and Components in Nuclear Power Plants, SSG-30" [7] and associated supporting guidance "Application of the Safety Classification of Structures, Systems and Components in Nuclear Power Plants, IAEA-

TECDOC-17878" [8]. However, there is no one set way to meet these expectations. The approach put forward may differ based on the RP's reactor design, safety case objectives and structure, design codes and standards followed, operating and maintenance procedures etc. as well as individual preference, experience and the extant approach followed on entry to GDA. The terminology to use is similarly not mandated but it should be self-consistent and it makes sense not to introduce unnecessary confusion or ambiguity against the terminology used in ONR or IAEA guidance.

32. Inspectors are advised to review the approach that is proposed to be adopted for safety function categorisation and classification of Structures, Systems and Components (SSCs) (and the impact this has on the design codes and standards applied) at a very early stage in GDA, and consider its consistency against ONR's expectations. The details of any approach could, of course, evolve and be improved upon over the course of GDA but the basic principles being applied need to be established at the start. All previous GDA RPs have needed to change or modify their original approaches. These changes have been most significant for RPs starting from a US-style two-tier approach to SSC classification.

33. The appropriate categorisation of safety functions and classification of SSCs is vital for the GDA safety case and is of interest to most technical areas as it links the fault analysis with engineering requirements.

34. Any approach needs to apply to all nuclear safety functions (notably reactivity control, cooling and confinement / containment) and SSCs that are within the scope of the GDA safety case. Therefore, it needs to be applicable and appropriate to the overall NPP, i.e. not just the reactor / nuclear steam supply system but also the fuel route, radioactive waste treatment and balance of plant systems.

35. In ONR's experience from previous GDAs, the development and application of categorisation and classification scheme to design basis reactor faults is an area where there can be a gap against regulatory expectations. Previous RPs have been able to modify their extant approach and associated design without too many difficulties. What has often required additional attention in GDA is a demonstration from the RP that their scheme can deliver appropriate and proportionate engineering requirements for initiating events, faults and potential severe accidents that may arise on the wider site that are not directly associated with the reactor.

36. Notable examples of where the application of categorisation and classification has required additional scrutiny during previous GDAs include:

- Very high integrity structural components.
- Cranes and fuel handling equipment.
- Protection against faults without offsite consequences but with significant on-site consequence to workers.
- Radioactive waste facilities.
- Plant control systems.

37. Ensuring that the categorisation and classification scheme can be applied to events and safety measures outside of the design basis (e.g. design extension conditions and severe accidents) has also required additional attention in previous GDAs.

2.4 FAULT SCHEDULE

38. ONR considers a comprehensive fault schedule to be a vital part of any safety case, and is often the place of entry for a safety case professional or operator into the detailed analysis or safety case discussion. For GDA, a complete fault schedule is a

very useful vehicle for the RP to demonstrate to ONR the completeness and coherence of the safety case and the robustness of the design. However, fault schedules are not widely used or understood by overseas reactor vendors. As a result, it should be an early discussion item between ONR and the RP and its development should be kept under review throughout GDA so that a useful and complete fault schedule will result.

39. ONR does not prescribe the format of a fault schedule. It is for each RP to come up with a format that works for its technology, safety case and individual preferences. At its most basic, a fault schedule is a tabular summary of the faults considered in the (design basis) safety case. ONR's expectation is that fault schedules submitted by RPs during GDA need to provide clear and concise description of those points listed below. It should identify:

- Design basis initiating events considered in the safety case.
- Initiating event frequencies.
- Unmitigated and unprotected consequences.
- Safety functions to be delivered including reactivity control, cooling and containment.
- Safety measures to deliver the safety functions (SSCs plus any human actions).

40. The best fault schedules provide more information than this, often utilising bold/italicised/coloured fonts, or alpha-numeric coding to provide extra added value. The main constraint to what information can be included is what can be fitted into a landscape table with it remaining legible and helpful.

41. Additional items which have been included in fault schedules include:

- Links to Failure Modes and Effect Analysis (FMEA) or Hazard and Operability Study (HAZOP) analysis detailing the identification of faults.
- Beyond design basis/DEC-A initiating events.
- Clarity of all faults bounded by the limiting event entries included on the fault schedule.
- The operating mode, plant configuration or plant state assumed for the initiating event.
- Links to references for initiating event frequency information.
- Safety functions and associated safety measures broken down to sub-function level (e.g. short term and long term cooling, systems to get to a controlled state and then to a safe shutdown state).
- The category of the safety function to be delivered, and the classification of the SSCs delivering the safety function.
- Minimum number of trains or divisions required to deliver the safety function.
- Number of trains or divisions available in a specific operating mode/plant state to deliver the safety function.
- Whether a safety measure is passive, automatic or manually initiated.
- The key parameters and control and instrumentation (C&I) platform, including systems and/or equipment, that initiates operation of a safety measure.
- Defence-in-depth model that fully describes safety measures at a plant in addition to "front-line" design basis measures.
- Essential support systems (e.g. containment functions, power, cooling water requirements etc.) required by the front-line safety measures.
- Links or references to where to supporting narrative and transient analysis can be found in the main safety case submission.
- Links or references to where to find additional engineering details and substantiation in the main safety case submission.

42. There can be value in having more than one fault schedule, and to have supplementary information in supporting tables:

- It may be appropriate to identify essential support systems claimed by front-line safety systems in a supplementary table. This can be an effective means of demonstrating that diversity extends to the heat sinks, C&I platforms (including systems and/or equipment) and power supplies used by the different safety measures.
- Fuel route faults or radioactive waste facility events will almost certainly require different safety functions to be delivered to the reactor, and reactor operating modes may not be relevant. A differently formatted table may therefore be merited.
- Fault schedules can be used in combination with engineering schedules (a system by system view of requirements including design codes, maintenance and inspection regime etc.)
- Fault schedules can be used in combination with hazard schedules (a compartment by compartment view of the threats and provided protection for hazards).

43. The Inspector should engage early, and have on-going dialogue (primarily through ONR's fault studies specialists) on the fault schedule throughout GDA. However, it should be fully integrated within the wider safety case, framing and providing context to interactions across many engineering and analysis disciplines.

2.5 GENERIC SITE ENVELOPE (GSE)

44. Although many details of a NPP design will be independent of the location chosen for its construction, some assumptions about the characteristics of the plant's environment need to be considered in developing the design of certain safety-related features. To ensure that a design submitted for GDA will be suitable for construction on a variety of sites within GB, the RP should specify the 'site envelope' within which the plant is designed to operate safely. The definition of the site envelope can be as broad or narrow as the RP wishes. However, it should be unambiguous and specify any site-related characteristics which have been explicitly included within or excluded from that definition.

45. If a subsequent site licence application is made for a site which has characteristics bounded by the GSE then the time taken for ONR's licensing assessment is likely to be minimised. If the intended site has characteristics which lie outside the GSE, the site licence applicant should demonstrate that the proposed plant is acceptable at the intended site during licensing assessment; this may involve additional safety analysis and / or plant redesign.

46. ONR's expectations for a GSE are as follows:

- Heat sink.

The type and capacity of potential heat sinks should be specified.

- Grid connections.

Assumptions about the type and reliability of grid connections should be identified. The need to satisfy the requirements of the Grid Code for connection to the UK National Electricity Transmission System should also be taken into account.

- Density and distribution of local population.

When considering the GSE, account should, as necessary, be taken of factors that might affect the protection of workers, individual members of the public and population groups from radiological risk. Key factors include assumptions about the local population distribution and density, and the provision for effective emergency preparedness and accident management.

Assumptions regarding the density and distribution of the local population should also take account of UK government policy on determining the strategic suitability of potential nuclear sites in GB. The current government policy is given in the National Policy Statement for Nuclear Power Generation [9].

- External hazards.

External hazards that could affect the safety of the plant should be identified and treated as events that can give rise to possible initiating faults. The RP should demonstrate that an effective process has been applied to identify typical external hazards and potential environmental changes such as climate change (e.g. a change in sea level) which may affect sites in GB. Foreseeable variations in these factors during the expected lifetime of the site should be identified and taken into account.

The sensitivity of the design to the magnitude of external hazards should be well understood. This will be particularly important at the site-specific application stage, where a rigorous comparison of the GSE against the characteristics of the proposed site will be undertaken.

Further guidance is available in section 3.7 External Hazards and in the ONR's SAPs.

- Dose assessment considerations.

The RP will need to make assumptions about the distance of the reactor (and other buildings with radiological inventories) from the site boundary fence, and expected weather conditions to allow off-site dose calculations to be undertaken. These should bound, or at least be broadly consistent with, what could reasonably be expected for GB NPP site.

In addition, the EA will also require the RP to submit a description and characteristics of the generic site (or sites) to allow dose assessment to be undertaken. This will be described in the EA's own GDA guidance.

2.6 SAFETY CASE

2.6.1 INTRODUCTION AND BACKGROUND

47. A GDA RP is required to provide ONR with a safety case for the NPP design under scrutiny to enable ONR's assessment and, ultimately, if appropriate, ONR's granting of a Design Acceptance Confirmation (DAC). Further, the GDA RP must develop the safety case with a potential licensee's legal duties in mind, not solely as a means to satisfy ONR. By the end of GDA, ONR will expect the generic safety case to be fit for use by a future licensee as the starting point for their site-specific phases of a new NPP project.

48. During previous GDAs there have been difficulties in the RP establishing the robust processes and controls necessary to develop and deliver a generic safety case for assessment during GDA and that can be transferable to a future licensee. This led to ONR's increased oversight of the RP's safety case production, control, development and use, including raising Regulatory Observations (e.g. Refs SC.1-3) in this area.

49. This chapter of the report provides guidance on regulatory oversight of safety case in the context of GDA. The guidance reflects lessons learned by ONR during its past and ongoing GDA work related to the RP's safety case production.

50. It is important to stress that this guidance is consistent with, but does not duplicate, ONR's relevant SAPs SC.1 to SC.8 on "the regulatory assessment of safety cases", and TAG NS-TAST-GD-051 on "The Purpose, Scope and Content of Nuclear Safety Cases".

2.6.2 THE SAFETY CASE IN THE CONTEXT OF GDA

51. The safety case encompasses the totality of the documentation developed by a duty holder (in GDA this is the GDA RP) to demonstrate high standards of nuclear safety and radioactive waste management. Put simply, the safety case is the justification that enables the RP to assure itself, ONR, the public and any future licensee who chooses to build such a NPP design, that the proposed generic design would be safe to operate. ONR expects the safety case to clearly demonstrate: how the design achieves defence in depth, how accidental sequences leading to large or early radioactive releases have been practically eliminated, and how the risks have been reduced to ALARP.

52. In GDA, ONR will assess the safety case for the generic NPP design provided by the RP. ONR expects the RP's safety case to encompass all those aspects of the design and operation of the NPP that could impact the risk to public and workers during any stage of the life of the facility; to obtain a DAC, these should include, but are not limited to, all plant and operations related to the reactor, fuel storage and handling, radioactive waste storage and handling, etc.

53. Key safety matters such as conventional health and safety and conventional fire safety will normally be an integral part of the safety case although they can be provided by the RP via a separate suite of documentation. Also, the RP will provide a security case for the generic design in the form of a Generic Security Report (GSR) and associated references. ONR inspectors should note that, regardless of the architecture of the nuclear safety, conventional safety and security cases chosen by the RP, the guidance and lessons learned discussed here are still relevant.

54. A safety case is a logical and hierarchical set of documents that demonstrate the safety of the facility. Even for a less mature NPP design there may be thousands of documents that together constitute the safety case. ONR will not assess the totality of the safety case documentation, but it will seek evidence that a coherent, consistent and cogent safety case structure exists.

55. The safety case is for the dutyholder, not for the regulators and, therefore, ONR does not prescribe the structure of the safety case. The GDA RP is free to select a safety case structure and architecture that better suits its objectives (including the end point sought for GDA, i.e. a DAC). Generic safety report structures used elsewhere may be acceptable as long as the gaps with respect to ONR's expectations are properly covered.

56. Whatever the safety case structure and architecture selected by the RP, ONR expects the RP to develop a top tier summary document or safety case head document to provide cogency and coherence of the overall safety case. This summary should be meaningful if read in isolation and should provide the main entry point and clear links to the underpinning documentation. ONR inspectors across all disciplines will normally commence their GDA assessment from the safety case head document, and they will expect it to:

- Explain how safety is demonstrated for the specific design and how this is articulated / demonstrated within the safety case head document.
- Identify and describe the nuclear safety principles and criteria used in the design.
- Describe the characteristics of the generic site used in the design.
- Describe the role that each chapter of the document plays in the overall safety case.
- Provide a route map to the underpinning documentation with clarity on the safety case architecture and hierarchy of documentation. The supporting documentation is part of the safety case and should include methodologies as well as analyses and other evidence underpinning the safety demonstration, including any relevant existing / applicable Operational Experience.
- Describe how ALARP is demonstrated and summarise the RP's activity and outcomes of its ALARP evaluations, as applicable to the NPP design overall, and individually for each aspect of the safety case.
- Explain how consistency across all aspects of the safety case is achieved.
- Include a fault schedule covering internal initiating events, internal hazards and external hazards. The fault schedule is a key foundation of the safety case providing the bridge between the requirements from the fault analyses to the engineering which delivers such requirements.
- Explain and demonstrate how the requirements, assumptions and commitments in the safety case are captured to ensure that the safety case will be realised in practice in any future new nuclear build project using that design.
- Include a comprehensive list of references.

57. A Preliminary Safety Report (PSR) style document could deliver the above expectations for a design which is not fully developed / mature, to provide the basis of a fundamental regulatory design review within GDA (Steps 1 & 2). A Pre-construction Safety Report (PCSR) style document could deliver the above expectations for a mature design to provide the basis of a detailed regulatory design review with the aim of obtaining a DAC.

58. As indicated in the GDA Guidance to RPs (Ref. SC.4), ONR accepts that RP's who have already available a substantial amount of safety documentation (e.g. prepared in the form of a submission to another regulator overseas) may choose to develop a safety case head document and safety case architecture making optimum use of the documentation already available (See Figure 1).

59. As well as assessing the adequacy of the safety case for the generic design, ONR inspectors should seek confidence that the RP has developed robust arrangements to ensure that a future licensee would be able to develop a site-specific safety case (headed by a site-specific PCSR) with the information transferred from GDA, including arrangements for the safety case to be met in practice in a future new nuclear build project using that design.

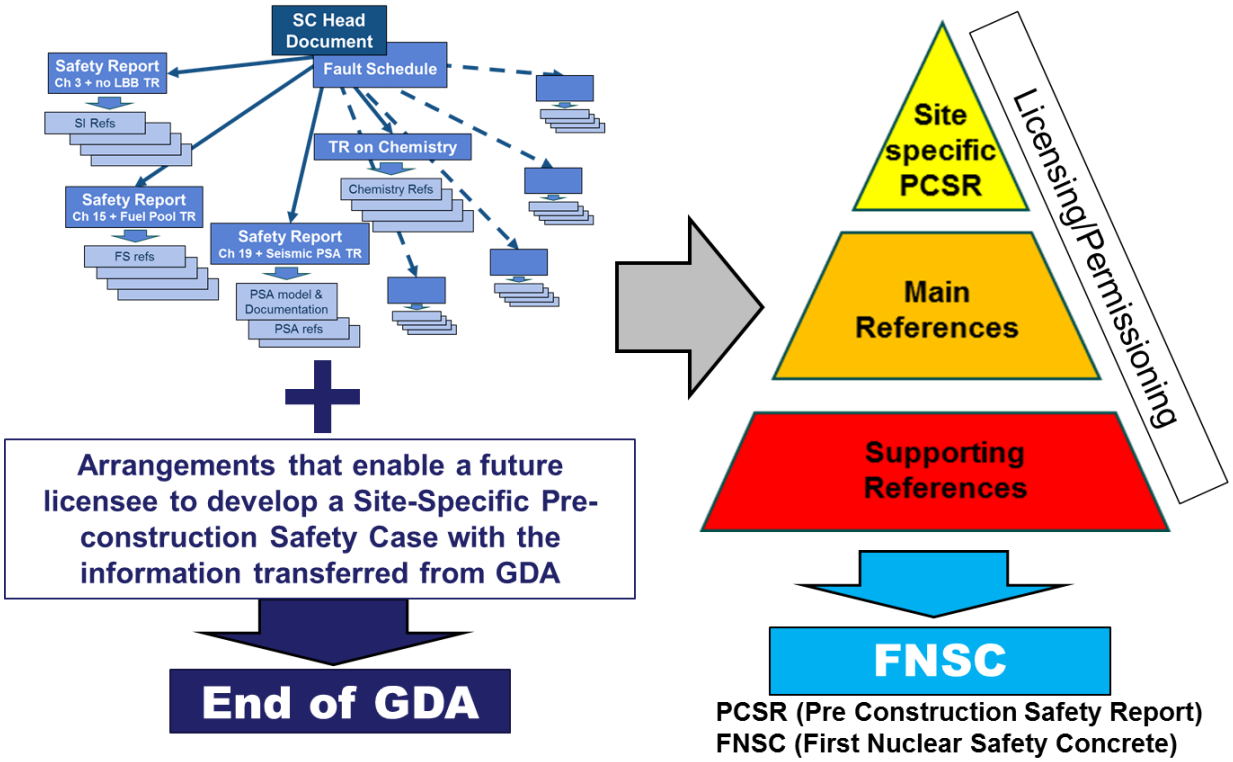

FIGURE 1: Flexibility in Safety Case Approach

2.6.3 REGULATORY OVERSIGHT OF THE SAFETY CASE IN GDA

60. ONR recognises, based on GDA experience to date, that, in addition to delivering assessment in the individual technical disciplines, it also needs to pay special attention to, and focus on, the RP's overall safety case development arrangements. To accomplish this, each ONR GDA team should have an inspector nominated as Safety Case Lead. One of this inspector's key GDA regulatory activities will be to clearly convey to the RP ONR's expectations for the production of an adequate safety case. ONR's GDA Safety Case Lead should work closely with the GDA MSQA inspector(s) and other specialists inspectors, as / when appropriate. Throughout GDA, ONR's Safety Case Lead and their team will make use of interactions with the RP, assessments, inspections and safety case health checks to identify early any potential shortfalls in the RP's safety case arrangements and / or implementation and ensure timely resolution.

61. Early in GDA ONR will seek evidence that the RP has put in place adequate processes and controls to ensure timely development and delivery of the generic safety case. ONR will expect to see a strategy, plan and suitable implementation arrangements. The RP is expected to have organisational arrangements in place to control the development of the safety case, with appropriate oversight being provided by individuals with authority and sufficient expertise to ensure that the safety case strategy and plans are suitably implemented by safety case authors.

RP's SAFETY CASE STRATEGY

62. Early in GDA ONR should seek confidence in the RP's ability to produce a suitable and sufficient safety case. Development of a safety case requires forethought and planning. Therefore, ONR expects the RP to establish, early in Step 1 of GDA, a strategy for the process, which considers matters such as the objectives, scope, interactions, structure and outputs from the work. In essence this is the framework

which defines the development of the safety case. For ONR to be able to judge early in GDA whether a suitable and sufficient safety case will be produced which is likely to meet its expectations, ONR will seek, and may choose to assess and / or inspect the following information and evidence:

- RP's safety case strategy, associated processes, approaches and manuals, which provide information on the objectives, scope and purpose for the overall safety case and how this will be cascaded into individual documents.
- Integration of the overall strategy with any secondary strategies, such as those which may be produced to develop the safety case at a topic, system or process level.
- Technical and safety case interfaces, with clear identification and definition of these and how they are being managed.
- Definition of the architecture / hierarchy of safety case documentation, demonstrating how the different levels and types of safety case documentation and the arguments and evidence contained therein, will be produced and linked together to cover the full scope, interactions and content of the safety case.
- RP's plans to secure: delivery of high quality documentation, and a right-first-time culture in the RP organisation; independent safety case reviews to be carried out on its behalf; and, engagement and collaboration with prospective licensees in matters related to safety case development.

RP's SAFETY CASE DEVELOPMENT PROGRAMME

63. Early in GDA, ONR should seek confidence in the RP's ability to deliver the safety case in a timely manner. The RP should develop the safety case programme early in Step 1 of GDA to ensure that the safety case strategy is enacted in a timely manner, and that the purpose, objectives and scope are clearly understood at the outset of the project. These need to be developed into a set of deliverables and submissions which together, constitute the full scope of the safety case. At the highest level should be the safety case head document (discussed above), below which sit the full suite of supporting documents which constitute the arguments and evidence to support the safety claims. ONR will expect the RP's safety case development programme to cover, and may choose to assess and / or inspect, the following:

- Definition of the main safety case tasks required to be completed during GDA and identification of any interface with future (post GDA) tasks.
- Identification of the various reports (e.g. safety case head document, topic reports, basis of safety case, support studies, etc.) which will be produced with clear presentation of their hierarchy and interfaces.
- Timeline for production of the deliverables, including any review period and their submission date to ONR (if applicable).
- Dependencies between technical areas, topics or documentation.

RP's SAFETY CASE DELIVERY ORGANISATION

64. Early in GDA, ONR will seek confidence in the RP's capability and capacity to deliver the safety case. As part of the safety case planning process, the RP needs to design the safety case delivery organisation and identify the resources required to produce the safety case. This should include consideration of both technical and specific safety case production resource. It is also vital that a "controlling mind" is in place, with authority to direct and determine what type of safety case documentation is required, coordinate the different technical disciplines to ensure that high quality, consistent and integrated safety case arguments and evidence are produced in a timely manner and documented in an adequate safety case. All those responsible for delivering the safety case need to understand the plant design and be conversant with ONR expectations for modern standards safety cases, as well as having the relevant technical expertise

and experience in their topics areas. ONR will seek, and may choose to assess and / or inspect the following information:

- The organisational arrangement, roles and associated responsibilities and authorities related with the production of the generic safety case.
- The decision making processes to be employed, including the "controlling mind" in the production, review and approval processes.
- The arrangements to ensure that suitably qualified and experienced (SQEP) safety case professionals are used to provide advice on and support writing of the safety case.
- Any training undertaken / planned to inform safety case authors or other individuals who have a role in producing the safety case.
- Any independent or peer review activities and processes that may be employed.
- How any third party inputs will be specified, controlled, managed and integrated.
- How involvement of personnel with relevant plant and operating experience (OPEX) will be achieved, including consideration of the full lifecycle including construction, commissioning, operations and decommissioning.

RP's SAFETY CASE OUTPUTS

65. Throughout GDA, ONR should seek confidence that the RP's safety case will be a suitable and sufficient demonstration that the design would be safe throughout the full lifecycle of the plant.

66. Undoubtedly the safety case will evolve throughout GDA, for example, to capture additional work by the RP, design modifications, resolution of regulatory comments, additional documentation developed within GDA, etc. The RP's safety case final output will be a consolidated version of the generic safety case (referred to in the DAC if / when granted). To ensure that the safety case development process is effective and produces a high quality safety case, ONR expects the RP to put in place, early in GDA, a "commitment capture log". This document (database) should provide the means to capture, track implementation in the safety case documentation, and demonstrate closure of, all the commitments made by the RP throughout GDA, in particular those made in responses to Regulatory Queries (RQs), Regulatory Observations (ROs) or Regulatory Issues (RIs). ONR will assess, on a sampling basis, the various formal versions of the safety case (as agreed with ONR), and may choose to assess and / or inspect the RP's system to capture and track commitments.

67. A key output from the safety case is the ability to transfer the assumptions, requirements and commitments made within the safety case documentation into the as built and the operating regime. While building and operating a NPP are responsibilities of the future licensee, ONR requires the GDA RP to put in place an effective process to ensure that assumptions, requirements and commitments made within the safety case documentation are captured and transferred, taking into consideration how this may be achieved in practice, post GDA. Where reasonably practicable, ONR expects the RP should ensure the involvement of future operators in developing this safety case in order to ensure its operational considerations are included and the safety case will be of practical use during the site-specific phase. ONR will seek, and may choose to assess and / or inspect the following information:

- Method (and guidance to safety case authors) for clearly identifying any safety related assumptions, requirements and commitments in the text of the safety case, including how they are:
  - Recognised.
  - Uniquely identified and tracked.

- Collated and catalogued.
- Graded based on safety significance.
- Consolidated into a single consistent set, applied throughout the safety case.
- Updated and managed throughout GDA.

- Any training given / planned to the safety case authors, or others involved in the safety case production process, to ensure they are able to effectively identify and capture assumptions, requirements and commitments made within the safety case documentation.
- How it will be ensured that assumptions, requirements and commitments made within the safety case documentation are transferred to the future licensee to be included in operating rules, manuals, procedures, training requirements, commissioning tests, etc. as appropriate; including identification of, and mapping to, any documentation with may be produced past GDA (such as in construction and commissioning documentation).

2.6.4 ADDITIONAL LESSONS LEARNED

USE OF CLAIMS, ARGUMENTS, EVIDENCE (C/A/E)

68. SAPs 2014 specifically indicate ONR's expectation that the safety case should clearly set out the trail from safety claims (C), through arguments (A), to evidence (E). At a high level, C/A/E can be explained as follow:

- Claims (or assertions) are statements that indicate why the facility is safe. For example: "all design basis faults have been assessed and shown to meet the identified success criteria", "the fuel maintains its integrity as a barrier to fission product release in normal operation and anticipated faults", etc.
- Arguments (or reasoning) explain the approaches to satisfying the claims. For example, the methods used and the assumptions made to support the claims would be considered to be arguments.
- The facts presented to support and form the basis of the arguments or the safety claims constitute the evidence. Examples of evidence are safety analysis calculations and results, code verification and validation reports, operational experience data, experimental results, test findings, etc.

69. The C/A/E concept was developed from C&I research in the 1990s to be applied to complex systems to strengthen links between design and safety and provide give high degree of confidence that what is required from the system has been delivered.

70. Application of C/A/E for the development of safety cases in GDA does have its challenges. Experience shows that a formal C/A/E structure (e.g. with every element being uniquely identified) is not easily or readily applicable to all aspects of the safety case. C/A/E is easier to implement for requirements-based aspects of the safety case ("engineering" and "systems-based" disciplines) than for "science" or "safety analysis" disciplines where an extended narrative may be necessary to articulate the safety case. Therefore, the approach to C/A/E needs to be carefully considered and implemented by the RP so that the resulting safety case flows and makes sense.

71. It is important to note that the C/A/E is not mandatory but may help to structure the safety case and provide traceability in some areas. ONR's GDA inspectors are encouraged to discuss this topic with the RP early in Step 1 to ensure that expectations and good practices for each technical discipline are well understood.

LESSONS LEARNED FROM USING SAFETY CASE DOCUMENTATION DEVELOPED FOR OTHER OVERSEAS REGULATORS

72. It should be recognised that safety documentation written to demonstrate compliance with regulatory requirements elsewhere, in particular in countries with prescriptive regulatory regimes, will make reference to a comprehensive and fixed suite of rules, regulations, expectations, codes and standards relevant to those countries. Thus, unsurprisingly, ONR has identified a number of important shortfalls against its regulatory expectations when assessing, in previous GDAs, regulatory submissions originated overseas. Examples of these are recognised and captured in the guidance for individual technical disciplines later in this report.

73. However, despite those gaps, ONR could make significant use of the information and documentation developed for overseas regulators. Often, the identified shortfalls could be addressed via development of additional topic reports.

74. Both in Ref SC.4. and in this guidance, ONR explicitly indicates that the RP may make formal use of submissions to other regulators as long as the gaps against ONR's expectations are recognised early and addressed in the safety case development strategy, plans and outputs. The development of a safety case head document (as discussed above) should clearly describe how the safety documentation submitted to overseas regulators integrates into the overall GDA safety case architecture, and how the gaps against ONR's expectations are addressed.

2.6.5 LINK TO RELEVANT TAGs

75. For further details the reader should refer to TAG NS-TAST-GD-051 on "The Purpose, Scope and Content of Nuclear Safety Cases". It is worth highlighting Appendix 1 (Common Problems with Safety Cases) and Appendix 2 (NIMROD Review – Safety Case Shortcomings & Traps) of this TAG.

2.6.6 REFERENCES

- SC.1 Hitachi-GE Nuclear Energy Ltd. Safety Case Process and Capability. RO-ABWR-0025. November 2014
- SC.2 Hitachi-GE's Development of Arrangements for the Safety Case to be Met in Practice. RO-ABWR-0057. June 2015
- SC.3 Development of a Suitable and Sufficient Safety Case. RO-UKHPR1000-0004. September 2018
- SC.4 New Nuclear Power Plants: Generic Design Assessment Guidance to Requesting Parties. ONR-GDA-GD-006. ONR. Date TBC

Office for Nuclear Regulation

Technical Assessment Topic Guidance

3 TECHNICAL ASSESSMENT TOPIC GUIDANCE

76. This chapter of the technical guidance for GDA provides guidance to RPs on ONR's expectations relating to individual topic areas. The table below lists the individual disciplines that are normally considered for any design undergoing GDA with the aim of obtaining a DAC.

TYPICAL TECHNICAL ASSESSMENT TOPICS

Topic		
Chemistry	Fuel and Core	Safeguards
Civil Engineering	Human Factors	Security
Control and Instrumentation	Internal Hazards	Severe Accident Analysis
Conventional Fire Safety	Management for Safety and Quality Assurance (MSQA)	Structural Integrity
Conventional Health and Safety	Mechanical Engineering	
Electrical Engineering	Nuclear Liabilities Management	
External Hazards	Probabilistic Safety Analysis	
Fault Studies	Radiological Protection	

77. The sections in this chapter have been written by individual specialists and reflect the experience of these individuals. They also reflect areas where RPs have needed additional guidance. The sections have been written using a consistent template but for these reasons the reader may find that there is a different emphasis across these sections.

3.1 CHEMISTRY

78. Chemistry can affect materials, systems and processes and their associated hazards in a variety of ways. In the broadest sense the topic of chemistry can be considered as being: “the influence of chemistry on reactivity, pressure boundary integrity, fuel and core component integrity, radioactive waste generation and radiological doses to workers and the public”. The objective is for the RP’s safety case to demonstrate that relevant effects are understood, and their impact on safety is minimised to reduce risks to ALARP. In the description that follows, the term ‘chemistry’ should be interpreted to mean chemical or radiochemical parameters or effects.

3.1.1 SCOPE FOR GDA

KEY ASSESSMENT TOPICS

79. ONR considers five main sub-topics within the scope of a typical chemistry assessment during GDA:

- The effects of chemistry on reactivity.
- Protection of the structural materials (especially pressure boundaries).
- Maintaining fuel integrity and performance.
- Minimisation of out-of-core radiation fields.
- Minimisation of releases during accidents.

80. These sub-topics align with the broad description of chemistry given at the beginning of this section, when applied to a NPP.

81. It is likely that most of ONR’s assessment will focus on the influence of chemistry during normal operating conditions (namely at-power operations, commissioning, start-up, shutdown, transients, stand-by and outages), in particular on the safety claims made on controlling the coolant chemistry within defined limits, the adequacy of these and the consequence of operating outside those limits. This includes the ‘chemistry regime’ (the set of conditions, parameters, which define the particular chemistry environment to which the plant will be exposed) and the ‘chemistry programme’ (the totality of provisions which allow the licensee to control and monitor the status of the chemistry regime). This latter aspect will consider the adequacy of the generic plant design and engineering to achieve effective control of chemistry, but will not consider matters which are site or licensee specific, such as detailed operating instructions.

82. ONR also considers the effects of chemistry during fault conditions as part of this topic, as this can influence the rate and ultimate consequences of a particular fault. This includes the generation, transport and behaviour of radionuclides and reactive species and in particular, will focus on the adequacy of any assumptions or treatment in supporting analysis. This will span the full range of fault conditions from Design Basis faults up to and including Severe Accidents.

DOCUMENTS SUBMITTED

83. Given the breadth and depth of these assessment topics it is likely that chemistry considerations will feature in numerous parts of the RP’s safety case. ONR does not prescribe the approach or content for this documentation, although an important focus for this should be a clear and unambiguous justification that the chemistry regime reduces relevant risks to ALARP with an appropriate and proportionate range of supporting evidence. The supporting documentation may therefore include reports, analysis, research findings, OPEX and theoretical analysis, amongst others. In such

instances, ONR would expect that there is a transparent evidentiary trail linking the supporting evidence with the safety claims and requirements.

SAMPLING AREAS

84. The relevant inspector will chose to sample a number of areas of the safety case where the risks are highest, or appear to be least well controlled. The sampling will be done in a focused, targeted and structured manner with a view to revealing any specific or generic weaknesses. For chemistry this will also consider any distinguishing features of the design or proposed chemistry regime, and will look to establish whether the RP's proposals align with RGP.

3.1.2 BASIS FOR DECISION

STANDARDS AND GUIDANCE

85. ONR's SAPs [1] constitute the regulatory principles against which RP's safety case will be judged. SAPs ECH.1 to 4 (chemistry) are directly relevant and would form the core of the assessment. These SAPs explain the main chemistry related aspects that ONR would expect an RP to demonstrate as part of their safety case, with demonstration that a balanced approach to the relevant risks has been adopted, as in ECH.2, which is an important consideration during a GDA.

86. SAPs ECM.1 (commissioning); EAD.1 to 4 (ageing and degradation); EMC.2, EMC. 3, EMC.13, EMC16, EMC.21, EMC.22 and EMC.25 (integrity of metal components and structures); EGR.1, EGR.2 and EGR.7 to EGR.9 (graphite reactor cores); ENM.1 to ENM.7 (control of nuclear matter); ERC.1, ERC.3 and ERC.4 (reactor core); EHT.4 and EHT.5 (heat transport system) are also likely to be of significant relevance to the chemistry assessment.

87. In addition to the SAPs, the following TAGs [2] are of relevance:

- NS-TAST-GD-088 (Chemistry of Operating Civil Nuclear Reactors) and NS-TAST-GD-089 (Chemistry Assessment) are directly relevant.
- A number of other TAGS are likely to be used including, but not limited to: NS-TAST-GD-005 (Guidance on the Demonstration of ALARP); NS-TAST-GD-016 (integrity of Metal Components and Structures); NS-TAST-GD-035 (The Limits and Conditions for Nuclear Safety (Operating Rules)); and NS-TAST-GD-051 (The Purpose, Scope and Content of Nuclear Safety Cases).

88. ONR's expectations outlined in the SAPs and TAGs are generally consistent with international standards and guidance. International standards and guidance are detailed within the TAGs.

89. A number of documents are produced by industry bodies, which contain recommendations for the chemistry regimes which may be employed for a given reactor type. It should be noted that ONR does not consider such recommendations can be directly used as part of the safety justifications, and would expect an RP to demonstrate how their proposed chemistry regime takes account of the RGP included within these documents, and how they have derived a set of conditions under which the proposed design is safe to operate. This is important to ensure that there is a clear separation between safety and commercial matters.

KEY EXPECTATIONS FOR THE SAFETY CASE JUSTIFICATIONS

90. In applying these standards and guidance, ONR would expect to find evidence that the RP has:

- Appropriately considered the influence of chemistry on safety within the safety justifications, and there is clarity over which measures are applied for safety benefits, as opposed to other purposes (for example, commercial benefit), and the consequences of not achieving these.
- Where a balance needs to be achieved between conflicting effects, both within the chemistry regime itself (between parameters) or due to the wider interactions of the chemistry regime (between chemistry and other design choices, such as materials), a holistic approach has been adopted to overall plant safety. This should give due priority to those which are the most relevant, likely to occur and have the potential to lead to the largest consequences or are the least well controlled.
- Provided a clear demonstration that the chemistry regime reduces risks to ALARP. This should also consider the hierarchy of controls and seek to demonstrate that claims made on chemistry to mitigate hazards are minimised.
- Produced a safety case which takes appropriate account of operating experience and relevant industry standards and guidelines (i.e. RGP) in defining the chemistry regime and chemistry programme.
- Provided a suitable demonstration that the design and engineered features will provide an adequate level of control over the required chemistry parameters, including dosing, monitoring and clean-up, and timely operator intervention can be achieved where necessary.
- Considered the different chemistry requirements likely to be necessary during different operating modes, and during different stages of the plant's lifetime.
- Demonstrated that the chemistry related SSCs have been appropriately classified on the basis of their safety function and significance to nuclear safety, including their safety functions related to the control of chemistry.
- Considered the through life performance of the chemistry related SSCs and has taken this into account for defining their examination, maintenance, inspections, testing and decommissioning requirements.
- Clearly defined the safe operating envelope relating to chemistry, including any limits and conditions necessary in the interests of safety and the chemistry programme. These are appropriately graded based upon their safety significance and the timeliness of corrective actions is commensurate to the potential consequences.
- Adequately considered the safety case assumptions regarding the behaviour of chemical species or processes and demonstrated that these are adequately justified and underpinned by supporting evidence, including sensitivity analysis if appropriate. The consideration is proportionate to the importance of the assumption to the safety justification.

3.1.3 INTEGRATION WITH OTHER TECHNICAL ASSESSMENT TOPICS

91. The following are considered the most important interactions that will need to be considered during the chemistry assessment:

- Chemistry provides input to the integrity and corrosion aspects of the assessment. The effects of the chemistry regime (the environment) on the susceptibility to material degradation mechanisms will be led by the chemistry inspector. However, the overall judgement on the adequacy of the safety case for material degradation aspects will also need to be informed by other factors, such as material and stress factors, which will be led by the structural integrity inspector. An important distinction is that the chemistry assessment will also consider those corrosion mechanisms which may have limited impact on component integrity, but could have a strong effect on other hazards, such as radioactivity.

- Chemistry tends to take the lead on the assessment of radioactivity generation, minimisation, transport and accumulation. This includes the radioactive "source term" for normal operations. This is a broad area requiring coordination between several disciplines: radiological protection, radioactive waste management, structural integrity (to a lesser extent) and interactions with the environment agencies' areas of assessment. Chemistry will lead the assessment of the impact of material choices, surface finishes and chemistry regime on radioactivity, including the justification that this has been reduced ALARP. Chemistry will also need to input to the overall assessment of hard wearing materials, with mechanical engineering, where component longevity and maintenance are important concerns.
- Chemistry provides input to the cladding corrosion and fuel crud aspects of the fuel and core assessment. The effects of the operating chemistry on these aspects will be led by chemistry, as would the assessment of any chemistry related consequences (e.g. on radioactivity or deposition), but any non-chemistry related consequences will be led by the fuel and core inspector.
- Chemistry provides input into the fault studies and severe accidents areas, where chemistry effects are important in determining the consequences or effectiveness of mitigation measures and in the analysis of combustible gas and radiological accident source terms. This area will be led by fault studies, with input from chemistry. There will also be an interaction with probabilistic safety analysis (PSA) for severe accidents.
- Chemistry may also interact with other disciplines, such as safeguards and human factors.

92. Chemistry will also be looking at evidence of adequate chemistry control in gaseous and liquid radioactive waste treatment systems, which will require close working with the environment agencies and radioactive waste inspector.

3.1.4 LESSONS LEARNED

93. Based on experience from previous GDAs a number of important lessons have been learned on the approach and shortcomings in the chemistry related aspects of RPs' safety cases. Key themes are presented below:

- Chemistry is a safety related matter and needs to be considered appropriately within the safety case, to a breadth and depth commensurate to the resultant hazards, their likelihood and potential consequences.
- The presentation of the chemistry related aspects of the safety case need careful consideration. Previous experience has shown that chemistry does not readily fit within a rigid claims-arguments-evidence structure. This can also impact on where the chemistry related information features within the safety case. Whatever the approach, ONR expect there to be a clear and concise evidentiary trail.
- The requirement to demonstrate that the chemistry regime reduces risks to ALARP is particular to the GB context. This is important where there are potential choices in the chemistry regime to be employed.
- ONR does not consider following industry chemistry guidelines as a safety justification. The safety case needs to be specific to the design and justify why the chemistry regime is safe, clearly separating safety from commercial considerations.
- The safety case needs to present a balanced approach to evidence, present an objective view, and should justify its relevance when OPEX is used to underpin the safety of the design.

- The safety case needs to present a consistent approach to where there are safety claims made on chemistry, across the different technical assessment topics.
- A rigorous justification will be needed, demonstrating an overall ALARP balance. This is particularly relevant to the interactions between the chemistry regime and the material choices. Materials and chemistry should both be optimised to reduce risks to ALARP, and they should be compatible with each other. Neither materials nor chemistry choices should be selected in isolation to compensate for shortfalls in the other, and the chemistry regime should instead be complementary and reinforcing to other design choices.
- ONR expects the reliance on chemistry as a mitigation to hazards should be minimised, particularly where there are means available to eliminate or greatly reduce the risk, in line with the hierarchy of controls.
- The safety case should clearly define what chemistry controls are necessary to safely operate the reactor, under all conditions it may operate including the definition of related limits and conditions.
- The engineered systems should be demonstrated to be adequate to maintain the chemistry within the limits defined within the safety case.
- The safety case needs to demonstrate chemistry can be controlled, via monitoring and sampling.

3.1.5 REFERENCES

94. Further details for each of these lessons learned can be found in ONR's Step 4 technical assessment reports for the EDF and AREVA UK EPR™, Westinghouse AP1000® and Hitachi-GE UK ABWR (www.onr.org.uk/new-reactors/assessment).

3.2 CIVIL ENGINEERING

95. In general, civil engineering structures provide support to SSCs and protect them against the environment. Nuclear safety significant structures will also confine, shield and mitigate radioactive release.

96. ONR's civil engineering assessment includes the design, construction, operation, maintenance and decommissioning of a wide range of civil engineering structures (from steel framed structures to concrete structures).

3.2.1 SCOPE FOR GDA

97. In civil engineering, the RP identifies the buildings and civil engineering structures that will be in the scope of GDA. The number of SSCs within the scope of GDA will depend on the design and the RP's judgement, but should include key nuclear safety significant buildings and structures. The RP will need to demonstrate that the layout of the buildings has been optimised from a safety perspective and that interactions (including collapse) between the buildings are prevented throughout the design.

98. Key SSCs expected to form part of the scope of GDA are the civil engineering structures enclosing the reactor, the fuel route safety buildings, the control building and structures housing radioactive inventory. The GDA design for each of the buildings will include the design of the superstructure, foundations and where applicable aircraft impact protection.

DOCUMENTS SUBMITTED

99. The RP's documentation justifying the civil structures within the scope of GDA should provide the safety case that identifies the key functional requirements, and the design,

construction and management approaches that support these and should include the following:

- Generic site layout including plans and section drawings. This will allow the inspector to understand the interactions between civil engineering structures.
- The key functional requirements of the structures.
- The design basis for the civil engineering structures, including a description of the structures, generic civil engineering parameters (e.g. geotechnical parameters), materials, loadings, design codes and computer programmes.
- Assumptions made in the design (i.e. loadings, site characteristic, modelling assumptions, etc.), this may include sensitivity analysis to determine the sensitivity of the analytical results to the assumptions made.
- A demonstration that design codes and standards are relevant and applicable to the reactor technology and have been adequately interpreted and applied.
- A demonstration that the analyses methods/computer programmes are adequate to assess the civil engineering structures, and have been adequately validated and the data verified.
- A demonstration that the modelling of the civil engineering structures follows RGP; considers interaction between buildings (load transfer) and represents the building/structure as per the GDA submissions.
- Evidence that the civil engineering design meets the safety functional requirements, is robust and can withstand design basis loads. In some cases, notably the containment design, the most important safety functional requirements could come from severe accident scenarios and beyond design basis challenges. Appropriate justifications need to be provided, including analysis of margins and failures modes to demonstrate the robustness of the design.
- Clarity and consideration of the interactions of the civil engineering design with other disciplines.
- Clarity over the reliability claims of the civil engineering structures achieved through the design and defence in depth.
- Evidence that the design considers ageing management and decommissioning.
- A demonstration that the risks to conventional and nuclear safety are reduced ALARP.

100. The number and the level of detail in the documents submitted by the RP can vary. However, previous RP's have found useful to present the safety case following an approach based on claims, arguments and evidence.

101. Some examples of safety documentation submitted in previous GDAs include:

- Generic safety case – This normally includes the claims on the SSCs.
- Basis of Design – It provides the design requirements of the structures and arguments regarding the robustness of the civil engineering design.
- Design reports, supporting calculations and technical drawings (General Arrangement drawings and a selected sample of detailed drawings) for nuclear safety structures, containments and foundations. These documents will provide the evidence to substantiate the arguments.

KEY ASSESSMENT TOPICS & SAMPLING AREAS

102. ONR is a sampling organisation with limited resources, therefore during GDA sampling is used to limit the areas scrutinised and to improve the overall efficiency of the assessment process.

103. The initial sampling strategy for assessment may consist of undertaking a "broad brush" review of all the documents provided by the RP and then to carry out a "deep

dive" detailed technical assessment of the topics that are important or less clearly explained.

104. The relevant inspector will decide the areas of design that ONR will sample. ONR will seek confidence that the design in line with RGP and the risks to nuclear safety have been reduced to ALARP levels. The following list provides a number of areas that the civil engineering inspector will (normally) assess:

- Safety case claims made on the civil engineering structures.
- Civil engineering design requirements or design basis. This will include: Cat & Class, Seismic category, design codes and standards, loading, loading combinations, material properties, etc.
- Applicability of the design codes and standards used in the design of the civil engineering structures.
- Analysis methods and verification and validation studies. Any "in-house" programmes should be assessed in detail.
- Seismic analysis methodologies.
- Leak detection systems in liquid retaining structures in contact with nuclear material (e.g. fuel pool).
- Aircraft Impact Assessment.
- Multi-disciplinary issues identified in the assessment (e.g. substantiation of barrier for internal hazards loadings, severe accident loads, consideration of decommissioning during the design).
- Application of ALARP principles to the design.
- Civil engineering containment structures, in terms of design basis, beyond design basis, ultimate capacity of the containment and reliability.

105. Other areas that the inspector may assess:

- Assumptions regarding the definition of the generic site such as ground conditions and site envelope properties.
- General site layout and interactions between the civil engineering structures (e.g. Structure Soil Structure Interaction).
- Structural materials are intended to conform to European and British standards, but this cannot be assumed if other design codes are used (e.g. American design codes). In this case, a justification of construction materials or a comparison study will be required.
- Examination, Inspection, Maintenance, and Testing arrangements (EIMT).
- Assess the approach to beyond design basis and its effects in the civil engineering design, e.g. assessment of cliff edge effects in the structures.
- Reliability of the civil engineering structures.
- Design risks as required by Construction, Design and Management Regulations 2015 (CDM 2015).
- Novel construction techniques, such as modularisation or Open Top Parallel Construction.

3.2.2 BASIS FOR DECISION

STANDARDS AND GUIDANCE

106. The standards and criteria normally adopted in any ONR assessment are:

- SAPs - There are 26 civil engineering SAPs that cover design, construction, inspection, maintenance and decommissioning. Other SAPs, such as internal and external hazards, safety case, layout, reliability, containment and maintenance and inspection SAPs will also apply to the civil engineering assessment.

- TAGs:
  - NS-TAST-GD-017 Civil Engineering Revision 3
  - NS-TAST-GD-020 Civil Engineering Containment for Reactor Plants Revision 3
  - NS-TAST-GD-005 Guidance on the demonstration of ALARP Revision 8 NS-TAST-GD-051 The purpose, scope and content of safety cases Revision 4
  - NS-TAST-GD-009 Examination, Inspection, Maintenance and Testing of Items Important to Safety, Revision 3
  - NS-TAST-GD-013: External Hazards
  - NS-TAST-GD-014: Internal Hazards
  - NS-TAST-GD-076: Construction Assurance
- For International Atomic Energy Agency (IAEA) guidance and standards and Western European Nuclear Regulators' Association (WENRA) guidance, see the References section below.

ASSESSMENT PROCESS

107. The guidance described above provides high level principles. The technical standards used to design the civil structures will be considered in the ONR GDA assessment. If those standards are already considered by ONR as RGP, ONR will then focus the assessment on the application of those standards. However, if the RP designs the SSCs with novel or "in-house" design codes (see lessons learned section) then, the RP will need to demonstrate that those technical standards provide a design outcome which is consistent with what an approach using RGP would achieve.

108. As mentioned in the main guidance, the ONR inspector has a number of tools for use on the GDA assessment:

- Technical Support Contractor (TSC) – In GDA, the volume of information to examine and the level of expert knowledge expected requires the use of TSCs.
- RQs and ROs are the available tools to question and challenge aspects of the GDA design.
- The inspector Assessment Plan should highlight the scope of the assessment, timescales and assumptions.
- Level 4 meetings and workshops with the requested party – provide an open forum to debate technical issues.

109. In order to help the inspector in the assessment, it is recommended that design reviews with the Professional Lead (PL) are carried out at different stages of the assessment. Also it is advisable that the structure of the report is considered and discussed with the PL before the final submission.

3.2.3 INTEGRATION WITH OTHER TECHNICAL ASSESSMENT TOPICS

110. GDA requires the submission of an adequate, coherent and holistic generic safety case. Regulatory assessment of the civil engineering structures cannot therefore be carried out in isolation, as there are often safety issues of a multi-topic (or multidisciplinary) nature. Civil engineering interacts with a wide number of disciplines as it needs the input (loadings) from other disciplines to design the civil engineering structures that provide support to other SSCs.

111. The following interactions are normally considered during the civil engineering assessment:

- Radioactive waste and decommissioning – Interactions with radioactive waste and decommissioning topic are required in reviewing how the civil engineering construction may influence decommissioning techniques.
- Structural integrity – Interactions with the structural integrity topic are required, normally, on the containment or confinement design. Civil engineering structures provide support to structural integrity components (e.g. the reactor pressure vessel is supported by a civil engineering structure).
- Internal hazards – Provide input to the civil engineering design. Interactions with the internal hazards topic are required on civil and structural barriers identified to provide withstand against internal hazards. Interactions revolve around identification of the internal hazard load case and the structural substantiation to assess the civil structure stability and capacity under those loads.
- External hazards – Provide input to the civil engineering design (e.g. seismic loads, wind load, temperature load, etc.). Interactions with external hazards are normally required on the assessment of the effect of the external hazards on the civil engineering structures (e.g. seismic load cliff edge).
- Conventional safety – Interactions with conventional safety are required in reviewing the RP's approach to implementation of CDM 2015 and novel construction techniques.
- Severe accidents analysis (SAA) – Interactions with severe accidents are required during the evaluation of the containment capacity withstand to a severe accident scenario.
- Fault studies (FS) – Interactions with fault studies are required during the evaluation of the containment and other nuclear safety significant structures.
- Probabilistic safety assessment (PSA) – Civil engineering provides input to the containment structural analysis for the level 2 PSA assessment.
- Mechanical engineering (ME) – Interactions between both disciplines are needed as civil engineering structures support mechanical equipment. Some examples of these structures are the crane support columns and the turbine pedestal.

112. Civil engineering also has interactions with other disciplines, such as conventional fire, human factors, radiological protection and safeguards.

3.2.4 LESSONS LEARNED

113. There have been three GDAs completed in GB and as a result there are a number of lessons learned to inform new GDA inspectors and the RPs. Some of the lessons learned are generic and apply to more than one discipline. Table 1 summarises them. The main reasons behind the lessons learned are noted below:

- Design standards change with time and also computation techniques, hence the design submitted to GDA should consider if the design standards and computational techniques are regarded as RGP.
- Designs licenced outside GB do not guarantee a shorter or less complex GDA. All GDA submissions will be assessed in accordance to the GDA process described above.
- The GDA design should consider the structural material properties in combination with appropriate (RGP) standards and codes.
- In some cases, the GDA assessment may change the original design and this may have consequences in the rest of the civil engineering design or to other disciplines.
- ONR's expectations may differ in certain areas (i.e. aircraft impact).

- Inexperience on ONR's regulatory regime: the concept of ALARP, non-prescriptive regulatory regime, the concept and structure of a safety case (claims, arguments and evidence).
- Inexperience on UK regulations, e.g. CDM 2015.
- Selecting a large GDA scope carried out at different levels of detail.
- Underestimating the level of cross cutting issues – See below.

114. The cross cutting issues are complicated and civil engineering is involved in many of them. It is recommended that the inspector has an appreciation of these interactions and plans accordingly, with the rest of inspectors, which of their deliverable are likely to require civil engineering input.

115. The above areas are not the only areas where civil engineering input will be required, but they are the most demanding ones, in terms of resources and timescales.

116. Early engagement with the RP on the areas below is recommended:

- Scope of the civil engineering element of GDA.
- Definition of the "generic site".
- Analysis methods, including seismic analysis.
- Standards and codes. Discussion on ONR's expectations and RGP.
- Identify areas in the design and construction which are novel or First of a Kind (FOAK) in GB.
- Aircraft impact protection.
- Containment analysis.
- Beyond design basis expectations.

117. The table below provides an overview of the common GDA lessons learned which led to design changes in terms of physical changes or added justification/substantiation to the design.

Area	Lesson Learned
Generic - Categorisation and Classification	Robust categorisation and classification considering the effects on SSCs is needed. Better demonstration of design basis analysis (DBA) and cliff edge effects is needed. The RP should consider the effect of qualification of monitoring equipment and class 1 barriers on civil engineering structures.
FE and Seismic Electronic Models	It is considered good practice that the seismic models for SSI and Structural Analysis include Finite Element Models.
Code and Standards Compliance	Extensive code comparison is required if bespoke codes are used in the design.
Beyond Design Basis Events	Where no appropriate established codes or standards are available extensive justification of the use of similar codes and demonstration of the reliability achieved by their use is required.
Dropped load and Pipe Whip	The RP should consider that ONR has different assumptions regarding the type of aircraft involved in the impact load case.
CDM 2015	The RP should consider the cliff edge effects from combined hazards.

Area	Lesson Learned
Concrete Containment – Ultimate Pressure Capacity	There are different assumptions on incident loads informed by internal hazards.
Modern code requirements	ONR requires the designer (RP during GDA) to understand (and mitigate) the risks associated with construction, commissioning, operations and decommissioning of the plant
UK material codes and standards	ONR requires a demonstration that the risks of failure of the concrete containment are ALARP and the design has sufficient margin. RP had to confirm the margins on the concrete containment (ultimate pressure capacity).
Containments	Modern approaches to the design for the fire safety of novel forms of construction are required.

3.2.5 REFERENCES

- IAEA – Safety Standards: Safety of Nuclear Power Plants: Design, Specific Safety Requirement Series No. SSR-2/1, 2012
- IAEA – Safety Standards: Fundamental Safety Principles Series No. SF-1, 2006
- IAEA – Safety Standards: Safety of Nuclear Power Plants: Seismic Design and Qualification for Nuclear Power Plants Series No. NS-G-1.6, 2012
- WENRA - Statement on Safety Objectives for New Nuclear Power Plants and Safety of New NPP Designs

3.3 CONTROL AND INSTRUMENTATION

118. C&I performs a significant nuclear safety role through the provision of automatic and manual control of equipment that has a nuclear safety function, and by providing feedback on the status of the reactor and associated equipment to operators and support staff.

119. ONR's C&I assessment covers the design, analysis, commissioning, operation, testing and maintenance of a wide range of C&I systems. Some designs may make claims on passive systems or inherent safety to deliver safety functions, with only limited demands on C&I systems.

3.3.1 SCOPE FOR GDA

DOCUMENTS SUBMITTED

120. The RP's C&I documentation should demonstrate that C&I systems can achieve an adequate level of risk control, in response to challenges such as failure of the reactor control system to maintain reactor parameters within defined limits, failure of mechanical systems, the effects of internal hazards, and external phenomena such as lightning. C&I safety analysis should also cover cyber threats.

121. Documentation is normally in the form of a safety case that presents safety claims, arguments, and evidence to support the claims and arguments. This should be sufficiently detailed to identify the role of each different layer of protection, and specific systems within these, in terminating all postulated design basis faults.

122. The RP should demonstrate resilience of C&I systems to common cause failures which could challenge the operation of more than one layer of protection or equipment train.

123. It is normal for a large number of C&I documents to be submitted covering the following areas:

- A safety case head document that sets out the high level C&I claims that will be argued. The claims should be related to the overall plant safety claims and should be based on input from fault studies, deterministic criteria and PSA assessments. Safety functional claims and safety property claims should both be identified.
- A description of the C&I architecture, connectivity and layers of protection, including displays and controls, how this meets the C&I claims, and its dependence on systems and platform performance.
- A description of each relevant C&I system and how this meets the C&I architecture and higher level claims.
- A description of each relevant C&I platform and how this meets the C&I system and higher level claims.
- Evidence that the C&I systems and platforms are engineered to achieve adequate reliability, including analysis and schemes for testing and maintenance.

SAMPLING AREAS

124. The relevant inspector will decide the areas of design that ONR will sample. ONR will seek confidence that the design is in line with RGP and the risks have been reduced so they are ALARP.

125. The C&I inspector will typically assess the following:

- Fault schedule.

A prerequisite for determining the adequacy of C&I systems is the development of a comprehensive fault schedule using appropriate hazard identification and analysis techniques (see the generic topic on fault schedules within this document). The fault schedule should include the potential for spurious actuation arising from C&I faults.

- Categorisation of safety functions and classification of C&I systems important to safety.

The safety case should present a mechanism to identify and categorise safety functions to be delivered by C&I systems. Typically a three-tier categorisation scheme would be expected that is fully integrated with scheme used in the wider safety case whilst being fully consistent with the requirements of International Electrotechnical Commission (IEC) 61226.

C&I systems that perform safety functions should be classified. Again, a three-tier approach is expected which is both consistent with the approach adopted in the wider safety case and the methodologies described in in IEC 61226 and IEC 61513.

- Severe Accidents.

Any claims on severe accident C&I systems to actuate or inform actions taken during the management of a severe accident need to be identified in the submitted documentation. It is important that the functional requirements, system classification, independence assumptions, and qualification expectations are all captured and

substantiated, in addition to design basis requirements. This should take into account learning from the Fukushima event.

- Overall C&I Architecture.

The architecture of the C&I systems should be described and demonstrated to be adequate. This should describe the provision of sufficient layers of protection that are suitably independent and diverse. In GB the overall architecture of NPP C&I systems is often based on a three platform design. This is:

  - Platform 1 – Primary Protection System.
  - Platform 2 – Secondary (or Backup) Protection System.
  - Platform 3 – Control System.

Areas to be covered in the safety case include:

  - There should be sufficient layers of protection to demonstrate an adequate level of risk control. The individual layers of protection should provide balanced risk control without too much reliance on any single layer of protection. ONR's TAG NS-TAST-GD-046 provides guidance on the maximum risk reduction that can be claimed for software-based and other C&I systems.
  - Each layer of protection should be sufficiently independent of the others, including sensors, actuators, support systems, and resistance to internal hazards. Highest class systems should continue to deliver safety functionality in the presence of a fault.
  - Each layer of protection (including displays and controls) should be adequately diverse from the others to avoid common cause failures leading to complete loss of ability to take safety actions. It should be demonstrated that lower class systems cannot compromise the function of higher class systems through the avoidance of communication links and other connections.
  - Where different layers of protection control the same actuator, design features to ensure the highest classification system takes priority should be present, sufficiently reliable, resistant to common cause failures, and unaffected by all faults of lower class systems.
  - It should be demonstrated that C&I equipment can be maintained to support continued reliable operation, without significantly increasing risks.

- Platform qualification.

The safety case for each C&I system platform should demonstrate how reliability will be achieved. This should cover hardware and software (operating system, firmware and application software), and demonstrate adequate reliability for its configuration and operational environment, using modern hazard identification and analysis techniques. A demonstration of adequate software reliability should include evidence of Production Excellence (PE) and of the application of suitable Independent Confidence Building Measures (ICBM's), see NS-TAST-GD-046. Hazards arising from software tools should be identified and demonstrated to be eliminated or adequately managed.

- Smart device qualification.

Smart devices are individual devices such as sensors that contain a microprocessor or complex logic. These may be standalone or integrated into mechanical plant or other equipment. Where a smart device is used to perform a safety function, evidence suitability should include PE and ICBMs, as necessary, according to its classification.

In GB, evidence of PE can be gathered using an Emphasis assessment. Smart devices should be qualified to demonstrate they are suitable for their intended application environment. It should be demonstrated that the common cause failure of multiple smart devices deployed across multiple systems does not result in significant risk increase.

- Displays and Controls.

The requirement for displays and controls, and their functionality, should be established using an appropriate operational and human factors assessment. It should be demonstrated that the C&I design is suitable to meet the identified requirements. This should include a demonstration of adequate reliability, independence and diversity of displays and controls relating to different layers of protection, resistance to common cause failure, and suitability for the intended environment. There should be a means to monitor the plant status and take action in the event the main control room becomes uninhabitable, and under severe accident conditions.

- Cyber security.

Resistance to cyber threats on C&I systems important to safety should be demonstrated, and mitigation(s) identified. This includes the potential for malware to be inserted within the supply chain, and should not be solely reliant on air gaps. The selection of suitable technologies and architectural approaches are the most effective approaches to achieve this.

- Essential services.

Essential services ensure the continued operation safety systems. For C&I systems this is likely to include electrical power, and cooling and ventilation systems (e.g. HVAC), although other essential services such as hydraulic power may be necessary to ensure that a C&I system can take action.

Essential services would normally be assigned the same classification as the safety systems they are supporting.

3.3.2 BASIS FOR DECISION

126. ONR's sampling strategy during GDA is to focus on the areas of greatest technical challenge or which have the greatest safety significance.

127. The initial sampling strategy for assessment may consist of a "broad brush" review of the documents submitted by the RP, followed by a "deep dive" detailed technical assessment of areas that require regulatory attention.

STANDARDS AND GUIDANCE

128. The C&I platforms, systems and their connectivity will be assessed to confirm alignment with the objectives of the relevant ONR SAPs and TAGs.

129. TAG's important to the assessment of C&I systems performing safety functions include but are not limited to:

- NS-TAST-GD-003 – Safety Systems.
- NS-TAST-GD-015 – Electromagnetic Compatibility.
- NS-TAST-GD-019 – Essential Services.
- NS-TAST-GD-031 – Safety-related Systems and Instrumentation.
- NS-TAST-GD-046 - Computer Based Safety Systems.

- NS-TAST-GD-094 - Categorisation of Safety Functions and Classification of Structures and Components.

130. In addition, ONR uses a range of international standards, including those published by the IAEA and the IEC to inform its assessment of C&I systems (see the Reference section below).

ASSESSMENT PROCESS

131. The guidance described above provides high level principles. ONR will seek to confirm the design meets regulatory expectations, as expressed in standards, guidance and GB RGP. The assessment will be based on a generic plant design. Claims regarding design features relevant to a specific site are not relevant to GDA.

132. The ONR inspector has a number of tools and activities to direct and inform the C&I assessment:

- The inspection assessment plan will set out the scope of the assessment, timescales and limitations.
- RQs and ROs are used to request further information from the RP, and raise challenges on the adequacy of the design.
- Level 4 technical meetings and workshops to clarify understanding and confirm regulatory expectations.
- TSC – In GDA, the volume of information to examine and the level of the expert knowledge required often requires the use of TSC's.

3.3.3 INTEGRATION WITH OTHER TECHNICAL ASSESSMENT TOPICS

133. C&I system designs influence and are influenced by a number of other topic areas. There will be a requirement for coordination across various topic areas to consider the adequacy of the overall design integration.

134. The following interactions are normally considered during the C&I assessment:

- Fault studies – These specify claims on the C&I systems and consider C&I failures.
- Electrical engineering – These cover control interfaces, smart device qualification and essential services.
- Mechanical engineering – These cover design features of safety systems and reliance on C&I.
- Internal and external hazards – These identify risks to C&I operation and failure independence.
- Human factors – These have many interactions with C&I, including displays and controls, alarms, and maintenance.
- Probabilistic safety assessment (PSA) – These confirm the capability of the C&I systems' design to meet risk targets.
- Security – These cover the requirements for the protection against computer security threats.

135. Other examples of disciplines which C&I may interact with include: conventional fire, radiological protection, safeguards, and severe accident analysis.

3.3.4 LESSONS LEARNED

136. Significant lessons learned from previous GDA assessments in the C&I technical area are as follows:

- RPs should fully understand regulatory expectations for the C&I safety case to be presented in a claims, arguments and evidence (CAE) format to support the safety case head document. As the role of the C&I systems is that of actuating safety systems the claims should be established from the requirements of the safety systems primarily arising from the fault schedule. Claims should also be established for the capability of the C&I systems to withstand faults, and internal and external hazards.
- There is a requirement for overall risk to be demonstrated to be ALARP. This generally means that a number of options will have been shown to have been considered, and why the design selected is ALARP.
- Many designs have been presented to ONR where the layers of protection are not demonstrated to be independent and adequately diverse. Particular challenges include common electrical supplies, common microprocessors/software, shared sensors and communications from lower class systems to higher class systems.
- It is common for excessive risk reduction claims to be made for software-based and other C&I systems. Guidance on limits that will be accepted by ONR is in NS-TAST-GD-046.
- Where priority systems are used to enable more than one class of system to take a safety action, it is important that the RP is able to demonstrate that the risks arising from common cause failure, and spurious actuation are demonstrated to be acceptable.
- The RP should specify the intended approach to Smart Device qualification and confirm this is suitable for each safety class within the GB context. This should cover PE, ICBM's, and environmental qualifications. Consideration should be given of the potential for common cause failures to occur where Smart Devices are used in multiple points in the C&I architecture.
- The GDA assessment should be based on a generic design. Site-specific design features should not be taken into account in the GDA assessment.

3.3.5 REFERENCES

- IAEA – Safety Standards: Specific Safety Requirements SSR-2/1 – Safety of Nuclear Power Plants: Design.
- IAEA – Safety Guide SSG-30 – Safety Classification of Structures, Systems and Components in Nuclear Power Plants.
- IAEA – Specific Safety Guide SSG-39 – Design of Instrumentation and Control systems for Nuclear Power Plants.

137. IEC standards commonly used in ONR's C&I assessment, include but are not limited to:

- IEC 61513 - Nuclear power plants - Instrumentation and control important to safety — General requirements for systems.
- IEC 61226 - Nuclear power plants — Instrumentation and control systems important to safety — Software aspects for computer based systems performing category A functions.
- IEC 61508 - Functional safety of electrical electronic programmable electronic safety-related systems.
- IEC 60880 - Nuclear power plants - Instrumentation and control systems important to safety. Software for category A functions.
- IEC 62566 - Nuclear power plants — Instrumentation and control important to safety — Development of HDL-programmed integrated circuits for systems performing category A functions.
- IEC 60987 - Nuclear power plants - Hardware design requirements for computer based systems.

- IEC 62138 - Nuclear power plants — Instrumentation and control important for safety - software aspects for systems performing Cat B or C functions.

3.4 CONVENTIONAL FIRE SAFETY

138. The aim of ONR's conventional fire safety assessment within the GDA process is to ensure the final structural design of the power station meets ONR expectations for fire safety for protection of people from the danger of fire.

3.4.1 SCOPE FOR GDA

139. In UK safety law, there is a requirement for risks to be reduced ALARP. One way of achieving this is by ensuring the design meets RGP, but in the case of departures from this practice the legal requirement can still be satisfied provided ALARP Is demonstrated. For fire, this would require suitable and sufficient risk assessment. Within GDA, some building design elements may be yet to be defined, but ONR is looking for considerations of potential fires and their potential impact on life safety to be addressed as far as is appropriate, and for design processes to be aware of this need.

140. In some cases design for fire safety can potentially conflict with design requirements relating to the function of a NPP or there may be conflicts with considerations of nuclear safety and security. If this is the case a holistic ALARP demonstration will need to adequately address all safety and security aspects.

141. Fire modelling can be used to support ASET / RSET claims; however this is likely to be time consuming for the RP and may require ONR to consider independent verification.

KEY ASSESSMENT TOPICS

142. The GDA for fire safety should focus mainly on the structural requirements to achieve satisfactory means of escape for site personnel and access arrangements for firefighters.

143. Typical structural arrangements relevant to GDA include:

- Numbers and width of exit doors and staircases.
- Escape distances to places of safety.
- Escape provisions for areas where escape is possible in one direction only.
- Fire protection provided for escape routes.
- Arrangement of exit routes from within rooms.

144. "Non-structural fire provisions" such as the details of fire warning systems, emergency lighting, signage and management arrangement will be site-specific issues, These will be considered during the Licensing process and based on more detailed design details. As a result they may not need to be considered in GDA. However, if these arrangements are claimed within GDA as a part of the ALARP demonstration for a building with departures from codes of practice, then it will be necessary for the designer to provide clear specification of the intended non-structural fire provisions.

DOCUMENTS SUBMITTED

145. **Safety Case**: Further guidance on what is acceptable to ONR as the top tier safety case summary document or Head Document for GDA is available elsewhere, and these may take a variety of potential forms, as agreed with ONR. For the current discussion, the term "Pre-Construction Safety Report" is used for the first substantive

documents to contain conventional fire safety information. With respect to conventional fire safety, these documents should give adequate emphasis to; -

- Arrangements to protect people from fire (however a safety case head document historically often focuses solely on equipment and building protection, i.e. the effects of fire on the nuclear safety case).
- Means of escape in case of fire should, ideally, be a discrete subject in the PSR.
- There should be adequate emphasis on risk assessment and ALARP justification in fire safety design of buildings. The application of prescriptive codes alone is insufficient to satisfy UK legal requirements.
- There should be evidence of the use of the hierarchy of risk controls in the selection and application of mitigation measures.

146. **High-level Fire Strategy document:** This is a project-wide document intended to demonstrate the interaction of fire safety legislation, building regulations and ALARP principles. The conventional fire safety strategy will cover the protection of people from the dangers of fire and give a clear presentation of the designer's understanding of UK fire safety legislation, which is goal setting and mainly non-prescriptive. Alternative approaches to demonstrate the same requirements may be put forward by the designer.

147. **Fire Safety Design document:** ONR will be looking for evidence that the design of any building on the nuclear site will be a structure that meets its expectations for the protection of people from the danger of fire. This can be by the production of a Fire Safety Design document for each building, to describe the application of the published guidance; and the degree of compliance with GB good practice. The designer may identify that it will not be possible to completely meet all the recommendations of guidance in achieving the functions of a NPP, but the Fire Safety Design document should include detail about how departures from compliance with building design guidance will still satisfy the requirements of UK law. This will include methods to:

- Identify all areas where the design departs from accepted codes of practice.
- Assess and prioritise the risk gap from UK design guidance.
- Optioneer a range of alternative mitigation measures.
- Provide a convincing ALARP justification for the selected fire engineered alternative mitigations.

148. **Fire Safety Strategy Documents**: A set of documents fulfilling the needs described will be required for each facility. The form this will take and the schedule of supplying this will be agreed with ONR. Fire Safety Strategies should describe the preventative and protective arrangements to reduce the risk to life safety from fire and to describe the measures to ensure escape to a place of safety. The document will clearly identify all departures from building code compliance and describe the fire engineered mitigations. The Strategy should fully demonstrate the implementation of the management process described in the Fire Safety Design document. Additionally, information on characteristics of the building relevant to fire performance are expected, such as:

- A description of the function of each facility.
- Building occupancy levels.
- Number and arrangement of doors giving access to final exits.
- Number and arrangement of staircases including their access to open air.
- Fire protection arrangements for staircases.
- Fire load characteristics of the building.
- Arrangements to protect the means of escape in case of fire.

- Site plans, details of internal layout and 3-D models: These may help in the understanding of this information provided in other documents.

149. **Reports from Fire modelling:** Fire modelling can be used to support claims within the conventional fire risk assessments; however this is likely to be time consuming for the RP and may require ONR to consider independent verification.

3.4.2 BASIS FOR DECISION

150. Nuclear Licensed Sites are exempt from the Building Regulations which normally ensure that the dutyholder, in the final occupied building, can achieve compliance with the structural means of escape requirements of the Regulatory Reform (Fire Safety) Order 2005. However the published guidance to satisfy the Building Regulations for fire safety in the design of similar buildings represents RGP against which new buildings should be benchmarked – and this applies to GDA.

151. Compliance with International fire safety specifications alone will not guarantee the building satisfies UK legal requirements. The RP is still required to demonstrate that their design achieves RGP and that risks are reduced ALARP.

STANDARDS AND GUIDANCE

152. Approved Document B to the Building Regulations is the appropriate fire safety design guide for conventional smaller buildings on the nuclear licensed site. For these types of building there is little justification for departures from the recommendations in guidance and full compliance is expected. However the RP may wish to submit this type of building for assessment during Nuclear Site Licensing since there is less regulatory risk with these buildings.

153. Buildings on the nuclear island benefit from benchmarking against British Standard 9999: the Code of Practice for Fire Safety in the Design Use and Management of Buildings: 2017. This code of practice provides a systematic but flexible approach to design, and allows the fire engineer to take advantage of the additional fire protection arrangements routinely provided in a nuclear facility.

154. For most areas, the RP should achieve compliance with BS 9999. Where departures are necessary to achieve the function of a NPP, individual fire compartments should be assessed by extending the provisions of BS 9999 with the application of fire engineering principles contained within BS 7974.

155. Departures from compliance with guidance should be addressed by the RP, consistently, systematically, and be supported by a robust holistic ALARP justification. In many cases an adequate justification can be provided through extension of the applicable mitigations contained within BS 9999, without resorting to the full procedure described in BS 7974. Relevant mitigation, with examples within the current nuclear fleet, which may be provided to reduce the risk to life safety from fire, include:

- Enhanced automatic fire detection.
- Fixed firefighting water sprinklers, or other installed fire suppression systems.
- Smoke control / Ventilation.
- Compartment geometry and volume.
- Control and assessment of fire loadings within buildings and fire compartments.
- Management restrictions / access control.
- Training & evacuation arrangements.

3.4.3 INTEGRATION WITH OTHER TOPIC AREAS

156. There are strong links with the internal hazards assessment area (since this addresses the effects of fires and explosions on nuclear safety), and with civil engineering. There are also important interactions with Security (because of the tension between means of escape and egress and the necessary controls over access to plant areas).

157. Some other disciplines also have interactions. This may include C&I (with respect to some areas of fire alarms), electrical engineering (fire risks), emergency planning (because emergency provisions may include manual firefighting and access provisions), nuclear liabilities (during decommissioning) and human factors (fire response, evacuation, movement of personnel, design of fire-fighting equipment).

3.4.4 LESSONS LEARNED

158. In the earliest applications of GDA to NPP designs new to GB, conventional fire safety assessment was excluded from the scope of ONR's assessment. Instead, these issues were discussed as part of the initial licensing phase and further addressed in the detailed design permissioning phases subsequent to the granting of a site license. This was rectified in the application of GDA to later applicants. This was because it was realised that it was beneficial to both parties to commence this assessment activity in the GDA phase for regulatory risk reduction and because of the links with other design decision affecting Safety and Security. Based on experience from the GDAs that considered conventional fire, a number of important lessons have been learned on the approach and shortcomings in the conventional fire related aspects of RPs' safety cases. Key themes are presented below:

- Engagement of GB technical support.

Since designers may be more used to a prescriptive regulatory approach rather than a goal directed one, and therefore unfamiliar with a risk based approach to safety, then in previous GDA projects it has been found helpful for the designer to engage GB technical support. This may be a person or organisation familiar with UK safety law and the application of benchmarking against GB RGP for fire safety. A SQEP or support organisation can also advise on the early identification of significant risk areas.

- Production of a High-level Fire Strategy document.

ONR has found advantage during previous GDA and licensing projects in asking the designer to confirm their understanding of UK Legislation relating to fire safety by producing a high-level Fire Strategy document. The purpose and content of these has been described in section 3, above, but it allows an overview of the fire strategy for the site.

- Production of a Fire Safety Design document for each building.

In previous GDAs, a useful way of demonstrating that the design of any building on the nuclear site has properly considered how to meet ONR's expectations for the protection of people from the danger of fire was by the production of a Fire Safety Design document for each building. This describes the application of the published guidance; and the degree of compliance with good practice (Approved Document B, British Standard 9999 and British Standard 7974). This has also been described in section 3 above.

- Targeting of resource onto areas of priority for designers and regulators.

In previous GDA projects, with respect to conventional fire safety, there have been advantages in targeting areas for early resolution. ONR and the designers have benefited in cases whether the designer has provides a document which surveys the building designs across the site to give an initial overview of life safety issues. The aim is to identify areas that significantly depart from guidance or areas where there are obvious major fire safety risk areas. When considered against ONR's expectations, initial building designs from other legal jurisdictions, may require a structural alteration to meet GB goal driven expectations (including that risks are reduced ALARP). In particular this may include areas which depart significantly from the recommendations contained within British Standard 9999. In other GDA projects for new NPPs the following subject areas have caused challenges:

- Extended escape distances particularly where escape is available in one direction only.
- Inner-inner room situations.
- Inadequate fire resisting protection for, or the presence of, combustibles in escape routes.
- Staircases which do not discharge directly to open air.

For early resolution of difficult areas, priority of delivery should be given to the facilities identified in this targeted assessment of major fire safety risk areas. Typically, for previous GDA projects, this has been the reactor building, safeguard building and fuel buildings.

3.4.5 REFERENCES

159. ONR at the moment has no TAG covering conventional fire safety, and GB RGP appropriate to other industrial sites are adopted. This includes an expectation that for any areas where relevant UK building regulations have not been met, the designer is providing a fire strategy and fire risk assessment for the practice that they have adopted.

- Fire Safety: Approved Document B to the Building Regulations, https://www.gov.uk/government/publications/fire-safety-approved-document-b
- British Standard 9999: the Code of Practice for Fire Safety in the Design Use and Management of Buildings: 2017
- BS 7974:2001**:** Application of fire safety engineering principles to the design of buildings. Code of practice**:** 2001

3.5 CONVENTIONAL HEALTH AND SAFETY

160. ONR's assessment of this subject area focusses on elements of the design within the scope of GDA with the potential to pose significant conventional (non-nuclear) risks to the health and safety of persons who are either engaged in the construction, operation, maintenance or decommissioning of the nuclear power station, or may be affected by these undertakings.

161. ONR regards the design, intended for construction and operation in GB, to be a construction project under the CDM 2015, and accordingly, that the concept design, and any modifications arising, should address, so far as is reasonably practicable, health and safety issues arising both during construction (including decommissioning) and operational use and maintenance of the building structures.

162. This topic does not include life fire safety or radiation protection – these are dealt with in separate sections of this document.

3.5.1 SCOPE FOR GDA

163. ONR will assess the RP's understanding of UK health and safety statutory requirements on a sampling basis against confirmed topics selected for their risk significance, applicable to the construction and decommissioning phases of the reactor design, and also its operation and associated maintenance.

164. The Health and Safety at Work etc. Act 1974 is the primary piece of legislation covering occupational health and safety in GB, which together with secondary legislation ('regulations') provides the legal framework for ONR's approach.

165. A fundamental principle of UK health and safety law is that those who create risks are best placed to control them. ONR expects the RP to demonstrate ownership of the design hazards and control measures, via understanding of the GB risk-based and goal-setting assessment approach.

166. ONR's approach to the assessment of the generic design is founded upon the requirements upon the designer in CDM 2015 in the preparation or modification of a design. CDM 2015 requires the designer, with consideration of 'The general principles of prevention' (a requirement of the Management Regulations 1999) to eliminate, so far as is reasonably practicable, foreseeable risks to health or safety, or where this is not possible, to reduce or control such risks to persons arising during construction (including decommissioning), maintenance, cleaning and operation.

KEY ASSESSMENT TOPICS

167. ONR 's key topic areas for assessment will be selected in the context of the design and recognised areas of known conventional health and safety risks that are most likely to cause harm, including, but not limited to:

- Work at height.
- Lifting operations.
- Health risks.
- Work in confined spaces.
- Structural stability.

168. Additionally, GB novel, innovative or unusual design approaches, with potential health and safety implications may also be reviewed and assessed.

169. It is to be anticipated that ONR multi-disciplinary inspector interaction will prompt additional assessment topic queries requiring a coordinated response by the RP to relevant, assigned topic inspectors.

DOCUMENTS SUBMITTED

170. It is ONR's expectation the RP's submission for the defined scope concentrates on those risks that are most likely to occur and which cause most harm, demonstrating, as appropriate, action to reduce serious risks so far as is reasonably practicable.

171. The RP's documentation should demonstrate measures are in place during the design process to:

- Identify hazards.
- Assess the risks and the consequences of those hazards being realised.
- Put in place suitable measures and procedures to control the risks.

172. The RP should demonstrate an understanding of and appropriate reference to relevant 'good practice' in the determination of control measures to address and reduce health

and safety risks which cannot be eliminated Good practice includes Approved Codes of Practice (ACOPs), published by HSE (the UK's lead health and safety regulator), providing practical advice on how to comply with the law; and HSE guidance available at www.hse.gov.uk. Other sources of recognised good practice include Standards produced by Standards-making organisations, including British Standards, CEN; and trade federation and professional bodies.

173. The RP is expected to demonstrate via their submissions their chosen design or design concept reduces risks so far as is reasonably practicable, with due reference to relevant statutory provisions and good practice. Assessment includes, but is not necessarily limited to, the preparation by the RP of Topic Reports on agreed risk topic areas.

174. ONR expects to receive RP topic specific submissions demonstrating, with reference to supporting examples across the lifecycle of the design, encompassing construction, plant operation, maintenance and decommissioning, RP understanding of relevant UK subject legal requirements. The submissions should describe, with evidence, action taken to eliminate, or, where this is not possible, to reduce or control risks to the health and safety of construction workers, operatives and others, so far as is reasonably practicable.

175. The RP is expected to demonstrate how significant risk design information will be recorded and shared with relevant parties, including use of information technology.

3.5.2 BASIS FOR DECISION

STANDARDS AND GUIDANCE

176. The non-nuclear requirements to prepare a safety case are limited to specific regulations, for example The Control of Major Accident Hazards Regulations 2015 (COMAH), which requires that the report show arrangements are in place both for the control of major accident hazards and to limit the consequences to people and the environment of any that do occur. The RP may wish to produce holistic safety cases in which both nuclear and relevant conventional health and safety risks are considered.

177. ONR will assess Topic Report and other RP submissions against UK legal requirements, relevant ACOPs, HSE published guidance, relevant Standards, and where applicable, guidance published by trade federation and professional bodies, to confirm that legal compliance has been achieved and RGP considered and appropriately referenced. These are listed in the reference section below.

178. ONR will give consideration to the hierarchy of risk control measures presented, prioritising collective over individual measures.

179. ONR will assess whether the RP's design proposals are proportionate and risk-based.

180. In the event of GB novel work methods being proposed the RP will be approached for qualitative and quantitative evidence to inform risk assessment outcomes.

3.5.3 INTEGRATION WITH OTHER TOPIC AREAS

181. The conventional health and safety inspector works closely with inspectors in other topic areas, both in consultation with those inspectors and in the provision of conventional health and safety input to those inspectors. Examples of joint working include civil engineering, on novel construction method assessment; mechanical engineering on matters including lifting operations and work at height; radioactive waste and decommissioning; and human factors on worker – equipment interface

matters. These are important and relevant interactions which positively inform the GDA process.

182. Conventional health and safety may also interact with other disciplines, such as internal hazards.

3.5.4 LESSONS LEARNED

183. Dedicated conventional health and safety input has been assigned to only one of three completed GDA projects. The following matters are emerging challenges in the assessment of conventional health and safety submissions.

- The GB risk-based and goal-setting assessment approach requires the provision of evidence demonstrating a design reduces risk as low as is reasonably practicable. This requirement may be in contrast to more prescriptive regulation in some non-European states.
- Education of those involved in the design process may be required to support necessary justification that the design reduces health and safety risk as low as is reasonably practicable across the lifetime of the plant - during construction, operation and maintenance and decommissioning in accordance with UK conventional health and safety legislative requirements.
- The RP must be alert to the necessity for and challenges arising when undertaking gap analysis to confirm detail of differences in regard to critical health and safety compliance.
- Limited (or absent) comparative health and safety incident data can result in difficulties for the RP when seeking information to support an application demonstrating effective risk assessment for GB novel techniques, including construction methodologies.

3.5.5 REFERENCES

184. Reference should be made to UK Health and Safety Legislation accessible at www.legislation.gov.uk including:

- Health and Safety at Work etc. Act 1974
- Construction (Design and Management) Regulations 2015
- Management of Health and Safety at work Regulations 1999
- Provision and Use of Work Equipment Regulations 1998
- Workplace (Health, Safety and Welfare) Regulations 1992
- Lifting Operations and Lifting Equipment Regulations 1998
- Work at Height Regulations 2005
- Confined Spaces Regulations 1997
- Control of Substances Hazardous to Health Regulations 2002
- Manual Handling Operations Regulations 1992
- The Control of Noise at Work Regulations 2005
- The Control of Vibration at Work Regulations 2005
- Dangerous Substances and Explosive Atmospheres Regulations 2002
- The Electricity at Work Regulations 1989
- Pressure Systems Safety Regulations 2000

185. Reference should be made to RGP from sources including the following.

- Approved Codes of Practice, including:
  - “Safe use of lifting equipment. Lifting Operations and Lifting Equipment Regulations 1998. Approved Code of Practice and guidance”. L113 www.hse.gov.uk/pubns/books/l113.htm

- "Safe work in confined spaces. Confined Spaces Regulations 1997. Approved Code of Practice". L101 http://www.hse.gov.uk/pUbns/priced/l101.pdf
- "Control of substances hazardous to health. The Control of Substances Hazardous to Health Regulations 2002 (as amended). Approved Code of Practice and guidance". L5 (Sixth edition) http://www.hse.gov.uk/pubns/priced/l5.pdf

- Published HSE guidance, including:
  - "Reducing Risks: Protecting People – HSE's decision making process" www.hse.gov.uk/risk/theory/r2p2.pdf
  - "Managing health and safety in construction: Construction (Design and Management) Regulations 2015". L153 www.hse.gov.uk/pubns/books/l153.htm
- Relevant British Standards, available from the British Standards Institution, www.bsigroup.com/en-GB/ including:
  - BS 5975:2008 "Code of practice for temporary works procedures and the permissible stress design of falsework"
  - BS 7121 series of Standards "Code of practice for safe use of cranes" (there are several within the series tackling various types and standards of crane).

3.6 ELECTRICAL ENGINEERING

186. The electrical power distribution network at a NPP performs a significant nuclear safety role through providing power to all SSCs with electrically driven equipment that have a nuclear safety function.

187. ONR's electrical engineering assessment considers the design, installation, operation and maintenance of the electrical power distribution network.

3.6.1 SCOPE FOR GDA

188. Safety analysis of the electrical power distribution network should assess the capability of the electrical power system(s) to support electrically operated safety systems in response to challenges, including:

- Loss of offsite power.
- Electrical transient disturbances both onsite and offsite.
- Electrical fault conditions.
- External phenomena such as lightning and severe weather that can cause disturbances to normal plant operation and severe accident conditions.

189. The RP should demonstrate the resilience of the electrical system to common cause failure which could challenge the operation of redundant and diverse components that are provided to achieve high reliability.

190. A demonstration of the safety of the plant should be presented in the top tier safety case summary document. In addition, the RP should submit supporting design documents for ONR assessment of the capability and resilience of the electrical power distribution network to perform its safety functions.

191. These documents should include the relevant chapters of the safety case head document, single line diagrams, layout drawings, design reports and system study documents to facilitate assessment of the key assessment topics.

KEY ASSESSMENT TOPICS

192. The following aspects of the electrical power distribution network should be assessed:

- System Architecture.

An assessment should be undertaken of the basic architecture of both the Alternating Current (AC) and Direct Current (DC) electrical systems. This should examine the capability of the divisional structure of the electrical system to support SSCs, including safety systems, in accordance with the plant design philosophy. The design aspects to be assessed should include the following:

  - Connections to the main generator and main and standby connections to the transmission system operator network.
  - Provision and design of the on-site AC electrical distribution network.
  - Provision and design of standby AC power sources including station black-out aspects.
  - Provision and design of DC systems and electrical batteries.
  - Independence of electrical power systems in each division.
  - Maintainability of electrical equipment to support reliable operation.

- Electrical Protection.

An assessment should be undertaken of the electrical protection philosophy for the NPP. This should confirm that the design of the electrical protection system and the settings used ensure the continuity of supplies by isolating electrical faults close to the source of the fault to reduce the risk of common cause failure which could impact on the continuity of supply to nuclear safety systems.

- Cable Routing.

An assessment should be carried out of the basic principles to be adopted for the routing of electrical cables. This assessment should focus on the design of cable routes to meet specific electrical requirements regarding segregation and separation of cable routes and thermal rating of cables. This assessment should be performed in conjunction with internal hazards assessment of specific hazards such as fire, flood and internally generated missiles, and external hazard risk assessments.

- Earthing and Lightning Protection.

An assessment should be carried out of the design of plant earthing and lightning protection. This should focus on assessment of the earthing system design for compliance with the safety classification of the system and the capability of the lightning protection system to protect plant equipment from the effects of lightning strikes. Particular attention should be given to protection against common cause failure.

- Basis of Safety Cases.

The safety case for the electrical power system and associated equipment and components should be supported by a Basis of Safety Cases (BSC) document which presents the safety claims made on the plant electrical distribution system. The claims should be related to the overall plant safety claims and should be established based on input and from fault studies and PSA assessments. A structure of supporting arguments and documentary evidence should be provided in the BSC to substantiate the safety claims.

- Electrical System Model.

A computer based model should be established by the RP for the purpose of studying the system under steady state conditions and in response to a range of postulated disturbances which can challenge the system performance. The studies should consider all modes of operation including normal operation, plant shutdown, on line plant maintenance, testing of standby sources and operation from standby sources.

The model should be based on a recognised form of standard commercial software package. The studies to be performed should include:

- Load flow study to verify equipment ratings.
- Short circuit studies to demonstrate that equipment has appropriate short circuit fault capability.
- Motor starting studies to demonstrate that motors can be started under the most onerous conditions.
- Bus transfer system transient studies.
- Transient studies of the consequences of failure or malfunction of the main generator AVR.
- Post electrical fault recovery studies.
- Studies of system response to grid faults and loss of grid supplies.
- Studies of system response to TSO grid code operating requirements.
- Studies of the effects of voltage transients.

The results of the studies should be assessed to confirm compliance with pre-defined acceptance criteria.

3.6.2 BASIS FOR DECISION

STANDARDS AND GUIDANCE

193. ONR carries out its assessment activities on a proportionate and sampling basis and in GDA assessment sampling is used to improve the overall efficiency of the design review process.

194. The initial sampling should assess the architecture and physical layout of the electrical power distribution network to consider compliance with relevant ONR SAPs. More detailed assessment should then be undertaken of key features of the system to provide confidence in the robustness of the electrical engineering design.

195. The following TAG is key to the assessment of the electrical system design:

- NS-TAST-GD-019 – Essential Services.

196. In addition, ONR uses a range of international standards, namely those published by the IAEA and the IEC to inform its assessment of C&I systems. These include, but are not limited to, those standards listed in the reference section below.

197. ONR should assess the generic design for compliance with the relevant guidance. The assessment should be based on a generic plant design. Claims regarding design features relevant to a specific site should not be taken into account. In particular, this applies to site-specific grid connection arrangements.

198. An important aspect of the assessment is considering the diversity in the design and mitigations against the risk of Common Cause Failure (CCF). ONR's expectation is that design diversity is demonstrated in the RP's GDA submissions.

3.6.3 INTEGRATION WITH OTHER TOPIC AREAS

199. The electrical distribution system provides support to safety systems across a number of topic areas. There will be a requirement for coordination across various topic areas to consider the adequacy of the design integration.

200. The following interactions should normally be considered during the electrical engineering assessment:

- Fault studies – Interactions are required to consider the safety claims made on the electrical distribution system.
- C&I – Interactions are required to consider control interfaces with the C&I system and smart device qualification requirements.
- Fault studies/C&I – Interactions to consider substantiation by the RP of the impact of the grid code requirements on the reactor operation and fault response.
- Mechanical engineering – Interactions are required to consider integration of design features for main and standby generators.
- Probabilistic safety assessment (PSA) – Interactions are required from the PSA assessment to confirm the capability of the electrical system design to support safety systems in meeting risk targets.
- Internal hazards – Interactions to consider the internal hazards assessment of layouts of electrical equipment and cable routes. This will include identification of fire risks.
- External hazards – Interactions to consider the hazards to electrical equipment from lightning and geomagnetically induced currents (GIC).
- Human factors – Interactions to consider the maintenance and operability of the electrical distribution system.

3.6.4 LESSONS LEARNED

201. Significant lessons learned from previous GDA assessments in the electrical engineering area are as follows:

- The RP should fully understand the expectation for substantiation of the safety role of the electrical distribution system in a claims, arguments and evidence format to support the safety case head document. As the role of the electrical power distribution system is to support safety systems the claims on the electrical system should be established from the claims on the supported safety systems which should primarily be derived from the fault schedule. Claims should also be established for the capability of the electrical distribution system to withstand disturbances such as lightning strikes, loss of grid and electrical faults with no adverse impact on its capability to support the safety systems.
- The RP should fully understand the requirements for meeting the requirements of the UK Grid Code in order to establish a grid connection agreement. Grid Code requirements are generally for generators to remain connected during grid disturbances in order to support the grid and it is not acceptable for plants to be shut down in order to protect the plant. Full Grid Code compliance is the expectation for connection to the UK National Electricity Transmission System with any non-compliances requiring derogations from the UK electricity regulator (Ofgem). Derogation requests will generally require a supporting ALARP presentation.
- ONR requires the development of a comprehensive computer based model of the electrical system in order to verify the capability of the system to support plant loads and to withstand a range of plant disturbances. Development should start at an early stage of the GDA process. A range of studies should be performed in line with IEC 62855. The GDA model can be based on existing

designs but ONR expects the capability of the design to be demonstrated in all cases.

- In demonstrating the integrity of the electrical system design particularly with regard to resilience to common cause failure the RP needs to take account of maintenance requirements. This should address under what operating conditions maintenance can be performed and definition of conditions for taking equipment out of service in order to perform maintenance activities. It is important that there is a clear distinction between maintenance surveillance activities and maintenance activities which require equipment to be taken out of service.
- The RP should define where smart devices are to be used in the electrical system and should define its approach to protect against the risk of common cause failure where smart devices are implemented. Where a claim is made that analogue technology will be used then the availability of such technology for long term applications should be substantiated.
- The GDA assessment should be based on a generic design. Site-specific design features should not be taken into account.

3.6.5 REFERENCES

- IAEA Safety Guide SSG-34 – Design of electrical power systems for NPPs.
- IEC standards commonly used in ONR's EE assessment activities include but are not limited to:
- IEC 62855: Nuclear power plants – Electrical power systems – Electrical power systems analysis.

3.7 EXTERNAL HAZARDS

202. ONR's assessment of external hazards would typically include those natural or man-made hazards that originate externally to both the site and the process and over which the operator has little control. External hazards include earthquake, aircraft impact, extreme weather, and flooding, and the effects of climate change. Terrorist or other malicious acts are also assessed as external hazards in coordination with ONR security assessors.

203. The overall objective is to ensure that the effects of external hazards are minimised as adequate protection against them has been provided for in the design. This is in order to ensure that external hazards do not adversely affect the functionality or reliability of systems important to safety designed to perform essential safety functions, and that potential common cause effects of external hazards have been adequately addressed. Items important to safety (i.e. safety systems and safety related systems) should be either qualified to withstand the effects of external hazards or protected against the hazards, i.e. appropriate use of equipment qualification, redundancy, diversity, separation or segregation.

3.7.1 SCOPE FOR GDA

204. The list of external hazards to be screened for inclusion into GDA should be proposed by the RP. Prior to screening, the list would typically include the hazards listed in TAG 13, Table 2. This list is not exhaustive and other external hazards not included on this list may be identified as potential initiating events that could affect the design.

205. The RP then identifies and justifies the list of external hazards that will be within the scope of GDA on the basis of a screening process. The external hazards included within the GDA scope will depend on the design and the RP's judgement, but should include those external hazards that can be considered on a generic basis, are relevant to the GB context, and could have an effect on nuclear safety. The criteria used for

screening hazards into GDA or deferring them until site licensing are up to the RP. However the RP needs to present a robust screening process as part of GDA and be able to identify when each external hazard will be considered and in what level of detail. The hazards that are likely to be screened in to GDA will differ depending on the design-specific context but these will be divided into the following categories:

- Within scope of GDA.
- Site-specific but reassurance can be provided during GDA.
- Site-specific and only able to be treated as such in any detail.

206. The level of claims, arguments and evidence, the relevance of the GSE and the interaction with site characterisation differ among these groups.

207. It should also be borne in mind that climate change, while not an external hazard in and of itself, is likely to have an impact on a number of external hazards.

208. Once the RP has developed the list of external hazards to be included in the scope of GDA, the RP will then need to define a GSE value for that hazard, and consider the generic plant / SSC design features against external hazards defined in the GSE.

DOCUMENTS SUBMITTED

209. The RP's documentation should provide the safety case that identifies the external hazards requirements, and the design, construction and management approaches that demonstrate adequate protection against these hazards. Within its submissions, the RP will need to demonstrate that:

- The identification of external hazards has been thorough and complete.
- The screening of external hazards into GDA or into the site-specific phase has been performed in a logical and consistent manner.
- The selection and processing of source data has been performed in accordance with RGP and the application of climate change in external hazards submissions is adequate.
- Adequately conservative GSE values for the hazards that have been screened in to GDA have been defined. The conservatism should be commensurate with the intention that the GSE values will bound the site-specific values for a site in GB (significant reassessment and design changes may be needed prior to first nuclear safety concrete if insufficiently conservative GSE values are used).
- Reasonably foreseeable combinations of hazards have been considered.
- Adequate margins exist beyond the design basis to the point(s) where safety functions would no longer be achieved.
- The potential effects of external hazards on the generic design have been analysed.
- External hazards have been included in the fault schedule or within a hazard schedule (a compartment by compartment view of the threats and provided protection for hazards).
- The demonstration of safety margins against external hazards and the link to protection of SSCs are clearly documented.
- Due consideration has been given to lessons learned post-Fukushima applicable to the external hazards area, including the implications of the IAEA director general's report.
- Multidisciplinary issues identified in other discipline areas have been adequately considered.

KEY ASSESSMENT TOPICS AND SAMPLING AREAS

210. The inspector will decide the areas of design that ONR will sample. Sampling is done in a focused, targeted and structured manner with a view to revealing any topic-specific, or generic, weaknesses in the safety case. ONR will seek confidence that the design is in line with RGP and the risks to nuclear safety have been reduced ALARP.

211. Generally, within external hazards, an inspector will perform a detailed assessment of the screening process and analysis of the hazards retained within GDA, including combinations of hazards, and the way that external hazard definitions are input into DBA, interfacing with the fault studies discipline.

212. The inspector may adopt a sampling approach towards examining the linkages between external hazards and other disciplines by examining the way external hazards definitions are applied as loading functions within the Engineering topic areas. In this case, the sampling approach should be based on the importance of these loading functions, either due to their widespread use within the discipline or due to the importance of the system in terms of its overall contribution to core damage.

3.7.2 BASIS FOR DECISION

STANDARDS AND GUIDANCE

213. The standard and criteria normally adopted in an external hazards ONR assessment are:

214. SAPs - The specific EH SAPs are: EHA.1 to EHA.19, which cover the wide range of EHs and the tasks needed for their identification and analysis. There are a number of supporting and related SAPs, all of which are relevant to the analysis of EHs and some of which make explicit reference to EHs. These SAPs include the engineering key principles, safety classification and standards, fault analysis, civil engineering, safety case, layout, siting and reliability SAPs.

215. TAGs:

- NS-TAST-GD-013: External Hazards Revision 7.
- NS-TAST-GD-005 Guidance on the demonstration of ALARP Revision 8.
- NS-TAST-GD-051 The purpose, scope and content of safety cases Revision 4.

216. For IAEA guidance and standards and WENRA guidance, see the References section below.

CAPTURING ASSUMPTIONS

217. The RP should endure that there is a suitable mechanism to transfer the outputs from the GDA to any licensee choosing the reactor technology in question and developing a site-specific safety case. This should include arrangements for ensuring that safety claims and assumptions will be realised in the final as-built design, an arrangements for moving the safety case to the operating regime.

218. Within the external hazards topic stream, there are likely to be a large number of these safety case claims and assumptions that will need to be communicated to the future licensee so that they can be taken forward as part of the site-specific work. The RP therefore needs to put in place a systematic method of capturing these assumptions and a plan for their transmittal. The external hazards inspector will need to be satisfied that an effective process has been implemented and that relevant assumptions can be taken into account.

3.7.3 INTEGRATION WITH OTHER TOPIC AREAS

219. GDA requires the submission of an adequate, coherent and holistic generic safety case. Regulatory assessment of the external hazards cannot therefore be carried out in isolation, as there are often safety issues of a multi-topic or multidisciplinary nature. External hazards interact with a wide number of disciplines as it provides the required external hazards input (loadings) to other disciplines that must be taken into account in the design.

220. The following interactions are normally considered during the external hazards assessment:

- Fault studies - External hazards are potential fault initiators, and this needs to be considered as part of the fault studies discipline's assessment. However the completeness of the list of hazards considered by the RP and input into the DBA is considered as part of the external hazards assessment.
- PSA - The PSA inspectors consider the screening and prioritisation of external hazards as part of their review of the PSA. The external hazards inspector provides advice and guidance to the PSA team on external hazards matters.
- Internal hazards – Internal hazards inspectors provide input to and receives output from the hazard screening and hazard combinations aspects of the external hazards assessment. Collaboration is also required to ensure that measures taken to provide protection against internal hazards do not undermine protection against external hazards and vice versa.
- Other disciplines (including civil engineering, electrical engineering, C&I, mechanical engineering, severe accident analysis, human factors and security). External hazards load definitions are considered as part of the external hazards assessment. The ability of an SSC to deliver its safety functions during normal operations (including for shutdown), fault sequences and accident conditions (with adequate consideration of external hazards loads) is assessed by the relevant engineering specialisms.

3.7.4 LESSONS LEARNED

221. There have been three GDAs completed in GB, and as a result there are a number of lessons learned for new GDA inspectors and for the RPs:

222. Proposed GSE values may not be sufficiently conservative:

- The methodologies used to define the GSE values should be aligned with RGP.
- The values selected should be appropriate for the proposed reactor sites in GB.
- The values selected should be compared to those proposed during previous GDAs – any which are less conservative than those proposed by other vendors should be subjected to detailed examination and justification.

223. Specific external hazards that have required significant attention during previous GDAs are as follows:

- The High Air Temperature value is important for the design of HVAC systems. In previous GDAs it has been difficult for RPs to design these systems to meet the requirements of the high air temperature GSE value and this led to the requirement for design changes late in the process, including in the site-specific stage. This should be a topic for early review to ensure that the high air temperature value adopted is sufficiently conservative, taking climate change into account.
- RPs have proposed that external flooding should be screened out of GDA on the basis that the reactor will be built on a "dry site", i.e. that the platform height

will be above the level of the design basis flood. However, some of the proposed GB sites for new NPPs will not meet the “dry site” criteria, and in addition, the “dry site” refers only to the design basis and does not address beyond design basis flooding. Therefore it is important that the RP is able to present the plant’s robustness against water on the platform, including any assumptions and operator actions. This is independent of the assumption of a “dry site” or flood defences.

- RPs may propose to take a code-based approach to lightning protection – however, the application of the IEC 62305 code does not provide a GSE value that is likely to bound a design basis at a 10^{-4} /yr hazard level.

224. Caution should be applied if RPs propose to use site-specific values for a particular candidate site during GDA because:

- Site-specific values are unlikely to have undergone analysis and assessment to an adequate standard for a nuclear safety case by GDA stage. Therefore these values are subject to change.
- The use of site-specific values rather than generic values suitable for the GB context can lead to margins being eroded.
- The use of site-specific values undermines the generic nature of GDA, and this may lead to significant difficulties if the design is then proposed to be built on a subsequent site.

225. The RP should supply a BDB margin evaluation for external hazards for all SSCs involved with the management of control, cooling, containment and spent fuel during GDA.

226. There may be gaps /shortfalls in the design’s ability to meet the requirements of the GSE withstand values when it enters GDA. Early in the review, the RP should identify any aspects of the generic design that require modification to meet the requirements of the generic safety case and GSE and should propose a plan to ensure these gaps are addressed within GDA. In cases where GDA is being performed in parallel with site characterisation for a specific site, the GSE may need to be updated during the GDA process as external hazards and site characterisation develop.

227. It is often useful for ONR to discuss the following topics with the RP early in the review:

- The adequacy of the processes to develop and use the GSE, including how the GSE values will inform, and will reflect, design development (including design changes), the demonstration of ALARP and the process to capture and review assumptions (as it is likely that assumptions will become key issues to follow up after GDA). Establishing these processes early helps the RP to record evidence in an adequate way from the beginning, avoiding inefficiencies and iterations.
- The quality of the documentation and production of a documentation map / list of the references and submission dates. Documentation is often neglected. In some cases the RP may need to translate documents, document input decks, etc. which will need time to prepare. Identifying these early can help efficiency.
- The RP external hazards capability and capacity. The RP may sometimes benefit from acquiring additional support at early stages, if the RP is not sufficiently familiarised with the GB context and expectations and international good practice in external hazards. This will avoid inefficiencies and repetitions in any work that needs to be developed during GDA.

3.7.5 REFERENCES

- IAEA Safety Standards Series - Site Evaluation for Nuclear Installations – NSR-3
- IAEA Safety Standards Series – Volcanic Hazards in Site Evaluation for Nuclear Installations – Specific Safety Guide (SSG)- 21
- IAEA Safety Standards Series – Meteorological and Hydrological Hazards in Site Evaluation for Nuclear Installations – SSG-18
- IAEA Safety Standards Series – External Events Excluding Earthquakes in the Design of Nuclear Power Plants – NS-G-1.5
- IAEA Safety Standards Series - Seismic Design and Qualification of Nuclear Power Plants - NS-G-1.6
- IAEA Safety Standards Series - External Human Induced Events in Site Evaluation for Nuclear Power Plants – NS-G-3.1
- IAEA Safety Standards Series - Seismic Hazards in Site Evaluation for Nuclear Installations – SSG-9
- IAEA Safety Standards Series - Geotechnical Aspects of Site Evaluation and Foundations for Nuclear Power Plants – NS-G-3.6
- WENRA Report on Safety of new NPP (Nuclear Power Plant) designs

3.8 FAULT STUDIES

228. NPP safety cases need to consider the risks arising both from normal operation and from fault / accident conditions. Within ONR, the fault studies technical area takes a leading role in considering the latter. This is predominately through the assessment of a RP's deterministic analysis of design basis faults (as opposed to the probabilistic analysis considered by the PSA discipline). However, reflecting modern RGP, the fault studies scope also extends to the deterministic consideration of events outside design basis (i.e. Design Extension Conditions that do not result in significant fuel damage, also known as DEC-A events).

3.8.1 SCOPE FOR GDA

KEY ASSESSMENT TOPICS AND SAMPLING AREAS

229. Given the complexity of the analysis methods used and the significance of the results for demonstrating the safety of a NPP, the bulk of ONR's fault studies assessment attention will be on the reactor transient analyses provided by the RP for design basis faults. Typically, the RP's analysis in this area will be quite mature, using long-established methods, and already the subject of regulatory attention or licensing activities in other countries. ONR's fault studies assessment will therefore have many similarities in terms of scope and focus with US NRC's "Chapter 15" standard review plan for light water reactors (Ref FS.1).

230. However, it is important to note that the scope of ONR's fault studies assessment will be broader than this. Past-experience shows that many of the areas of challenge from ONR (and requirements for further work from the RP) will be away from the analysis methods for reactor faults at power and instead be on areas not considered in as much detail in submissions to other regulators. A prominent example of this in some of the previous GDAs has been a need to develop the design basis safety case for refuelling operations and the fuel route to the same standards and detail as the RP has initially supplied for the reactor.

IDENTIFICATION AND CATEGORISATION OF EVENTS

231. An early activity for ONR's fault studies assessment will be to understand what fault conditions and postulated initiating events have been considered in the RP's safety case.

232. In contrast to other regulatory bodies, ONR does not prescribe the list of postulated initiating events to be considered. However, ONR's SAPs (Ref. FS.2) do set expectations for the criteria to be used when selecting events (SAPs FA.2, FA.5 and FA.6).

233. Almost certainly, "classic" reactor faults such as Loss of Coolant Accidents (LOCAs), loss of feed faults, control rod withdrawal faults etc. will feature in any list presented by the RP. However, the basis for identifying and considering such faults is often historic or set by a standards body or an overseas nuclear regulator (such as Chapter 15 of Ref. FS.1). For GB, the completeness of the list of faults must be justified by the RP. The starting point can be a pre-existing list of faults, but it needs to be supplemented by e.g. comparison with the PSA, IAEA guidance, FMEA or HAZOP.

234. The list of faults should not be restricted to the reactor at power. Indeed, it should not be restricted to the reactor. Any events associated with facilities or activities within scope of GDA should be considered if they have the potential to result in a significant dose of radiation being received (see SAP FA.2). Examples of the types of faults which need to be identified and considered (perhaps for the first time) in the RP's safety case include:

- Faults associated with spurious C&I failures.
- Faults associated with failures in essential support systems (e.g. electrical systems, HVAC, instrument air, loss of the ultimate heat sink).
- Faults in all modes of reactor operation, including refuelling outages.
- Faults associated with the spent fuel pool and fuel route (including over-raise faults which may not have off-site consequences).
- Faults associated with any radioactive waste facilities or operations within the scope of GDA.
- Faults associated with an initiating event and failure of one or more safety measures.

235. With faults identified, some grouping and categorisation is to be expected to determine which events need to go forward for analysis. ONR has clear expectations for determining what faults should be considered within the design basis (SAPs FA.5, FA.6 and Numerical Target 4) but it is flexible on the terminology and categorisation that is used. ONR has considered submissions using a range of approaches, for example "anticipated operational occurrences", "design basis accidents", "frequent faults", "infrequent faults", "operational conditions I to IV", and "plant condition categories 1 to 4".

IDENTIFICATION OF DESIGN BASIS FAULT SEQUENCES

236. The role of DBA is to demonstrate that there is at least one effective measure that can provide a necessary safety function for an identified fault condition. To do this, a number of deterministic rules are followed to pessimise the fault sequence. This sometimes results in unrealistic assumptions or combinations of assumptions. However, by adopting this approach, there can be confidence that, regardless of how the reactor was operating before the fault occurred, or how severe the fault is (for example a small breach in a pipe or a complete guillotine break), the identified safety measures are correctly sized and will respond appropriately.

237. The specifics of how this is done can vary but there are some common practices:

- The reactor power is often pessimised to 102% of full power to account for measurement uncertainties.
- The coolant flow is assumed to be at its maximum or minimum value.
- A conservative decay heat curve is assumed.
- Operator actions are not assumed within the first 30 minutes of the fault sequence.
- Conservative assumptions are made for valve opening time, safety injection response, water levels, rod insertion times, availability of power from the grid, time for emergency generators to start etc.
- The worst conceivable single failure in the claimed safety systems is assumed.
- The correct performance of lower classification or non-safety related equipment should not be assumed unless this makes the transient more onerous.

238. Some RPs may start with analysis where the specifics of what should be assumed for a fault sequence has been prescribed by a regulator, notably LOCAs in the US which follow an “Appendix K” methodology (Ref. FS.3). This is acceptable but the RP will need to justify why they are appropriate for its GDA safety case.

239. ONR’s experience is that it is often of value to question the RP on the key assumptions used in the analysis, for example:

- Is it always bounding to assume the reactor is at full power?
- Is the assumed single failure within a safety system demonstrably the worst in all variations of the fault?
- In addition to a random single failure in the safety system, could there be consequential failures of safety systems (either complete or partial failures) as a result of the initiating event? Could there be pipe whip and / or steam damage to adjacent safety equipment if a steam line breaks? If a fault originates in a C&I system, can the same system be assumed to be available to protect against that fault?
- Could some safety equipment be unavailable due to maintenance? Even if planned maintenance is not permitted during reactor operation, if the fault occurred during shutdown would there be the same availability of safety equipment as is assumed in the at-power analysis?

DESIGN BASIS FAULT SEQUENCE ANALYSIS

240. Fundamental to reactor fault studies is the modelling of fault sequences with computer codes. The RP’s analysis will be subject to extensive consideration by ONR throughout the course of GDA however this should be in a phased manner. In the early interactions and stages of assessment, it will be important to establish confidence in the scope of the analysis and the standard assumptions made, before results for specific transients are interrogated or quality assurance records are explored in later stages.

241. The analysis provided by the RP needs to have clear safety objectives (in the GB regulatory regime, analysis is not performed just to meet an ONR requirement). It is important that these objectives are clearly stated in the submission. These objectives are likely to include:

- To demonstrate an understanding of how the reactor systems will perform during a fault condition.
- To demonstrate that all relevant safety criteria are met (e.g. adequate reactivity control, no fuel melt, over-pressure limits exceeded, etc.)
- To provide source term information for dose calculations.

- To demonstrate that key pieces of safety equipment are correctly sized / specified (or to provide minimum performance requirements for the safety equipment).
- To demonstrate that the set-points at which the C&I actuates safety equipment are adequate.
- To demonstrate that there is sufficient time for operators to take claimed actions.

242. There are two main types of computer models commonly used for DBA:

- Conservative, “limit of envelope” computer codes which can demonstrate that all safety criteria are met but do not necessarily predict every aspect of the plant response. These codes were often used historically when computing power was limited.
- More realistic “best estimate” codes which try to model all relevant phenomena but with appropriate (user defined) conservatisms and uncertainties allowed for in the parameters entered in the case-specific input files. With modern computing power, the use of these codes has become more practical.

243. In some regulatory regimes, the computer models used to license a reactor need to be formally approved. This is usually an onerous requirement for both the reactor designer and the regulator. As a result, it is often found that reactor designers continue to submit analyses with old (but approved) “limit of envelope” computer codes if they can demonstrate that all safety criteria are met. The designers only revert to more modern models where safety margins are challenged. In contrast, ONR does not formally approve the computer models used within a safety case and would not discourage the use of innovative, start-of-the-art computer models. However, that does not mean older, approved codes cannot be fit-for-purpose.

244. Regardless of whether the code is formally approved by another regulator, there must be documented evidence that the code is appropriate for the reactor design and the fault sequence it is being applied to. ONR will examine code verification and validation evidence in the later stages of GDA but the RP should commence GDA knowing it will need to provide this information.

245. ONR has accepted safety cases which make some use of so-called “best estimate plus uncertainty” approaches, where uncertainties are taken from appropriate probability distributions using Monte Carlo type methods. However, the level of justification needed to support such an approach can be difficult to provide unless it is backed by extensive and documented development work.

246. Unless the reactor design is particularly novel or unique, there are usually a number of alternative computer codes that can be used to model design basis faults, written and maintained by reputable international organisations. Therefore, it is an option open to ONR to undertake (via TSCs) independent confirmatory analysis of fault sequences using a different code. In the case of GDA, it is almost certain ONR will look to undertake some independent analysis and the RP should be prepared to support this by providing plant data, and then work with ONR and its contractors to understand the implications of the results. Previous experience shows that there can be a number of challenges to getting the necessary data for such independent analysis, and therefore it is recommended early consideration is given to resolving the following points:

- The RP needs reassurance that appropriate non-disclosure agreements are in place.
- Appropriate export agreements need to be established.
- Some required information may not be owned by the RP (for example fuel data).

- The RP has the design information it needs for its own conservative licensing computer models but it has not previously attempted to aggregate the more detailed information a realistic best-estimate code may need.
- The RP's data is in non-standard units.

247. ONR would not look to repeat every calculation undertaken by the RP; only a limited sample selected from those fault sequences with small safety margins or for which the timing or performance of a particular safety measure is crucial. It is likely that a realistic best estimate code would provide the most valuable insights into the limitations of the RP's analysis. However, given ONR's restricted analysis scope, it is very unlikely ONR will look to develop a complete system model capable of modelling all transients. A balance will need to be struck between investing in a model that is flexible enough to investigate future regulatory lines of enquiry while also avoiding developing capability that will never be used.

248. If the design employs novel features or makes strong claims on passive features which are difficult to test during the operational life of a facility, the RP should expect this to be an area for additional regulatory attention by ONR. Phenomena Identification and Ranking Table (PIRT) analysis to inform experimental test rig and detailed modelling (as set out in Ref. FS.4) illustrates one way evidence could be brought together to demonstrate adequacy.

249. For non-reactor faults (e.g. fuel route), complex thermal hydraulic analysis may not be necessary. However detailed shielding (in the case of over-raise faults) or radiological consequences (in the case of dropped loads) calculations will be central to the safety case. As with the reactor transient analysis, appropriate levels of conservatism should be identified and justified in the submissions and similar levels of verification, validation and quality assurance for the methods used should be demonstrated.

BEYOND DESIGN BASIS EVENTS

250. It is now RGP to identify events and sequences outside of the design basis for deterministic analysis. The objective of this type of analysis (DEC-A) is to demonstrate that core melt can be prevented with an adequate level of confidence using SSCs included within the scope of GDA.

251. IAEA guidance (Ref. FS.5) suggests three types of scenarios should be considered:

- Initiating events that could lead to situations beyond the capability of safety systems that are designed for design basis accidents. A typical example is multiple tube rupture beyond the design basis assumptions in a steam generator of a pressurized water reactor.
- Anticipated operational occurrences or frequent design basis accidents combined with multiple failures (e.g. common cause failures in redundant trains) that prevent the safety systems from performing their intended function to control the postulated initiating event. A typical example is a LOCA without actuation of the safety injection.
- Credible postulated initiating events involving multiple failures causing the loss of a safety system while this system is used to fulfil its function as part of normal operation. This applies to those designs that use, for example, the same system for heat removal both in accident conditions and during shutdown. The identification of these sequences should result from a systematic analysis of the effects on the plant of a total failure of any safety system used in normal operation.

252. The RP should therefore not limit itself to just identifying design basis events. Criteria will need to be established for what scenarios should be identified for DEC-A analysis.

A frequency cut-off is almost certainly going to be part of these criteria however it should not be the only consideration. One objective of the analysis is to show the effectiveness of SSCs included within nuclear plant design. Events and sequences should be chosen that allow the RP to demonstrate the full extent of the defence in depth and capability included in its design.

253. Once identified, these events and sequences need to be analysed with appropriate methods and compared against clearly identified acceptance criteria. By definition, if these scenarios are not within the design basis, the normal design basis rules and expectations applied by the RP and the regulator need not apply. It is reasonable to reduce some of the conservatism from that included in the DBA, for example, the assumptions single failure and decay heat uncertainty can be relaxed. However, only those systems that are that are unaffected by the initiating event and any consequential effects should be credited in analysis, and they need to be operable in the conditions experienced.

254. It should be noted that even before the recent introduction of DEC-A consideration by IAEA, it is long-established GB RGP to demonstrate diversity in safety measure provision for frequent faults (events with an initiating frequency more than 10^{-3} per year) as part of the design basis safety case. This approach is followed on all operating reactors and has been successfully demonstrated for all reactor designs going through the GDA process. This means ONR has a starting expectation that frequent faults occurring with a common cause failure of a claimed safety measure are considered by new RPs with conservative design basis techniques. One consequence of this approach is that it is GB RGP to consider some anticipated transients without scram (ATWS) faults within the design basis.

255. Adoption of this established GB approach for frequent faults can address some but not all of the international expectations for DEC-A analysis. The RP should still look to identify events and sequences outside of the design basis (even if the design basis is not restricted to single initiating events) to demonstrate the effectiveness of defence in depth SSCs in preventing core melt.

SAFETY CRITERIA AND RADIOLOGICAL CONSEQUENCES

256. SAP FA.7 (Ref. FS.2) sets an expectation that so far is reasonable practicable, analysis for all faults within design basis should show no loss of physical barriers, and no release of radioactivity. However, where this is not possible, Numerical Target 4 in the SAPs provides a basis for a graded approach being taken. For the more frequent events (typically with an initiating event frequency > 10^{-3} per year), it is expected that it will demonstrated with a high level of confidence that there will be no (or at least very limited) fuel damage or radiological releases. For less frequent (but likely more challenging) events, the requirements and analytical assumptions are often relaxed very slightly but compliance with appropriate acceptance criteria must still be demonstrated.

257. ONR's frequency-graded criteria set out in Numerical Target 4 for design basis faults are radiological. However for light water reactors there are some widely accepted design criteria such as limiting fuel temperature, limiting local powers, limiting oxidation, and avoiding departures from nucleate boiling. ONR's technology neutral SAPs do not prescribe what these criteria and values should be so the RP will need to identify and justify them in its safety case.

258. To allow ONR to reach regulatory judgements against the expectations set out in the SAPs, the RP will need to supplement demonstrations against technical or design criteria with evaluations of the radiological consequences for fault sequences. It is not necessary for the RP to undertake and present uninformative and trivial radiological

consequences analysis for every considered fault if transient analysis has shown that established design acceptance criteria have been met. However, if such criteria cannot be met, or fuel damage does occur, or there is a release to the environment, dose analysis should be undertaken and comparisons made against dose targets. The dose targets need to be identified and justified in the RP's safety case, so as to support the claims and arguments it is making.

259. The regulations or expectations which set limits on the doses received by workers or members of the public vary from country to country. The assumptions which go into the specified limits can also change from country to country (e.g. distance from the site assumed, weather conditions, etc.) and therefore the methods used to estimate the radiological consequences from faults often have to be regime specific to be consistent with the limits. Therefore, to allow ONR inspectors to make their judgements on adequacy, the RP's analysis methods and targets should be consistent with Numerical Target 4 set out in the SAPs. This may require a modification to an overseas-based RP's methods or limits from what it has applied elsewhere.

260. The RP will also need to define appropriate acceptance criteria for DEC-A analysis. The objectives of these criteria will be to give confidence that credited SSCs are effective in preventing core damage. In practice, they may be relaxed relative to design basis limits, such that some fuel damage is permissible. Alternatively, they may be identical to the criteria applied for design basis faults, but demonstrated with less conservative analysis.

261. It should be noted that ONR's Numerical Target 4 does not directly apply to DEC-A events. Targets 6 and 8 can provide ONR inspectors with some context to judge whether the predicted consequences for the considered sequences are acceptable, or whether further regulatory attention is required.

CATEGORISATION OF SAFETY FUNCTIONS AND CLASSIFICATION OF SSCs

262. ONR's fault studies assessment should take an early and leading role in the wider GDA consideration of the adequacy of the RP's approach to categorisation and classification. This follows from the need for fault studies to consider the list of initiating events to be protected against, and the redundancy / diversity requirements of the SSCs delivering safety functions. The RP's DBA is likely to be the main way the sizing and redundancy requirements of higher classified engineered SSCs will be established.

263. All the safety functions required to take a facility or activity to a safe stable state should be identified and categorised. It is normal to break these safety functions down into further sub-functions. Different sub-functions can be categorised differently, for example control of reactivity in normal operations would be expected to have a different safety categorisation to the need to scram the reactor in a fault condition.

264. It is also normal to apply different classifications to the different SSCs delivering the same safety function. For example, the principal means of providing safety injection to the reactor is likely to have a higher classification to the secondary or tertiary means, even though they are delivering the same safety function.

265. The approach should not only apply to SSCs delivering safety functions after a design basis fault, but also to SSCs whose failure could cause an initiating event, and to SSCs which respond to DEC-A (and DEC-B severe accident) events.

266. Some RPs have introduced a concept of a controlled state and safe shutdown state into their approach to categorisation and classification. This has been judged to be acceptable but consideration does need to be given to how such an approach is

applied to facilities and activities away from the reactor for which the definition of a controlled and safe shutdown state may not directly apply.

LIMITS AND CONDITIONS ARISING FROM FAULT ANALYSIS

267. A NPP can only be considered safe if it is built and operated in a manner which is consistent with the fault analysis. For example:

- A pump or heat exchanger can achieve the performance requirements assumed in the analysis.
- A pump or heat exchanger can achieve the necessary reliability and availability requirements assumed in the analysis.
- The reactor will be tripped and safety injection started consistent with the requirements assumed in the analysis.
- The reactor is operating at the power level (or within the band) assumed in the analysis.

268. Although the outcome of GDA is not an operational safety case, it is important that limits and conditions resulting from the RP's fault studies work are clearly identified and traceable. It could be several years before detailed design work or procurement activities are undertaken, and the reactor will then be operated for several decades. It is therefore vital that the reasons for design decisions and analysis assumptions are clearly documented, and that any resulting constraints on operation or maintenance are highlighted so that they can be respected when the plant is being built and operated.

ALARP FOR FAULT STUDIES

269. Undertaking conservative DBA, following well established deterministic rules and showing compliance with widely recognised acceptance criteria should be the solid foundations for the ALARP arguments put forward by the RP. The demonstration of defence in depth and resilience by showing the presence and effectiveness of safety measures for DEC-A events can further strengthen the RP's arguments that it would be grossly disproportionate to do more to protect against a particular fault or scenario.

270. Where the application of ALARP in the GB regulatory framework results in a divergence from common international practice is that simply meeting acceptance criteria or limits with analysis is not enough. The RP should demonstrably question itself on whether (for example) increasing the capacity of a safety injection system, the redundancy of injection lines, the automation of manual actions etc. is reasonably practicable and could improve safety even if the extant design meets widely accepted deterministic rules.

271. The other side of the ALARP approach is that blind compliance with all deterministic rules is not always essential. The RP may be able to argue that exceptions to its usual rules on (for example) automatic actions or single failure tolerance are permissible because it is not reasonably practicable to follow them. These exceptions will need to be justified with appropriate levels of detail and substantiation commensurate to the safety significance.

272. The results of fault studies analysis can also be very important for providing context for ALARP arguments in other topic areas. For example, whether it is reasonably practicable to add additional pipe restraints or barriers to protect against a damaged steam line interacting with adjacent lines will be informed analysis showing the consequences of multiple line breaks.

DOCUMENTATION SUBMITTED

273. ONR is not prescriptive about how the fault studies aspects of the safety case are presented, for example whether they are reported in length in a safety case head document or the detail is provided in lower level topic reports. However, ONR's expectations are broadly consistent with those other regulators, such as those set out for "Chapter 15" of Ref. FS.1 or the section on safety analyses set out in IAEA's "Format and Content of the Safety Analysis Report for Nuclear Power Plants, GS-G-4.1 (Ref. FS.6).

274. The biggest changes relative to submissions provided to other regulators are likely to be:

- ONR considers the safety case to be totality of documentation developed to demonstrate the safety of a facility. Therefore, there should be a clear audit trail (albeit potentially through several levels of documentation) from the top level summary of the safety analyses to the individual FMEA work/calculations/computer model runs which generated or informed the analyses results.
- The RP needs to explain and justify the scope of its safety case and analyses included in the documentation. It cannot simply be that the scope has been set by what (for example) the US Standard Review Plan (Ref. FS.1) requires.
- The RP needs to justify why acceptance criteria are appropriate and what can concluded about the safety of the plant by the analysis showing a margin to the identified criteria. The stated conclusion cannot be restricted to the regulatory requirements in the country of origin have been met.
- Appropriate discussion needs to be provided on whether risks have been reduced ALARP.

3.8.2 BASIS FOR DECISION

275. Given that fault studies is primarily associated with deterministic analysis showing that appropriate acceptance criteria and limits have been met by a design, the basis for a positive regulatory decision on the adequacy of the reactor design should follow logically from the results of the RP's own analysis. However, at the end of GDA, ONR will need to have confidence in:

- The scope and completeness of the safety case (and associated analysis) produced by the RP.
- The adequacy of the analysis methods used to model complex phenomena, including the adequacy of the validation and quality assurance.
- The adequacy with which the fault studies safety case and supporting analysis is documented.
- The links between the fault studies portion of the safety case and engineering aspects, such that origins of assumptions and design requirements are traceable (in both directions).
- How the results of analysis and compliance with established deterministic rules have been used to show the risks have been reduced to ALARP and to argue that it would be grossly disproportionate to provide additional design provision for fault conditions.

STANDARDS AND GUIDANCE

276. A wide range of SAPs (Ref. FS.2) will inform any fault studies assessment of NPP but there are a sub-set which will be central to the interactions between ONR and the RP:

- The Fault Analysis (FA) series.

- The Fault Analysis series on assurance of validity of data and models (AV).
- The Engineering Key Principles (EKP) series.
- The Engineering safety classification and standard (ECS) series.
- The Engineering design for reliability (EDR) series.
- The numerical targets, notably Numerical Target 4.

277. Similarly, several TAGs are likely to inform ONR's fault studies assessment, but notable amongst them are likely to be:

- NS-TAST-GD-005 "Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable)" (Ref. FS.7)
- NS-TAST-GD-034 "Transient Analysis for DBAs in Nuclear Reactors" (Ref. FS.8)
- NS-TAST-GD-035 "Limits And Conditions For Nuclear Safety (Operating Rules)" (Ref. FS.9)
- NS-TAST-GD-042 "Validation of Computer Codes and Calculation Methods" (Ref. FS.10)
- NS-TAST-GD-094 "Categorisation of Safety Functions and Classification of Structures, Systems and Components" (Ref. FS.11).

278. ONR's expectations in fault studies are founded on post-Fukushima international guidance for deterministic analysis:

- IAEA: Safety of Nuclear Power Plants: Design, SSR-2/1 (Rev. 1) (Ref. FS.12)
- IAEA: Deterministic Safety Analysis for Nuclear Power Plants SSG-2 (Ref. FS.5)
- IAEA: Format and Content of the Safety Analysis Report for Nuclear Power Plants, GS-G-4.1 (Ref. FS.6)
- WENRA Reactor Harmonisation Working Group: Safety of new NPP designs, March 2013 (Ref. FS.13)

279. In the case of light water reactors, many expectations for analysis, acceptance criteria and RGP for code validation can be found in US NRC requirements Refs FS.3 and FS.4. It is crucial to appreciate that these US requirements are not part of the GB regulatory framework and do not automatically apply. It is for the RP to explain why they represent RGP and there may be parts which are not consistent with GB RGP or evolving IAEA guidance.

280. RPs may also cite requirements, regulations or guidance from other organisations, countries and standards bodies. As is the case with US NRC guidance, ONR is open to accepting this relevant and applicable good practice for a particular design or technology, but it needs clearly identified, explained and justified.

3.8.3 INTEGRATION WITH OTHER TECHNICAL ASSESSMENT TOPICS

281. The nature of fault studies is that it interfaces with almost all technical areas, and it plays a central role in integrating other topics together. This equally applies for the RP, the safety case produced by the RP, and ONR's internal interactions during GDA.

282. There are some closely related topic areas with some clear interactions:

- The PSA topic area will be looking at many of the same fault conditions from a probabilistic perspective, complementing the deterministic view taken in fault studies. Close working (within both the RP and ONR) can be valuable for considering the completeness of the list of initiating events and attributing appropriate initiating event frequencies. ONR's fault studies team may be able to provide advice to PSA colleagues on the adequacy of transient analysis

(including the adequacy of methods and code verification/validation) used to determine success criteria.

- The fuel topic area will be looking at fuel acceptance criteria to be complied within the fault studies safety case (note, other acceptance criteria such as containment design temperature and pressure will come from other topic areas). The fuel topic area will also have an overlapping interest in the core designs / burn ups assumed in transient analysis, and the adequacy of reactivity insertion safety case arguments. Reactivity control in the reactor is also a multidisciplinary matter between the fuel and core and fault studies disciplines.
- If the fault studies topic area includes DEC-A events as well as design basis events, then this leads to an interface with analysis of DEC-B events undertaken in the severe accident topic area.

283. From experience, examples of interactions with other topic areas include:

- Civil engineering on the adequacy of containment and spent fuel pool designs.
- Structural integrity on reactor pressure vessel (RPV), steam line and safety relief valve (SRV) body failures, with transient analysis informing the safety classification required by components.
- Internal hazards on the consequential effects of missiles, pipe whip and jet impingement informing the size of initiating events considered in the fault studies. The other side of this interaction is fault studies analysis of events informing the safety classification requirement of barriers or restraints.
- C&I on the parameters and actuations required of the different protection systems, and the potential for control and protection systems to initiate events.
- Electrical engineering on loss of grid and loss of onsite power faults, and the potential for grid frequency variations to impact the reactor.
- Mechanical engineering on dropped loads and associated protection, notably on fuel route.
- Human factors on operator responses and requirements (control room and elsewhere).
- External hazards as potential fault initiators and the availability of SSCs to respond in the conditions experienced as a consequence of the initiating event.

284. Other examples of disciplines fault studies may interact with include: chemistry, radiological protection and security.

3.8.4 LESSONS LEARNED

285. GDAs have been completed on three different reactor designs. Each of these resulted in areas of learning, sometimes common to all of them, in other cases limited to the particular technology involved or the regulatory regime in which the design was developed. From a fault studies perspective, the following have been identified as being potentially relevant for future GDAs:

- Early discussions on a categorisation and classification should be held. These discussions should of course start by considering design basis reactor faults. However, the RP should consider the logical outcomes of its approach when applied to DEC-A/DEC-B events/provisions, fuel route and radwaste facilities. It is important to be able differentiate between safety function, safety classification, and any graded requirements of design codes (e.g. ASME) as they all may use similar terminology.
- Experience shows it is possible to successfully move from a two-tier US-style approach to classification (safety related and non-safety related) to a three-tier approach as set out in the SAPs and IAEA guidance, without radically changing the design. However, this cannot be done by a simple mapping process at the

component level. The transition needs to be done fully cognisant of what the safety case is arguing.

- Early discussions in GDA should be able to establish gaps in the RP's analysis and safety case, for example:
  - consideration of all operating modes
  - consideration of spurious C&I and essential support system failures
  - consideration of fuel route and radwaste facilities
- Gaps in the fault schedule and safety case do not necessarily require additional transient analysis. The list of events to be considered in the fault studies safety case does not automatically equate to the list of events to be modelled. It may be possible to determine the SSC availability requirements, operator actions, etc. for faults in shutdown modes without repeating bounding analysis undertaken for a reactor at power to show that acceptance criteria are met.

3.8.5 REFERENCES

- FS.1 US NRC, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition (NUREG-0800)
- FS.2 ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition, Revision 0
- FS.3 US NRC, Appendix K to 10 CFR Part 50—ECCS Evaluation Models
- FS.4 US NRC, US NRC Regulatory Guide 1.203 "Transient and accident analysis methods"
- FS.5 IAEA, Deterministic Safety Analysis for Nuclear Power Plants SSG-2, 2009 (expected to be superseded by a revised version in 2019)
- FS.6 IAEA, Format and Content of the Safety Analysis Report for Nuclear Power Plants, GS-G-4.1 (expected to be superseded by a revised version in 2019)
- FS.7 ONR, NS-TAST-GD-005 "Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable)"
- FS.8 ONR, NS-TAST-GD-034 "Transient Analysis for DBAs in Nuclear Reactors"
- FS.9 ONR, NS-TAST-GD-035 "Limits And Conditions For Nuclear Safety (Operating Rules)"
- FS.10 ONR, NS-TAST-GD-042 "Validation of Computer Codes and Calculation Methods"
- FS.11 ONR, NS-TAST-GD-094 "Categorisation of Safety Functions and Classification of Structures, Systems and Components"
- FS.12 IAEA, Safety of Nuclear Power Plants: Design, SSR-2/1 (Rev. 1)
- FS.13 WENRA Reactor Harmonisation Working Group, Safety of new NPP designs, March 2013

3.9 FUEL AND CORE

286. Within the topic of fuel and core (FC), ONR would typically look at the performance of the reactor fuel and in-core components under a wide range of in-reactor and storage conditions, both in normal operation and in fault conditions. The intention is to demonstrate that with the installed protection and monitoring, the fuel and core system will continue to perform its safety functions under anticipated conditions.

3.9.1 SCOPE FOR GDA

DOCUMENTS SUBMITTED

287. The starting point for the RP's submission is a clear definition of the safety functions of the fuel and core components and the functional requirements that need to be met in normal operation and fault conditions. This is particularly true for in-core monitoring;

neutron sources; shutdown and hold-down systems, but clarity is also important for the fuel system throughout its life (until disposal).

288. The next step in a systematic design process is for the RP to develop design criteria which need to be met in order to ensure that the functional requirements are met under postulated operating conditions (including faults). The basis of these criteria needs to be a systematic consideration of the degradation mechanisms which potentially apply and the conditions which limit these degradation mechanisms to acceptable levels. These conditions are intended to be used as success criteria in the fault analysis; as part of a demonstration of fault tolerance. The criteria need to be evidence based and in general are empirical in nature. The evidence needs to be made available.

289. In collaboration with the fault studies topic area, a set of operating rules and surveillance requirements need to be defined by the RP to ensure that anticipated fault transients are likely to respect the boundaries imposed by the design criteria. Generally this involves modelling the fuel and core response to transients and providing fault analysis with fuel and nuclear performance data which can be applied to the calculation of specific fault sequences.

290. The set of functional requirements and design criteria are typically described in a topical report in a narrative form; which provides sufficient discussion to ensure that the users of the criteria understand their basis and apply them correctly. Such reports will need to reference and interpret source data (which is used to substantiate the criteria and demonstrate that they are suitably conservative).

291. Proposed operating rules should also be provided with adequate discussion and where appropriate, there should be sufficient clarity provided on how these are likely to be reflected in Technical Specifications and/or Station Operating Instructions (see TAG NS-TAST-GD-035).

292. The substantiation of the core performance inevitably involves the use of fuel and core mathematical models. The RP will need to supply evidence of the validation of these models by comparison against separate effects tests and integral tests to demonstrate that the model adequately represents the physical processes and the plant respectively. This topic area will examine the strength of the arguments presented and the evidence for the levels of uncertainty assumed when establishing an estimate of the safety margin present under anticipated operating conditions.

SAMPLING AREAS

293. Much of the basis for assessment is set out in TAG NS-TAST-GD-075. The relevant inspector will decide the areas of design that ONR will sample.

294. In the review of the substantiation of the core performance, the relevant inspector will apply a graded approach based on safety significance and novelty of the arguments.

3.9.2 BASIS FOR DECISION

295. ONR recognises that the design of fuel assemblies routinely offered by fuel manufactures can change in the interval between applying for a GDA and fabrication of the fuel assemblies. However, the design of other plant items depends on the fuel assembly performance too much to allow a GDA based on a loosely defined concept design. Any potential problems with a fuel assembly design need to be identified at an early stage and resolved. It is therefore necessary for GDA to assess a detailed reference design. (A subsequent nuclear site license holder can then modify the design in accordance with their own arrangements and we would assess the change to determine whether risk remains adequately controlled).

296. ONR would expect that fuel cladding failure can be prevented in normal operation and frequent faults (initiating event frequencies > 10^{-3} per year) to a high confidence level. In design basis faults, the core structural integrity should remain intact, with the cladding also intact as far as reasonably practical. Typically, where core design and operating limits can reasonably be set to avoid fuel damage, this should be done. The RP should demonstrate this for a reference first and equilibrium core loading pattern.

297. In the case of the interim spent fuel storage design, ONR expects that in normal operation there are two barriers to the release and dispersal of radioactivity. It is necessary to substantiate design criteria for interim storage and to provide credible design calculations and arguments to demonstrate that sufficient spent fuel pool storage is available to safety operate the plant, but ONR will not expect detailed design of an interim spent fuel facility during GDA provided that no potentially ALARP design option is unreasonably foreclosed.

STANDARDS AND GUIDANCE

298. The standard and criteria normally adopted in any ONR assessment are:

- SAPs EKP.1 to EKP.4, ERC.1 to ERC.4, FA.4 to FA.9 and AV.1 to AV.7.
- NS-TAST-GD-005, ALARP.
- NS-TAST-GD-075, Safety Aspects Specific To Nuclear Fuel In Power Reactors.
- NS-TAST-GD-042, Validation of Computer Codes and Calculation Methods.
- NS-TAST-GD-081, Safety Aspects Specific to Storage of Spent Nuclear Fuel.
- NS-TAST-GD-041, Criticality Safety.
- NS-TAST-GD-035, Limits and Conditions for Nuclear Safety (Operating Rules).

299. For additional information please see the references section below.

3.9.3 INTEGRATION WITH OTHER TECHNICAL ASSESSMENT TOPICS

300. Since the fuel cladding provides the primary confinement for fission products, the fuel topic area interacts extensively with other topic areas.

301. The design criteria are used as part of fault analysis to demonstrate adequate fault tolerance and the fault analysis feeds back influences the operating rules and potentially on the fuel Design Criteria themselves.

302. Reactivity control in the reactor is a multidisciplinary matter between the fuel and core and fault studies disciplines.

303. The modelling used in the fault analysis is usually based on condensed forms of more detailed models employed in the fuel and core area. The interface is often based on decoupling criteria such as: core radial form factors; Doppler power defect; and moderator density coefficients. In order to limit the scope of the fault analysis, these will typically be set to bounding values. However, if it is not possible to substantiate adequate operating margin, it may be necessary to revise the values of the decoupling parameters and make more specific arguments.

304. In some cases, it may be necessary to apply detailed fuel and core models in the fault analysis and this will require collaboration as part of the assessment of code validation.

305. The need for design criteria and decoupling parameters applies also to the modelling of fuel performance in the fuel route.

306. A number of fuel degradation mechanisms relate to corrosion of fuel and core components; particularly stress-corrosion cracking and crud-induced corrosion. Two key parameters are pH and boiling duty. Adequate control of crud involved collaboration between fuel and chemistry (as does the management of failed fuel).

307. There are potential hazards associated with fuel handling and loading. These hazards are at least in part managed by procedural control and this needs collaboration with human factors specialists.

308. Severe accident analysis may also interact with fuel and core, to understand how the fuel fails in a severe accident.

3.9.4 LESSONS LEARNED

309. In many regulatory regimes, Design Criteria are for fuel and core are defined by the regulatory body and therefore detailed analysis of the performance envelope of the fuel will be outside the experience of the RP. The criteria are often based on analysis carried out for legacy fuel types and may not reflect the current state of knowledge. The substantiation of the fuel criteria may therefore require a significant amount of effort and should be reviewed early in the GDA process.

310. An illustration of a potential problem is criteria relating to clad stress: It is well established that the 0.2% strain yield criterion is not actually protective, but it remains established in some regulatory regimes on the basis that there is sufficient conservatism in the assessment method to compensate for the inadequate criterion. This approach is generally difficult to accept and IAEA advise that the design criterion should be based of fuel pin ramp tests. ONR's expectation is a demonstration that the fuel cladding is adequately protected against failure as far as reasonably practical; and especially in frequent faults.

311. In the area of core monitoring, there has been a trend towards intelligent core monitoring. Some reactor designs have made use of their digital protection system to monitor or the safety margins available; based on a combination of in-core instrument data and complex core-follow calculations. These systems provide high-fidelity, low-reliability data. ONR's experience is that such systems can be very useful to the operator, but are likely to include latent errors; so that there is a significant risk that operators may be misled. The use of such systems should be in the context of a system of safety function categories and system classification. This often means making a systematic study of the potential failure modes and effects; with the aim of reducing the impact of system failures as far as is reasonable.

3.9.5 REFERENCES

312. ONR's TAG documents listed in the standards and guidance section above are intended to provide guidance on GB practice and international standards (found in IAEA and WENRA documents). However, in addition to these, useful material is found in:

- IAEA Safety Guide: Design of the Reactor Core for Nuclear Power Plants No. NS-G-1.12, Vienna, 2005

313. Specific example criteria for a PWR are found in:

- Règles de Conception et de Construction applicables aux Assemblages de Combustible des Centrales Nucléaires, RCC-C, 2017, http://www.afcen.com/en/publications/rcc-c

3.10 HUMAN FACTORS

314. Human Factors (HF) is the scientific study of human physical and psychological capabilities and limitations, and the application of that knowledge to the design of work systems. Within the nuclear context, HF is principally concerned with the human contribution to nuclear safety during facility design, construction, commissioning, operation, maintenance and decommissioning, including normal, fault and emergency conditions. However, it is also appropriate to consider HF where a conventional health and safety, or security, risk exists.

3.10.1 SCOPE FOR GDA

KEY ASSESSMENT TOPICS

315. In the area of HF, the purpose of the GDA of a new reactor is to assess whether the RP has taken a systematic approach to understanding the human contribution to safety. In doing so, it should have demonstrated the feasibility and acceptability of the Human Based Safety Claims (HBSCs) and that the human contribution to risk has been reduced as far as is reasonably practical.

316. The scope of work necessary to achieve this includes, but is not limited to, demonstrating suitability and sufficiency in the following areas:

- The RP's organisational HF capability.
- The applied codes, standards, methods and guidance.
- HF Integration (HFI) into all risk important areas, systems, structures and components.
- HF input into: design (including analysis and testing) build, operation, EIMT and decommissioning.
- The HFI programme.
- Consideration of operational experience and research.
- Human Reliability Analysis (HRA) (including all normal and fault states and demonstration of task feasibility).

317. ONR expects that assumptions, relating to the future operating organisation and to nuclear safety, are captured for adoption / validation by a future licensee (including ongoing activities). These assumptions do not need to be fully developed, however, there needs to be sufficient information for ONR to judge their credibility. In the area of HF, these include, but may not be limited to:

- Training.
- Procedures.
- Staffing numbers.
- Accident response.

318. ONR also expects that submissions present a coherent set of claims, arguments and evidence in relation to the topics above. Taken together, these systematically identify the operator contribution to safety and justify why the HF aspects of the design and safety case are adequately considered and the risks reduced to as low as is reasonably practical.

DOCUMENTS SUBMITTED

319. There are no prescribed submissions for HF and the number and level of detail in the documents submitted by the RP can vary. However, in determining how to structure the submission, ONR considers the following to be RGP:

- PCSR or equivalent safety case HF chapters (i.e. the safety case summary).
- A human factors integration plan (HFIP).
- HFI guidance documents for the project, e.g. HSI design, environmental design, and equipment design.
- Task and Error Analysis reports.
- Verification and Validation reports (Design Assessment Reports).
- Substantiation of HBSC reports.
- HRA reports – it is important to note that HRA and the substantiation of HBSCs are considered part of the same process by ONR.
- Fault schedules which specifically capture HBSCs.
- PSA reports, specifically capturing human errors and showing the human contribution to nuclear safety.
- HF Issues and Assumptions register.

SAMPLING AREAS

320. As ONR is a goal based sampling regulatory organisation, this means it may not assess every document submitted. The strategy for sampling HF during GDA is based on risk and establishing confidence that that suitable and sufficient HF integration has been achieved across the design.

321. Areas subject to regulatory sampling include those arrangements necessary to deliver HFI, and specific submissions, which provide evidence that HFI has been adequately achieved.

322. The assessment of arrangements will include consideration of the suitability of the RP's HF organisation, HFI processes, and the HFI programme to appropriately influence the design and safety case considered in GDA. ONR will base its judgement on whether the RP has a sufficiently competent organisation, has established a suite of modern codes, methods, standards, and guidance, and developed a credible programme sufficient in scope and resource.

323. The assessment of the arrangements will be supplemented by the targeted assessment of specific submissions, which may include:

- The operating philosophy and approach to allocation of function.
- Guidance documents to inform the development of the design, for example, style and equipment design guides.
- Design aspects relating to a range of plant systems, structure, components and equipment to confirm that they have been designed in accordance with HF design principles.
- HRAs and their supporting analyses to gain confidence that the scope of risk important activities is understood, that they have been assessed to ensure that the design is suitably underpinned, and that risks have been reduced ALARP.
- The HF Issues and assumptions register to gain confidence that assumptions are being suitably captured and that issues are being appropriately managed and sentenced to ensure that the risk has been reduced ALARP.

324. The sampling strategy adopted by ONR will also give consideration to areas where the evidence base is weak, or where novel technologies could impact on human performance. ONR also expects to see evidence that operational experience has informed the design, and that where appropriate, experimental data is used to inform the application of new technologies.

325. ONR expects that where it is necessary to place a claim upon the human to perform a risk important activity, then the activity will be suitably assessed and optimised to ensure that the risk is reduced so far as is reasonably practicable.

3.10.2 BASIS FOR DECISION

STANDARDS AND GUIDANCE

326. ONR judgement and decision making is guided by a number of SAPs and TAGs. These summarise the regulatory expectations to be considered by inspectors during their assessment. In addition to the main HF SAPs, a number of others are judged to be of relevance to HF, therefore their expectations should be considered in a targeted and proportionate manner during the HF assessment and a judgement made of the extent to which the HF safety arguments and evidence demonstrate how the design meets the intent of these and that risk is being controlled to ALARP. Those SAPs relevant to HF are as follows:

327. SAPs: EHF 1-12, EKP.3 – 5, ERL 3, ELO.1, ESS. 3, ESS. 8 – 9, 11, 13, 15, 26, ESR. 1 – 2, 4, 7, ECV. 6 – 7, FA.5 – 6, 9 – 10, 13 – 14, 16, AV.3.

328. TAGs:

- NS-TAST-GD-058 Human Factors Integration.
- NS-TAST-GD-060 Procedure Design and Administrative Controls.
- NS-TAST-GD-061 Human Machine Interface.
- NS-TAST-GD-063 Human Reliability Analysis.
- NS-TAST-GD-064 Allocation of Function between Human and Engineered Systems.
- NS-TAST-GD-030 Probabilistic Safety Analysis.
- NS-TAST-GD-003 Safety Systems.
- NS-TAST-GD-051 Guidance on the Purpose, Scope and Content of Nuclear Safety Cases.
- NS-TAST-GD-005 ALARP.

3.10.3 INTEGRATION WITH OTHER TOPIC AREAS

329. As the HF discipline focusses on those areas where the human, by action or inaction, can affect the safety of the plant, it is multidisciplinary. ONR expects suitable integration with the following disciplines:

- Fault studies – Identification of Human Based Postulated Initiating Events; substantiation of design basis HBSCs.
- Internal hazards – Substantiation of HBSCs for Internal Hazard responses, evacuation.
- External hazards – Substantiation of HBSCs pertaining to site response and the design of equipment.
- Probabilistic safety analysis – Identification and modelling of HBSCs – considering: pre-initiator errors; initiator errors; post initiator errors (including omission, commission, and misdiagnosis).
- Severe accident analysis – Identification and substantiation of SAA response HBSCs.

330. In each of these areas, the RP's HF team should support in the identification, classification and substantiation (and quantification where relevant) of HBSCs to ensure a suitable and sufficient risk assessment.

331. The RP HF team should facilitate the integration of HF principles into the design of the plant to ensure that the human-system interactions are optimised. This can include design to support EIMT, reducing worker dose via task optimisation, and formal verification and validation activities to provide evidence that adequate HFI has been achieved and that the human-technology system is acceptably safe. Achieving this is

likely to require integration of HF with the engineering and scientific disciplines outlined below:

- C&I – Human factors integration into the design of Human Machine Interfaces – e.g. Hard-wired panels, screen based interfaces, design of RC&I cabinets to promote reliable EIMT.
- Electrical engineering – Human factors integration in the design of Electrical Systems and Components to promote reliable EIMT.
- Mechanical engineering – Human factors integration in the design of Mechanical systems and components to promote reliable EIMT.
- Structural integrity – Integration of human factors into the design of risk important SSCs, to ensure reliable EIMT activities.
- Civil engineering – Human factors integration into the constructability, accessibility for welding, inspect-ability, control of materials, behavioural safety.
- Chemistry – The identification and substantiation of HBSCs associated with chemistry sampling and testing.
- Nuclear liabilities – Human factors integration in the design of rad-waste processing and storage SSCs.
- Radiological protection – Substantiation of HBSCs, e.g. human performance whilst wearing PPE, design of tasks to minimise dose.

Other areas of HF integration can also include:

- Operational team – Task design support. Development of the concept and conduct of operations. Staffing levels.
- Security – Optimising the human safety and security responses where conflicts exist. Design support.
- Conventional and fire safety – Design support to hazard prevention / mitigation systems.
- Fuel and core – Integration of human factors into the task design and equipment relating to fuel handling and management. Identification and substantiation of HBSCs relating to this topic.
- Safeguards – Identification and substantiation of HBSCs relating to the control of nuclear material.

3.10.4 LESSONS LEARNED

332. To date, ONR has completed three GDAs of new reactor designs. As a result, there are a number of lessons learned which could benefit new RPs, which are summarised below. Key to these is developing an adequate understanding of the GB regulatory context and associated regulatory requirements. This is best achieved by early and regular engagement with ONR, and where necessary, the use of a SQEP supply chain familiar with GB regulatory requirements.

- Planning Lessons:

Quickly establish a credible HF work scope baselined against GB regulatory expectations and translate this into a detailed resource loaded programme with dependencies and the critical path identified.

- Organisational Lessons:

Ensure that adequate integration channels exist within the organisation between the HF and safety analysis and design disciplines and that sufficient expertise exists to service these areas. It is important to note that some areas may require specialist support not currently embedded within the RP organisation. Securing this additional

resource has the potential to delay GDA given the international shortage of specialist ergonomists.

- Analysis Lessons:

ONR expects that whichever HRA method is adopted, it is highly integrated with the qualitative HF analysis. The numbers derived using the HRA should be directly traceable back to the qualitative analysis, and should be informed by OPEX, or trials data. This can be particularly challenging as many international HRA methods do not require such a close coupling of the qualitative and quantitative assessments.

The scope of the HRA should be comprehensive and representative of the full range of HBSCs. ONR expects proportionate demonstration that:

- Type A, Type B, and Type C errors are modelled within the HRA.
- Dependency is formally assessed between human actions. For example, where the operator is the initiating event, any following human actions may be severely compromised.
- Violation potential is explicitly considered.
- Both commission and omission errors are explicitly considered.
- That misdiagnosis is considered with specific reference to the design and presentation of plant data.

There are no current HRA methods that are fully validated for modelling human-computer interaction. Given that the majority of modern reactor designs feature digital screen-based control rooms; this is a key challenge and an area of regulatory concern with respect to how these interactions are modelled within the PSA. To address this, it is important to give early consideration to HRA data on human-computer interaction; recognising how long it takes to develop proprietary methods or alternative data sources.

The scope and resource requirements for conducting verification and validation activities to substantiate elements of the design have sometimes been under-estimated. Early planning is essential to ensure that all necessary elements are identified, integrated and addressed through effective V&V activities and that they are delivered in a timely manner.

- Design Lessons

Ensure that a key focus of the early work is establishing a sound understanding of which areas of the design are important in HF terms and ensure that HF capability with experience of these areas is available.

3.10.5 REFERENCES

333. ONR has recently undertaken major HF assessments of the AP1000®, EPR™ and UK ABWR reactor designs. Key references are:

- UK ABWR GDA: Step 2 Assessment Report (http://www.onr.org.uk/new-reactors/uk-abwr/reports/step2/uk-abwr-human-factors-step-2-assessment-executive-summary.pdf)
- AP1000® GDA: Step 4 Assessment Report (http://www.onr.org.uk/new-reactors/reports/step-four/technical-assessment/ap1000-hf-onr-gda-ar-11-012-r-rev-0.pdf)

- EPRTM GDA: Step 4 Assessment Report (http://www.onr.org.uk/new-reactors/reports/step-four/technical-assessment/ukepr-hf-onr-gda-ar-11-028-r-rev-0.pdf)

334. IAEA Standards:

- SSR-2/1 - Safety of Nuclear Power Plant: Design Specific Requirements - Sets out international good practice expectations for the consideration of human factors in the design process and safety life-cycle.
- SSG-2 - Deterministic Safety Analysis for Nuclear Power Plant Specific Safety Guide - Sets out international good practice expectations for the consideration of human factors in the design process and safety life-cycle - Supports and informs assessment of the identification of HBSC / HF Engineering (HFE), supporting arguments and evidence.
- SSG-3 - Development and Application of Level 1 Probabilistic Safety Analysis for Nuclear Power Plant Specific Safety Guide - Supports and informs assessment of the identification of HBSC / HFE, supporting arguments and evidence.
- SSG-4 - Development and Application of Level 2 Probabilistic Safety Analysis for Nuclear Power Plant Specific Safety Guide - Supports and informs assessment of the identification of HBSC / HFE, supporting arguments and evidence.
- NS-G-1.3 - Instrumentation and Control Systems Important to Safety in Nuclear Power Plants. Safety Guidance - Sets out international good practice expectations for the consideration of human factors in the design process and safety life-cycle.
- NS-G-2.15 - Severe Accident Management Programmes for Nuclear Power Plants - Sets out international good practice expectations for severe accident management and response.

3.11 INTERNAL HAZARDS

335. In general, ONR defines internal hazards as 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. That is, the future licensee has control over the initiating event in some form. Internal hazards include fire and explosion, internal flooding, steam release, pipe whip and jet impact, internal missiles from failure of pressurised equipment or rotating machinery, toxic or corrosive gas releases, dropped loads, vehicle impacts, and electromagnetic interference.

336. Internal hazards have the potential to challenge the SSCs delivering Safety Functions (SFs) which prevent detrimental nuclear safety effects such as radiological releases. SSCs should be designed, manufactured, installed and maintained to deliver these functions reliably. For the most part, internal hazard challenges to SSCs are overcome in at an early stage in the design of plants by ensuring that redundant and/or diverse SSCs remain available to deliver the SFs. This is achieved, in order of preference, by providing physical segregation, separation and design for fail-safe operation under hazard conditions.

337. Internal hazards, whilst defined as those within the control of the future licensee, are highly dependent on early design choices. Designers should aim to deliver site and plant layouts that eliminate or minimise the potential from detrimental effects should hazards materialise. Inherently safe approaches such as eliminating or minimising hazardous materials, good engineering standards and design are all key goals which should be pursued and demonstrated early on in GDA.

3.11.1 SCOPE FOR GDA

338. It is expected that during GDA the RP will demonstrate that the risks to nuclear safety associate with internal hazards during normal operation and under potential faults and accident conditions (in the context of the facilities' generic engineering design and operational provisions) have been reduced to ALARP.

339. In order to achieve the above goal during GDA, it is considered essential that the RP will undertake a systematic identification of internal hazards and their combinations (as expected from SAP EHA. 1 and EHA. 14) focusing on those that may have hazardous consequences to the buildings and SSCs of nuclear safety significance. On this basis, key SSCs expected to form part of the scope of GDA are those delivering SFs such as reactivity control, cooling and containment.

340. It is also expected that, as part of GDA, the RP will characterise each relevant internal hazard using suitable tools and methods and that it will substantiate the generic design features ensuring the delivery of the SFs. For example, nuclear safety-significant barriers may be part of the design to provide segregation and ensuring availability of 'safety trains' (redundant safety systems delivering or contributing to the delivery of a nuclear safety function).

341. In an event sequence, internal hazards rarely occur in isolation from each other. For example, a full bore break in the primary circuit piping of a water-cooled reactor would result in a combination of hazards including steam release, pipe whip, jet impact and internal flooding materialising virtually simultaneously or in quick succession from each other. It is also an expectation of GDA that the design will be demonstrably resilient against combinations of hazards, and this includes combinations of internal and/or external hazards.

KEY CONSIDERATIONS AND DOCUMENTS SUBMITTED

342. The RP's documentation justifying that risks from internal hazards have been reduced to ALARP within GDA should include the following considerations:

- A comprehensive and systematic hazard identification process covering internal hazards which may challenge the facilities, considering those hazards individually and also in combination with consequential, concurrent or independent hazards and/or faults which may arise.
- The outcome of hazard characterisation exercises, using relevant methods and models.
- A demonstration of alignment with ONR expectations as outlined in the NS-TAST-GD-014: Internal Hazards (revision 5). These cover general and hazard-specific expectations on codes and standards, the use of analysis methods and computer codes, the type of failures and plant operational states assumed, hazard characterisation, cliff edge effects and treatment of uncertainty to cite some examples. For this demonstration, inspectors would expect:
  - Design codes and standards are relevant and applicable to the reactor technology and have been adequately interpreted and applied, and adequately validated and data verified.
  - A presentation of the unmitigated consequences from the materialisation of internal hazards and their combinations, and a demonstration that the severity of hazard consequences is used to define the appropriate design and engineering provisions.
  - Hazard characterisation considering plant operation in the worst credible operational state. For example, for systems which are not continuously energised or in use, failures should be postulated in the worst operational stage (mode of operation with the highest energy).

The worst operational state may also relate to the conditions of neighbouring plant or protective or of mitigative measures (e.g. maintenance or shutdown activities may require compartment isolations to be broken into and this may therefore provide pathways to hazard progression which would not be credible during other operational states).

- The assumptions made in hazard characterisation. Analyses should be performed to determine the sensitivity of the analytical results to the assumptions made. Analysis methods or computer programmes used for analysis should be shown to be adequate to characterise the hazards (including their combinations).
- Consideration of cliff-edge effects, where small but reasonable changes in the case (hazard source characteristics, state of plant or SSCs) would lead to more severe consequences.
- Demonstration that, for each internal hazard and in line with IAEA guidance, the design has followed the defence-in-depth approach. This involves, for each internal hazard that cannot be eliminated or prevented, that the severity is reduced e.g. by using more benign substances and operating conditions, lower temperature and pressures, minimum combustible or flooding inventories. It also involves for example providing evidence that the design safe envelope is supported by robust passive barriers designed to withstand the internal hazards loads so far as is reasonably practicable.

- Demonstration that SSCs with highest reliability claims are not challenged by internal hazards. This is an area which has led to some key lessons learned from earlier GDAs. These are items for which failure cannot be conceded in the design due to highly undesirable consequences and therefore require highly robust materials and care in the design, fabrication and inspection (to arguably deem that the failure frequency has been reduced to a very low value).
- Clarity in the consideration of interactions between internal hazards and other relevant disciplines, for example, fault studies, structural integrity, mechanical and civil engineering. A key consideration is, for example, that the engineering design of nuclear safety barriers delivering segregation of key SSCs meets the safety functional requirements placed on them by internal hazards.
- Confirmation that design selection processes to turn the generic design into a detail design will maintain the key features necessary for control of the effects of internal hazards.

343. The number and the level of detail in the documents submitted by the RP can vary. However, previous RP's have found useful to present the safety case following an approach based on claims, arguments and evidence.

344. Some examples of documentation submitted in previous GDAs include:

- The overarching internal hazards claims and arguments – this normally includes claims on SSCs that are applicable to all / each internal hazard.
- Generic site layout including plans and section drawings highlighting key systems (e.g. high energy systems, flammable inventories, toxic substance inventories) and key safety features and components e.g. segregation barriers, including their key functional requirements.
- 'Room data-sheets' documenting hazardous inventories, structures, systems and components that support the hazard identification and characterisation exercises.
- 'Safety-divisional' plans highlighting key segregation features ensuring delivery of SFs.

- Hazard-by-hazard analyses documenting the outcome of the hazard identification and characterisation exercises. These have been formally documented in topic reports for each individual internal hazard in turn.
- Substantiation reports documenting the resilience of claimed design features e.g. nuclear safety barriers, against each relevant internal hazard.
- A report documenting the outcome of the identification of hazard combinations (including internal and external hazards), the characterisation of hazard combinations and demonstrating resilience of the design against the combined loadings.
- Design reports, supporting calculations and technical drawings for nuclear safety structures. These documents will provide the evidence to substantiate the arguments.

SAMPLING AREAS

345. The relevant ONR inspector will decide the areas of design or substantiation that ONR will sample. This should be based on nuclear safety significance and stated in an assessment plan. ONR will seek confidence that the design is in line with RGP and the risks to nuclear safety have been reduced to ALARP levels. The following list provides a number of general areas that the internal hazards inspector will (normally) assess. The list is not meant to be exhaustive.

- Safety case claims made for each internal hazard in turn, and for combination of hazards.
- The completeness (extent, depth and quality) of hazard identification exercises, and justification for exclusions.
- The chosen internal hazards characterisation methodologies, verification and validation status of models, assumptions and sensitivities to gauge the design's safety margins.
- The substantiation of SSCs against internal hazards and their combinations. This includes confirmation that categorisation and classification of SSCs is consistent with the unmitigated consequences from the materialisation of hazards. Further information on Categorisation and Classification can be found in TAG NS-TAST-GD-094.

346. A specific area that the inspector will normally assess, and where there are GB-specific expectations, is the failure of high energy systems. Key points in this area are as follows:

- Inspectors expect that double ended guillotine failure (gross failure) is assumed for pipework, or other appropriate conservative assumption for other components.
- Leak-before-break is not generally accepted as the primary structural integrity safety claim. The expectation is that the safety case would demonstrate that the design can accommodate the consequences of gross failure, or otherwise that the pipework or components are of very high integrity.
- Inspectors also expect consequence analysis to consider failures in high energy modes of operation, including for systems which may only temporarily operate in high energy modes.
- Consideration of the combined loads in the substantiation of SSCs (to demonstrate that acceptable factors of safety or residual withstand capacity are provided by the design).

347. ONR expectations for each point above are discussed in the draft NS-TAST-GD-014: Internal Hazards (revision 5).

3.11.2 BASIS FOR DECISION

348. ONR is a sampling organisation with limited resources, therefore during GDA sampling is used to limit the areas scrutinised and to improve the overall efficiency of the assessment process.

349. The initial sampling strategy for assessment may consist of undertaking a “broad brush” review of all the documents provided by the RP and then to carry out a “deep dive” detailed technical assessment of the topics that are important to safety or less clearly explained.

STANDARDS AND GUIDANCE

350. The standard and criteria normally adopted in any ONR assessment are:

- SAPs: Key internal hazards SAPs are documented in the EHA series (Engineering principles: external and internal hazards). However, the SAPs are applied holistically. Other key SAPs of relevance to internal hazards assessment include the EKP (Engineering principles: key principles), ECS (Engineering principles: safety classification and standards) and FA (Fault analysis) series.
- TAGs:
  - NS-TAST-GD-014: Internal Hazards (Revision 5).
  - NS-TAST-GD-036. Diversity, Redundancy, Segregation and Layout of Mechanical Plant. Revision 3.
  - NS-TAST-GD-051. The Purpose, Scope and Content of Safety Cases. Revision 4.
  - NS-TAST-GD-094. Categorisation of Safety Functions and Classification of Structures, Systems and Components. Revision 0. November 2015.
  - NS-TAST-GD-005 Guidance on the Demonstration of ALARP Revision 8.
- For IAEA guidance and standards and WENRA guidance, see the References section below.

ASSESSMENT PROCESS

351. The guidance described above provides high level principles. The technical standards used to identify and characterise hazards and their combinations, and to substantiate SSCs against hazard loadings will be considered in the ONR GDA assessment. If those standards are already considered by ONR as RGP, ONR will then focus the assessment on the application of those standards. However, if the RP designs the SSCs with novel or “in-house” design codes (see lessons learned section) then, the RP will need to demonstrate that those technical standards provide a design outcome consistent with an approach using RGP.

3.11.3 INTEGRATION WITH OTHER TECHNICAL ASSESSMENT TOPICS

352. GDA requires the submission of an adequate, coherent and holistic generic safety case. The assessment of internal hazards cannot therefore be carried out in isolation, as internal hazard loadings challenge SSCs with obvious necessary interactions with engineering disciplines (such as civil and mechanical engineering, and structural integrity). Specifically, the following interactions are normally considered during GDA by internal hazards:

- Structural integrity is primarily related to the assessment of pressure part failure analyses the assumed failure locations and the potential effects of internal hazards on SSCs.
- Civil engineering - Internal hazards provides input to civil engineering as hazards loadings (fire, flooding, missile impacts) to be factored into the substantiation of structural barriers and the overall civil structures.
- External hazards - related to hazard combinations, which will include combinations of internal and external hazards.
- Conventional safety including fire safety – these interactions relate to reviewing the impact of hazardous substances and fire on personnel. There may be conflicting requirements e.g. provision of additional access/ egress routes to meet GB expectations for life safety, which may introduce further penetrations through nuclear safety-significant barriers.
- Fault studies (FS) – Interactions are required to ensure consistency between internal hazards and fault studies especially related to the indirect / dynamic effects on any credited SSCs.
- Probabilistic safety assessment (PSA) –consistency between the hazard identification and characterisation in both the probabilistic and deterministic assessments is required.
- C&I –This is related to the effects of potential hazards on vulnerable C&I systems, especially in locations such as the Main Control Room and/or alternative control locations. Full segregation between redundant safety systems may not be achievable at those locations, and continued operability may be needed to ensure nuclear safety.

353. Internal hazards may also interact with other disciplines, such as electrical engineering (e.g. layouts of electrical equipment and cable routes), human factors (e.g. on the feasibility of operator actions under hazard conditions), nuclear liabilities (e.g. protective barriers, segregation, separation and active protection systems to provide mitigation in the event of internal hazards) and security (e.g. in vital area identification studies).

3.11.4 LESSONS LEARNED

354. There have been three GDAs completed in GB and, as a result, there are a number of lessons learned to inform inspectors and RPs. Some of the lessons learned are generic and apply to more than a single hazard and discipline. Table 1 and the bullet points below provide a summary of key learning points. Further points are available in the assessment reports from previous GDAs and in ONR publications such as conference proceedings on internal fire and combination of hazards (see reference list):

- Challenges in hazard identification and characterisation:
  - Incomplete hazard identification and characterisation. For example, ONR has seen some combustible inventories excluded from assessment by implicitly claiming protection by cable coatings or wrapping. Initial analysis should be based on conservative assumptions of upper bounds of combustible inventories in specific locations. This allows controls and provision of sufficient margin to allow for design changes in the detailed design process. ONR regulatory expectations differ in certain areas (e.g. pressure part failure).
  - Selection of appropriate hazard characterisation methodologies and tools has been challenging for hazards such as pipe whip and jet impact, steam release and internal blast.

- The characterisation and presentation of the unmitigated consequences for internal hazards has proven challenging and so has the development of claims and the safety case for internal hazards inside containment.
- Modelling tools and models. A variety of tools have been used in the three GDA projects completed in GB so far. ONR does not prescribe tools or models and is up to the RPs to select models that are suitably validated for their intended use. This has on occasions proven difficult.
- Partial analysis / characterisation (e.g. room-by-room analyses) were not bounding of compartment-wide hazard effects on SSCs including barriers. Whilst quantitative analyses are generally expected for a safety case of a new nuclear plant, the level of information available and the timescales of GDA may direct RPs towards a reduction in scope. This may include selecting sets of representative scenarios for analysis, and then providing qualitative justification as to how SSCs elsewhere in the plant are substantiated by comparison to the quantified, representative case. Whilst this may be a sensible strategy and generally acceptable in GDA, the expectation is that bounding effects on SSCs are captured. The selection of bounding scenarios should follow a systematic approach and criteria, ensuring that there is coverage of the effects of all the variables that may influence the progression of the hazards.

- Substantiation. In past GDAs, ONR has seen that:

  - Evidence to support the substantiation of the generic design proved difficult to develop due to the level of design maturity and the need for hazard characterisation results. The expectation is that both global and local effects are analysed and therefore barrier substantiation challenged the latter stages of GDA.
  - Designs which credit leak-before-break or have not postulated failure in high energy modes of operation find meeting ONR's expectations challenging without changes to the generic design. This required reinforcement of segregation barriers and slabs.
  - The number of penetrations, including doors, HVAC ducts, cabling, pipework through barriers of nuclear safety significance were not kept to a minimum. As a result of GDA there was reduction in the number of penetrations through these barriers and the layout optimised.
  - Changes to the generic design of penetrations through barriers were necessary to meet ONR's expectations. For example, in the case of doors through barriers of high nuclear safety significance, self-closing designs and lobbied-configurations (double doors) were demonstrated to be reasonably practicable. For remaining single doors through these barriers, position alarms to permanently occupied stations are also expected and were similarly introduced to meet ONR's expectations.

- Underestimation of the effort required to demonstrate the resilience of the design against combination of hazards. Challenges in the identification and rationalisation of combinations, the characterisation of combined loads (which require characterisation of the individual hazard loads, hazard sequences) and residual withstand capacity of SSCs including barriers.

355. Other hazard-specific challenges:

- Implementation of protective, control or mitigative measures against fires (e.g. bunds to contain spills and limit fire spread, or flange shields to prevent pressurised flammable fluids from generating flammable sprays or mists) can

be relatively low cost and are almost certainly ALARP, on defence in depth considerations. Past GDAs resulted in the incorporation of these measures into the design.

- Novel construction materials and techniques for which tests or standards may not be available have in past GDAs required bespoke testing or models (e.g. CFD) to provide suitable substantiation evidence.
- Challenges in meeting the expectation in the Dangerous and Explosive Atmospheres (DSEAR) Regulations 2002 ACOP that a fraction of LFL is used to determine whether a hazardous explosive atmosphere can be present.
- Challenges in the analysis of catastrophic turbine disintegration within the design basis and in ensuring that a sufficient number of nuclear safety-significant SSCs are located away from areas of high probability of impact by low trajectory turbine missiles. Cases with unfavourable plant layouts and entirely reliant on calculated impact probabilities are unlikely to meet ONR's expectations for new plant if it is reasonable to site some systems in protected areas.
- Past GDA experience has showed the need to increase slab thicknesses to prevent failure under dropped load scenarios. The installation of mitigative measures e.g. impact limiters was shown to be reasonably practicable.
- Past GDAs have resulted in a reduction in both the number of lifts and lift heights across the design. ONR expects that lifting of radiological inventories is kept to a minimum and lifts should not be above the maximum drop withstand of the package. Similarly, lifting over SSCs of nuclear safety significance should be avoided and preferably within the impact withstand capability of the SSCs.

356. Early engagement with the RP on the areas below is recommended:

- Scope of hazard identification and characterisation within GDA.
- Identification of appropriate hazard characterisation methodologies.
- Analysis methods, including pressure part failure analyses (pipe whip, jet impact, steam release, internal flooding and blast in isolation and as combined loads).
- Standards and codes. Discussion on ONR's expectations and RGP.
- Methodologies for nuclear safety barrier substantiation against single hazards and hazard combinations (including internal and/or external hazards).
- Beyond design basis expectations.

3.11.5 REFERENCES

357. Approved Codes of Practice, in particular:

- Dangerous Substances and Explosive Atmospheres, Approved Code of Practice and Guidance L138 (2nd edition), 2013
- Safety of Pressure Systems, Pressure Systems Safety Regulations 2000 Approved Code of Practice L122 (2nd edition), 2014
- Safe Use of Lifting Equipment, Lifting Operations and Lifting Equipment Regulations 1998, Approved Code of Practice and Guidance, L113 (2nd edition), 2014

358. IAEA and WENRA Standards:

- Safety of Nuclear Power Plants: Design. Specific Safety Requirements No. SSR-2/1 (Rev.1). IAEA. Vienna. 2016
- Safety of Nuclear Power Plants: Commissioning and Operation Specific Safety Requirements No. SSR-2/2 (Rev.1). IAEA. Vienna. 2016
- Protection Against Internal Fires and Explosions in the Design of Nuclear Power Plants. Safety Guide No. NS-G-1.7. IAEA. Vienna. 2004

- Protection against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants. Safety Guide No. NS-G-1.11. IAEA. Vienna 2004
- WENRA Statement regarding the revision of the Safety Reference Levels for existing reactors taking into account the lessons learned from the TEPCO Fukushima Dai-ichi Nuclear Accident (October 2014) http://www.wenra.org/media/filer_public/2014/11/13/wenra_statement_on_updated_srl_2014.pdf
- WENRA Report Safety Reference Levels for Existing Reactors (September 2014) http://www.wenra.org/media/filer_public/2014/09/19/wenra_safety_reference_level_for_existing_reactors_september_2014.pdf
- WENRA Report on Safety of new NPP designs (March 2013) http://www.wenra.org/media/filer_public/2013/08/23/rhwg_safety_of_new_npp_designs.pdf
- WENRA Statement on Safety of New NPP Designs (March 2013) http://www.wenra.org/media/filer_public/2013/04/05/wenra_statement_newdesigns2.pdf
- WENRA Statement on Safety Objectives for New Nuclear Power Plants (November 2010) http://www.wenra.org/media/filer_public/2012/11/05/wenra_statementonsafetyobjectivesfornewnuclearpowerplants_nov2010.pdf
- Safety Objectives for New Power Reactors (December 2009) http://www.wenra.org/media/filer_public/2012/11/05/rhwg_report_newnpp_dec2009.pdf

359. Additional References:

- Step 4 Internal Hazards Assessment of the EDF and AREVA UK EPR™ http://www.onr.org.uk/new-reactors/reports/step-four/technical-assessment/ap1000-ih-onr-gda-ar-11-001-r-rev-0.pdf
- GDA close-out for the AP1000 reactor - Internal Hazards GDA Issues GI-AP1000-IH-01 to IH-06 http://www.onr.org.uk/new-reactors/ap1000/reports/assessment-reports/onr-nr-ar-16-020.pdf
- Step 4 Internal Hazards Assessment of the Hitachi-GE UKABWR http://www.onr.org.uk/new-reactors/uk-abwr/reports/step4/onr-nr-ar-17-033.pdf
- Lisbona, D. Alexiou, A. (2017), UK regulatory expectations in the assessment of internal fire and explosion hazards through the generic design assessment process, 24th International Conference on Structural Mechanics in Reactor Technology (SMiRT 24) -15th International Post-Conference Seminar on “Fire Safety in nuclear power plants and installations”.
- Lisbona, D., Alexiou, A., MacLeod, T., Smith, L. (2018), Nuclear power plant design resilience against hazard combinations – a multidiscipline view. Proceedings of the International Congress on Advances in Nuclear Power Plants (ICAPP), April 8-11, 2018 - Charlotte, NC (US).

3.12 MANAGEMENT FOR SAFETY AND QUALITY ASSURANCE

3.12.1 INTRODUCTION AND BACKGROUND

360. ONR’s GDA Guidance to Requesting Parties [3] provides guidance on the GDA process and describes what is required of the RP for each step of the process. The RP must therefore develop suitable management arrangements for the project, to ensure that ONR’s expectations are fulfilled. In practical terms, ONR’s MSQA inspectors, working jointly with the EA, will maintain oversight of the RP’s MSQA work to gain confidence that the RP has established an organisational structure,

arrangements and processes able to deliver GDA to time and quality. Therefore, very early in GDA the RP needs to develop robust arrangements to determine and manage the design, safety and security cases and overall project.

361. The reader should note that the DAC, if / when granted by ONR, will list a number of key RP references in order to unambiguously define the basis of what has been included within the scope of GDA and against which the DAC is granted. These are:

- GDA Design Reference.
- Safety Case Head Document.
- Generic Security Report (GSR).
- Master Document Submission List (MDSL).

362. It is therefore important that ONR inspectors are at all times confident that 1) they are assessing / using the correct versions of the RP's documentation; 2) the submissions being assessed are consistent with the GDA Scope agreed and the rest of the RP's documentation; and 3) the RP's management arrangements to deliver the project and underpin the cohesiveness of all its GDA work and outputs are robust.

363. Experience from previous GDAs shows that RPs generally have strong internal MSQA systems but have found difficulties when adapting / expanding their internal QA arrangements to support delivery of the GDA specific requirements. Moreover, it is acknowledged that the scope of this topic aligns and interfaces with the project management arrangements of the GDA for both ONR and the RPs.

364. It is important to note that the aim of this guidance is not to tell MSQA inspectors how to conduct their MSQA regulatory work in GDA. Rather, this guidance highlights those specific aspects of GDA where ONR's MSQA focus is essential. ONR's GDA MSQA inspector/s will work, throughout GDA, very closely with the rest of the assessment team and in particular with the Project Technical Inspector, Safety Case Lead and GDA Programme Manager.

365. This guidance does not duplicate ONR's relevant SAPs MS 1-4 on Leadership and Management for Safety or the Nuclear Safety Technical Inspection Guide (TIG) - LC 17- Management Systems - NS-INSP-GD-017.

3.12.2 SCOPE FOR GDA

366. The GDA RP will have to deliver numerous documents that will constitute the basis of ONR's assessment and, ultimately provision of a DAC.

367. ONR's MSQA assessment and inspection work in GDA will focus on the RP's management systems to deliver GDA and will therefore cover, but will not necessarily be limited to, the following areas:

- RP's GDA project and quality management plans describing the overall arrangements for delivery of the GDA. This should include the RP's GDA project organisation, structure and responsibilities, communication and reporting lines and decision making process. It should also include the management system processes and quality plans showing how the requirements for GDA will be fulfilled and identifying the additional processes beyond the existing company / companies management systems needed to achieve this. This should also include RP's arrangements to control progress of, and changes to, the programme including metrics and performance indicators. These matters can become quite complex if the RP is constituted by several companies jointly requesting, and working to deliver, the GDA.

- RP's procedures for management of the Design Reference, Design Reference Point (DRP), MDSL, RQs, ROs, Regulatory Issues (RIs) and any other processes which are specific for GDA. Examples of these processes are (RQ / RO / RI) commitments capture logs, and arrangements for capturing and transferring assumptions, requirements and commitments made within the safety and security documentation into the as built and the operating regime in a future nuclear construction project based on that design.
- RP's document and record control arrangements.
- RP's design development control and design change control arrangements. The process for managing and agreeing design changes, including specific process for agreeing with the regulators the inclusion in GDA of proposed design changes after the GDA Design Reference is frozen at the DRP.
- RP's management arrangements covering the production, verification and approval of safety and security documentation, including internal challenge, and learning from experience and feedback mechanisms. Management of interdependencies among technical topics.
- RP's arrangements for ensuring that all people involved in the GDA are SQEP, including arrangements for training people on GB specific regulatory philosophy and requirements.
- RP's purchasing arrangements and supply chain controls to ensure contractors engaged in the production of the GDA safety and security are suitably competent and able to deliver good quality outputs.
- RP's arrangements for GDA implementation and GDA Step change readiness.
- MSQA parts within the RP's safety and security documentation which provide information on safety and quality management to demonstrate that any future NPP constructed in GB based on the design undergoing GDA will be constructed, operated and decommissioned in accordance with the requirements of the safety and security cases.

3.12.3 BASIS FOR DECISION

STANDARDS

368. The basis for the decisions made by MSQA inspectors in GDA are:

- ONR SAPs MS 1-4 on Leadership and Management for Safety
- Nuclear Safety TIG - LC 17- Management Systems - NS-INSP-GD-017 Revision 4. http://www.onr.org.uk/operational/index.htm
- Nuclear Safety TAG NS-TAST-GD-051 on "The Purpose, Scope and Content of Nuclear Safety Cases"
- IAEA Safety Standards, Leadership and Management for Safety, General Safety Requirements No. GSR Part 2 IAEA. Vienna. 2016. www.iaea.org
- BSI Standards Publication, BS EN ISO 9001:2015, Quality management systems Requirements
- RGP informed from existing practices adopted on GB nuclear licensed sites

HOW THE MSQA INSPECTORS WORK IN GDA

369. In GDA ONR's MSQA team use a combination of assessment and inspections to undertake the MSQA work. As indicated above, ONR and the EA work jointly in most aspects of the MSQA in GDA.

370. In Step 1 of GDA, an Interface Arrangements document will be developed by the regulators setting out the working arrangements with the RP. This will set out the agreed system for transmission and tracking of submissions, correspondence, meetings, and regulatory questions. Measures are also developed and used to monitor the performance of the regulators and the RP against the agreed GDA programme.

The Interface Arrangements together with the GDA Guidance to RPs are key references for ONR's MSQA work in GDA.

371. Early in GDA the MSQA regulatory team, which typically includes the MSQA inspector, the Programme Manager and the Safety Case Lead, will assess the RP's management arrangements for the GDA project against standards and RGP and will judge whether they are adequate to fulfil regulatory requirements and expectations during GDA, as delineated in the Guidance to RPs and the GDA Interface Arrangements. Throughout GDA the regulators will also inspect the implementation of these arrangements to gain confidence of their suitability and effectiveness.

372. ONR's MSQA inspectors will work very closely with ONR's GDA Safety Case Lead to assess the RP's safety case development arrangements and monitor the development of the safety case and the quality of the outputs. Intelligence about the quality of the safety case documentation will be compiled with input from the specialist inspectors in the GDA team. RP documentation Quality Logs, Safety Case Health Checks and Safety Case inspections are normal regulatory tools used in GDA to support these activities.

373. Similarly, ONR's MSQA inspectors will work very closely with the specialist inspectors in the GDA team to inspect the implementation and effectiveness of the RP's arrangements such as those for ensuring that all people involved in the GDA are SQEP.

3.12.4 LESSONS LEARNED

TRAINING OF STAFF INVOLVED IN GDA

374. All previous GDA RPs have been, or have included, overseas organisations which were unfamiliar with ONR's regulatory philosophy and requirements. Concepts such as ALARP, safety case, fault schedule, as well as the GB context for technical topics such as human factors, internal hazards, etc. were not well understood by the RP staff delivering (including managing) the GDA. The regulators found that GDA specific training to RP staff involved in GDA work was not always provided early enough, was insufficient or did not achieve its intended aim in that it did not provide GDA personnel with a level of awareness of GB safety cases and UK legislation sufficient to deliver the GDA. ONR also found that the RP's GDA management did not have effective means to evaluate the effectiveness of the GDA-specific training, and so it was ONR's GDA team who found the shortfalls during assessment of the submissions, creating unnecessary delays and inefficiencies in the GDA programme. ONR's MSQA team should look early in the GDA at the RP's arrangements (including making appropriate use of GB supply chain) to ensure that all staff working on GDA develop a level of knowledge of GB safety cases and UK legislation sufficient to deliver the GDA.

DESIGN REFERENCE AND DESIGN REFERENCE POINT (DRP)

375. At the core of GDA, is the GDA Design Reference, which lists the documents that describe the design of the reactor and associated plant that the GDA submissions refer to. ONR will expect this to be 'frozen' at a specific date known as the DRP. The RP may wish / need to develop its design beyond the DRP, for which it should implement a GDA design change process. The RP's management of these are key aspects of ONR's MSQA work in GDA.

376. It is very important that very early in GDA the regulators discuss and agree with the RP its proposals for the exact contents and level of depth of the GDA Design Reference. This is particularly important as the design documentation for a NPP could, depending on the level of maturity, include many thousands of documents and it is therefore

important for ONR to make its expectations clear in relation to the depth and extent of the listings in the Design Reference. ONR expects the Design Reference to include descriptions as well as drawings, and to cover buildings, systems and (key) components, however the extent of the Design Reference list needs to be manageable, i.e. it would not be pragmatic to list many thousands of documents. However, whatever the depth of design documentation included, it is important to note that design changes made to aspects of plant not explicitly listed in the Design Reference but falling within the scope of GDA, should be subject to the RP's formal design change arrangements for GDA (which include ONR following DRP), even if none of the documents explicitly listed in the Design Reference change. This has caused confusion in previous GDAs in that RPs initially thought that, post DRP, they could make design changes at a very detailed level and include them in GDA without informing / seeking agreement from the regulators, as long as none of the documents listed in the Design Reference were affected.

377. Another matter for early discussion is whether plant (e.g. buildings, systems, etc.) out of the scope of the GDA should also be listed for transparency (marked as "out of scope"). In previous GDAs ONR found it useful if the Design Reference identified plant / aspects out of the scope of the GDA clearly marked as "out of scope", as this helped to enhance transparency and avoid ambiguities.

GDA RP's MANAGEMENT OF DOCUMENTATION

378. The GDA information submitted by the RP can become a very complex mix of documents adding up to many thousands. For example, several versions of the safety case head document and GSR, several levels of supporting references, proposals for design modifications, additional documents sent by the RP for information, responses to ONR RQs / ROs / RIs, letters, etc. In order to keep appropriate control of this mix of documents, RP's project management arrangements are required to keep track of the documents submitted, of subsequent changes to these documents, and of documents withdrawn. Key to this will be the RP's:

- Consolidated Programme.
- Master Document Submission List (MDSL).
- Document List.

Consolidated (integrated) Programme

379. The consolidated programme, often referred to as the integrated programme, should be developed by the RP to define the activities required to deliver GDA. In this instance, this is typically considered to be the development of the safety and security cases, including the identification of those documents to be submitted to the Regulators.

380. Historically, RPs have struggled to define and develop a programme that provides an appropriate level of detail whilst not becoming overly burdensome. Too many activities providing too much detail has been a common misstep in previous projects. Both extremes of too little detail or too much detail can have a negative impact on the schedule. Therefore, it is important that the RP agrees the structure and approach to management of the programme with ONR's GDA Programme Manager and MSQA Inspector.

Master Document Submission List (MDSL)

381. The MDSL is a 'live' document that allows ONR to understand and reference precisely what constitutes the latest versions of the GDA submissions, and ultimately, when / if a DAC is granted, what exactly they cover. At the end of GDA the MDSL will contain the

totality of the GDA submission that has been submitted to the Regulators, e.g. safety case head document and its references, GSR and its references, and Environmental Submission and its references.

382. In previous GDAs some RPs have taken a long time to formalise the means to track the GDA submission because they found the MDSL concept unclear. Therefore, it is very important that very early in GDA the regulators discuss and agree with the RP the contents and format of the MDSL.

383. Although there is no prescribed formula for the exact format of the MDSL, ONR inspectors need to take into consideration the following:

- The MDSL is referred to in the DAC and reflects the GDA submission, so documents not submitted for assessment should not be included.
- ONR expects all documents listed in the MDSL to be linked, via referencing at any tier, to the safety and security head reports (SC Head Document and GSR). Documents not connected, at any tier, with the safety and security head reports should not be included in the MDSL.

Document List

384. In addition to the consolidated programme and MDSL, the RP needs to develop a GDA Document List (DL) to list and track all the information sent to the Regulators and ensure that configuration, versions, etc., are controlled. The MDSL is only a subset of the totality of the documents in the tracker and therefore, the DL will be significantly larger than the MDSL. For example, RQ and RO responses will be listed in the DL and will be considered in GDA, but their contents will be ultimately captured and integrated into other safety or security reports; the latter will be listed in the MDSL, but not the original RQ or RO responses. Other examples of documents in the DL that will not appear in the MDSL are, for example, RP's presentations, other RP information sent to ONR for the purpose of illustrating how things are done in similar facilities, etc.

385. In previous GDA's, RPs have struggled to develop suitable arrangements to manage and maintain the DL. In particular, RPs struggled to maintain alignment between the MDSL and DL. Therefore, it is very important that very early in GDA the regulators discuss and agree with the RP the contents and format of the DL. Moreover, it will be equally important to understand the roles and responsibilities of the RP's Front Office and Quality Assurance teams in managing the DL and its interfaces with the MDSL.

RP's ARRANGEMENTS FOR CAPTURING ASSUMPTIONS, REQUIREMENTS AND COMMITMENTS IN THE SAFETY AND SECURITY CASES

386. This topic is discussed at length in the safety case section earlier in this report. The MSQA inspectors will work closely with the GDA Safety Case Lead to assess and monitor the RP's development and implementation of these arrangements.

387. In previous GDAs some RPs have taken a long time to develop and implement these arrangements leading to a final output that was not as good and useful to a future licensee as it could have been. Also it is difficult and time consuming to backfit these arrangements. Therefore, it is very important that very early in GDA the regulators and the RP discuss the RP's proposals for its arrangements for capturing assumptions, requirements and commitments in the safety and security cases, as early implementation is of essence.

THE COMPLEXITIES OF OVERSEAS RPs AND MULTI-COMPANY RPs

388. All the GDAs conducted to date have involved overseas RPs and / or multi-company RPs. ONR needs to be aware of the complexities that this adds to the delivery of GDA and how this impacts upon the RP's arrangements to deliver GDA. ONR's MSQA team should ensure that their assessments and inspections cover all offices / organisations involved and matters such as management of interfaces between the different organisations, or between the GB and the overseas offices.

GRANTING A DAC

389. Before ONR can grant a DAC, it has to be confident regarding the consistency of the RP's Design Reference, safety case head document, GSR, MDSL (all listed in the DAC) and ONR's assessment outputs. Attempting to establish this just ahead of granting a DAC would be a very difficult task if throughout GDA ONR has not accrued confidence that the RP's arrangements are robust and have been properly implemented. Therefore, the importance of the MSQA work in GDA cannot be stressed enough.

3.12.5 LINK TO RELEVANT TAGs

390. TIGs and TAGs:

- NS-INSP-GD-017 - LC 17- Management Systems.
- NS-TAST-GD-072 - Function and Content of a Safety Management Prospectus.
- NS-TAST-GD-049 - Licensee Core and Intelligent Customer Capabilities.
- NS-TAST-GD-048 - Organisational Capability.
- NS-TAST-GD-027 - Training and Assuring Personnel Competence.
- NS-TAST-GD-057 - Design Safety Assurance.
- NS-TAST-GD-077 - Supply Chain Management Arrangements for the Procurement of Nuclear Safety Related Items or Services.

3.13 MECHANICAL ENGINEERING

391. Mechanical engineering is the discipline that applies engineering principles to consider the design, analysis, manufacturing, installation maintenance and decommissioning of mechanical systems. It is one of the broadest of the engineering disciplines, covering everything from small individual parts and devices to large and complex systems. In practice, this is applied to a range of static and dynamic SSCs that provide important safety functions as part of the NPP design. This means that, within GDA, the mechanical engineering inspector plans a key role in ensuring that the requirements placed on the equipment are likely to be deliverable by the proposed design, including the use of appropriate codes and standards and the application of RGP.

392. An important distinction is that RPs often consider that structural integrity aspects of SSCs are within the mechanical engineering scope. However, within, ONR these aspects are the subject of a separate assessment by the structural integrity discipline.

3.13.1 SCOPE FOR GDA

DOCUMENTS SUBMITTED

393. A wide range of standards and criteria are normally required to justifying mechanical design. Mechanical engineering discipline's approach to effective assessment is to limit scope by selecting the most appropriate standards and criteria for the specific assessment. This is necessary because the range of SSCs can be extremely wide;

with large numbers of components, numerous interfaces, across various plant process systems and covering multiple disciplines.

394. Future licensees, in collaboration with its vendors, often complete the design of mechanical SSCs after GDA. This makes it difficult for ONR to assess detail design and gain confidence during GDA. Mechanical engineering discipline overcomes this difficulty by targeting the RP's design process to seek confidence that it ensures compliance with GB requirements. If the assessment can establish that the design process is adequate, it follows that detail design after GDA is also likely to be adequate.

395. The RP's documentation justifying the mechanical SSCs should include the following:

- Generic plant layouts, where appropriate, including; plans; drawings and process flow diagrams. These help the inspector to understand the interactions between SSC's, operational restrictions and interfaces other SSCs and civil engineering structures.
- The key functional requirements of the SSCs. It is useful to prepare an engineering schedule that links safety functional requirements to components and links functional requirements and generic design codes.
- Evidence that the SSC design meets the functional requirements, is robust and can withstand design basis loads. A justification for beyond design basis needs to be provided. In some cases this will include calculating margins and failure modes to demonstrate the robustness of the design.
- The design basis for the SSCs, including; a description, generic engineering parameters, materials, loadings, design standards and relevant legislative requirements.
- A demonstration that design codes and standards are relevant and applicable to the SSC design and have been adequately interpreted and applied.
- A demonstration that the analyses methods/computer programmes are adequate to assess the SSCs, and have been adequately validated.
- A demonstration that the SSC design considers interaction between other SSCs or civil structures (for example interaction between crane rails and the civil structure).
- A load schedule setting out key parameters for all lifting and handling operations.
- EIMT requirements. This should include any special requirements for undertaking EIMT (for example, safe isolation, lifting and handling requirements, containment, shielding).
- Clear evidence that the RP has implemented International Operation Experience (OPEX).
- Identification of assumptions and uncertainties where further detailed analysis or design are necessary during the detailed design phase.
- Clarity and consideration of the interactions of the mechanical engineering design with other disciplines.
- Clarity over the reliability claims of the mechanical engineering structures achieved through the design and defence in depth.
- Evidence that the mechanical design considers ageing management and decommissioning.
- A demonstration that the risks to conventional and nuclear safety are reduced ALARP.

396. The number and the level of detail in the documents submitted by the RP can vary. However, previous RP's have found it useful to present the safety case following an approach based on claims, arguments and evidence.

397. Some examples of safety documentation submitted in previous GDAs include:

- Relevant chapters of the top-tier safety case report in the form of a generic PCSR or other type of safety case – This normally includes the claims on the SSCs.
- Basis of Design – Provides the design requirements of the SSCs regarding the robustness of the mechanical engineering design arguments.
- Design reports, supporting calculations and technical drawings (General Arrangement drawings and a selected sample of detailed drawings) for SSCs. These documents will provide the evidence to substantiate the arguments.

SAMPLING AREAS

398. Previous GDA PCSR submissions have not included a dedicated mechanical engineering chapter. Instead, the RP has embedded mechanical SSCs into numerous chapters. In this case it is important that the RP provides ONR with a clear indication (route map) of those chapters relevant to mechanical engineering. For example, there may be a chapter on 'fuel route safety' that might cover many mechanical handling SSCs that are relevant to mechanical engineering.

399. ONR is a sampling organisation and therefore ONR uses sampling during GDA to limit the areas scrutinised and to improve the overall efficiency of the assessment process. The inspector will decide the assessment sample, starting with an initial "broad brush" review of all the documents provided by the RP. The inspector will follow this with a "deep dive" detailed technical assessment of the topics that are important or less clearly explained.

400. Examples of dynamic SSCs considered to be of interest to mechanical engineering include:

- Control rod drive mechanisms.
- Pumps.
- Valves (check valves, motor operated valves, safety relief valves, and isolation valves).
- Cranes.
- Mechanical handling systems.
- Nuclear ventilation systems used to augment nuclear containment barriers.
- HVAC.
- Gas turbines and diesel engines used for emergency power generators.

401. Examples of static SSCs considered to be of interest to mechanical engineering include:

- Pressure vessels.
- Gloveboxes, cabinets.
- Seals.

3.13.2 BASIS FOR DECISION

402. For each SSC sampled, mechanical engineering discipline will seek evidence that the RP has adequately addressed the following:

- Clear safety case claims made on the SSC.
- Clearly set out mechanical engineering design requirements or design basis. This will include: Category and Classification, seismic withstand, design codes and standards, loading, loading combinations, material properties, etc.
- Applicability of the design codes and standards used in the design of the SSC.

- Evidence of appropriate analysis methods and verification and validation studies. For example hazard analysis reliability claims, design qualification.
- Identification of multidisciplinary issues. For example, operability, conventional safety, radiological protection, design for decommissioning.
- Application of ALARP principles to the design.

403. Other areas that the mechanical engineering inspector may assess:

- General site layout and interactions between the civil engineering structures. For example access for construction and maintenance, interface of crane rails with civil structure.
- A justification and comparison study against conformity with European and British standards for any SSCs designed to non-UK design codes, e.g. American codes.
- Compliance or exemption, as applicable, with European product supply legislation. For example, Supply of Machinery Regulations and Pressure Equipment Regulations.
- The approach to beyond design basis and its effects in the mechanical engineering design, e.g. assessment of cliff edge effects in SSCs.
- Reliability of the SSC.
- Consideration of construction techniques particularly where novel techniques are proposed.

STANDARDS AND GUIDANCE

404. SAPs: a number of ONR SAPs are applicable to the mechanical engineering assessment as follows: EKP, ECS, EQU, EDR, ERL, ECM, EMT, EAD, ELO, EHA, EPS, EMC, ESS, EES, and EHT.

405. TAGs: a number of ONR TAGs are applicable to undertaking a mechanical engineering assessment as follows:

- NS-TAST-GD-003 – Safety Systems.
- NS-TAST-GD-004 – Fundamental principles.
- NS-TAST-GD-009 – Examination, Inspection, Maintenance and Testing of Items Important to Safety.
- NS-TAST-GD-016 – Integrity of Metal Components and Structures.
- NS-TAST-GD-022 – Ventilation.
- NS-TAST-GD-036 – Redundancy, Diversity, segregation and layout of mechanical plant.
- NS-TAST-GD-037 – Heat Transport Systems.
- NS-TAST-GD-056 – Nuclear Lifting Operations.
- NS-TAST-GD-057 – Design Safety Assurance.
- NS-TAST-GD-067 – Pressure Systems Safety.
- NS-TAST-GD-094 – Categorisation of Safety Functions and Classification of Structures and Components.
- NS-TAST-GD-098 – Asset Management.

406. Other RGP: documents produced by HSE, IAEA, and WENRA that are applicable to undertaking a mechanical engineering assessment are listed in the References section of this report.

ASSESSMENT PROCESS

407. The guidance described above provides high level principles to consider the design of the mechanical SSCs. A number of tools and techniques, described elsewhere in this report, are available to assist the ONR inspector.

408. Standards that ONR already considers RGP will be directly applied during the assessment. However, if the RP has used novel or “in-house” design codes then, the RP will need to demonstrate that those technical standards provide a design outcome which is consistent with what RGP would achieve.

409. For mechanical engineering the assessment process can be summarised as follows:

- Familiarisation with the RP safety case submission and reactor technology.
- Adoption of a hierarchical approach to identify SSCs for assessment. This involves collaborating with other assessment disciplines and regulators (both nationally and internationally). Identification of SSCs for assessment taking account of their importance to safety and their design novelty.
- Generation and sharing of an assessment plan that scopes planned tasks; technical engagements; deliverables; milestones and timeframes.
- Generation of an audit trail of the full assessment.
- Use of RQs and ROs to question and challenge aspects of the GDA design.
- Ensuring that responses to RQs, and the satisfactory close out of ROs or RIs, are received in a timely manner.
- Use of TSCs to assist the inspector in dealing with the volume of information necessary to examine mechanical SSCs. TSCs can also provide additional expert knowledge necessary to assess the SSCs in some cases.

3.13.3 INTEGRATION WITH OTHER TECHNICAL ASSESSMENT TOPICS

410. Regulatory assessment of the mechanical engineering SSCs cannot be carried out in isolation and mechanical engineering inspectors need to consult with inspectors in other topic areas to verify that the claimed safety function is appropriate. Many of these interactions will be of an informal nature but interactions are essential to prevent assessment gaps, duplications and inconsistencies. An electric overhead travelling crane is a good example where interaction with other topic areas is important.

411. Mechanical engineering inspectors are likely to interact frequently with a number of disciplines as follows:

- Radioactive waste and decommissioning – Interactions are required in reviewing how the mechanical SSCs design may influence decommissioning techniques. Furthermore, the SSC may itself be required to support decommissioning activities once generating operations cease, for example using a building crane during decommissioning activities.
- Structural integrity – Interactions are required when considering structural strength of components, integrity of pressure systems and metallurgical properties.
- Conventional safety – Interactions are normally required in reviewing the RP’s approach to installation, operation and maintenance of mechanical SSCs.
- Civil engineering – Interactions are required when considering the interfaces between mechanical SSCs and the civil structure. For example when considering the crane support columns and the turbine pedestal.
- Electrical engineering – Interactions with electrical engineering are minimal although the electrical power requirements for certain SSCs may require interaction with electrical engineering discipline.
- C&I – Interactions are necessary as many of the mechanical SSCs will have an associated control element. The overall reliability of the mechanical SSC is often dependent on this control aspect. The remote actuation of valves or the control of limits on a crane is two common examples where interaction is important.

412. Other examples of disciplines mechanical engineering may interact with include: chemistry, external hazards, fault studies, human factors, internal hazards, probabilistic safety analysis, radiological protection, safeguards and severe accident analysis.

3.13.4 LESSONS LEARNED

413. There have been three GDAs completed in GB resulting in a number of lessons learned to inform new GDA inspectors and RPs. Lessons learned for mechanical engineering assessment are summarised below.

- Assessment Approach.
  - Raising RQs can result in high work volumes for the RP and ONR particularly if they are difficult to close. It is better to try and group queries together where possible for example by selecting generic design themes such as safe isolation methodology, lifting and handling methodology. RQs must be considered carefully so that there is a clearly defined expectation placed on the RP that can be closed out within GDA.
  - Mechanical engineering is likely to be involved in many cross cutting (i.e. cross discipline) issues. These can introduce complexities if not properly planned and managed. The aim should be to ensure clear understanding of deliverables requiring mechanical engineering input.
  - Continuous engagement with the RP is recommended. This enables any ONR challenges or concerns to be discussed at the earliest opportunity so that the RP has more time to address these challenges and concerns.
  - Designs licenced outside GB do not guarantee a shorter or less complex GDA. All GDA submissions will be assessed in accordance to the GDA process described in this report and associated references.
- Deviation from reference design.
  - GDA may be based on a design that has changed from the original reference plant design. This is acceptable providing the inspector is satisfied that the RP has adequately considered and justified any change. The inspector should also ensure that other ONR disciplines are aware of the change and that they are satisfied with the RPs justifications.
- RP Experience.
  - Some overseas RPs may not have sufficient experience of the GB regulatory regime and inspectors may need to offer advice and guidance on this. In particular they may not have experience in the following:
    - The concept of ALARP
    - Non-prescriptive regulatory regime
    - The concept and structure of a safety case (claims, arguments and evidence)
    - UK regulations, e.g. LOLER, PUWER, Supply of Machinery Regulations, Supply of Pressure Equipment Regulations, Pressure Systems Safety Regulations
- Categorisation and Classification.
  - RPs have not always had a mature categorisation and classification scheme available during early GDA interactions to apply to SSCs. This can make it difficult at the start of GDA to link design and qualification requirements to fault analysis. It is important that the RP considers the effect of qualification of equipment and indicate how it will achieve the necessary classification of SSCs, consistent with the wider safety case.

- Codes and Standards Compliance.
  - The use of UK codes and standards with non-UK design codes and standards requires careful alignment of the design requirements.
  - Design standards and computation techniques change with time and between countries. Inspectors should consider if those proposed are still in line with GB RGP, i.e. UK legislation, standards and guidance. For example, crane design codes and pressure equipment design codes differ between UK and non-European countries.
  - Where no appropriate established codes or standards are available, inspectors should be satisfied that chosen codes are justified and that they can demonstrate similar levels of reliability.
- Construction Design and Management Regulations 2015.
  - UK regulations require the designer (RP during GDA) to understand (and mitigate) the risks associated with construction, commissioning, operations and decommissioning of the plant. This may have an impact on the design of mechanical SSCs.
- Equipment Qualification.
  - Sufficient evidence is required that equipment qualification plans meet ONR's expectation. In particular, plans should demonstrate a suitable sample size and identify test standards commensurate with expected plant lifetime. ONR's lifetime expectations may be longer than those used for overseas reference plant designs.
- Diversity.
  - Claims of diversity in engineered provision made in the safety case need to be justified. In some cases, it may not be possible to provide complete diversity but the RP should demonstrate that it has considered diverse manufacturing practices and enhanced EIMT regimes within systems providing redundancy.
- Complexity.
  - Inspectors should be aware that RPs sometimes add unnecessary complexity to mechanical SSCs in and attempt to satisfy ONR's expectations. Inspectors should be satisfied that RPs have considered simpler alternatives that still satisfy ONR expectations as part of their justifications for the more complex solutions.
- EIMT.
  - RPs need to identify and adequately justify the reliability of any SSCs that will not be maintained or replaced during the plant lifetime. Furthermore, SSCs that have been qualified for the reference design may require additional qualification to justify them for extended operating periods in GB.
  - Adequate demonstration is required that EIMT activities can be performed safely, ensuring that risks are reduced ALARP. For example, safe isolation of plant to meet ONR's expectations of double isolation, safe handling and replacement of SSCs.

3.13.5 REFERENCES

414. The following national and international standards and guidance may be considered:

- Health and Safety Executive (HSE):
  - Health and Safety Executive, Approved Codes of Practice
  - http://www.hse.gov.uk/pubns/books/index-legal-ref.htm
- IAEA:
  - IAEA – Safety Standards: Safety of Nuclear Power Plants: Design, Specific Safety Requirement; SSR-2/1.

http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1534_web.pdf
- IAEA – Safety Standards: Fundamental Safety Principles; SF-1. http://www-pub.iaea.org/MTCD/publications/PDF/Pub1273_web.pdf
- IAEA – Safety Standards: Safety Assessment for Facilities and Activities General Safety Requirements Part 4; GSR Part 4 https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1714web-7976998.pdf
- IAEA – Safety Standards: Ageing Management for Nuclear Power Plants, Safety Guide; NS-G-2.12. http://www-pub.iaea.org/MTCD/publications/PDF/Pub1373_web.pdf
- IAEA – Safety Standards: Design of Fuel Handling and Storage Facilities for Nuclear Power Plants Safety Guide; NS-G-1.4. http://www-pub.iaea.org/MTCD/publications/PDF/Pub1156_web.pdf
- IAEA – Safety Standards: Maintenance, Surveillance and In-service Inspection in Nuclear Power Plants Safety Guide; NS-G-2.6. http://www-pub.iaea.org/MTCD/publications/PDF/Pub1136_scr.pdf

- Western European Nuclear Regulators Association (WENRA):
  - Reactor Safety Levels for Existing Reactors http://www.wenra.org/media/filer_public/2014/09/19/wenra_safety_reference_level_for_existing_reactors_september_2014.pdf
  - Statement on Safety Objectives for New Nuclear Power Plants (November 2010) http://www.wenra.org/media/filer_public/2012/11/05/wenra_statementonsafetyobjectivesfornewnuclearpowerplants_nov2010.pdf
  - Safety of New NPP Designs (March 2013) http://www.wenra.org/media/filer_public/2013/04/30/rhwg_safety_of_new_npp_designs.pdf

3.14 NUCLEAR LIABILITIES REGULATION

415. The nuclear liabilities regulation (NLR) topic covers:

- Management of radioactive materials and radioactive wastes.
- Management of spent fuels after removal from the spent fuel pool, with focus on long-term Spent Fuel Interim Storage (SFIS).
- Decommissioning of nuclear facilities.

416. The NLR topic includes all categories of radioactive wastes in all physical forms (solid, liquid and gaseous). In carrying out this work NLR specialists need to take account of relevant national and international standards and government policies and strategies.

417. A key role of the NLR assessment for GDA is to examine proposals for the minimisation, and safe handling, accumulation and storage of radioactive waste and the management of radioactive material, including spent nuclear fuel arising from all parts of the NPP, throughout the plant's lifecycle, taking due cognisance of UK disposal arrangements for radioactive wastes. This includes consideration of the radioactive wastes arising from the decommissioning of the NPP.

418. ONR's NLR specialists work closely with their counterparts in the relevant environment agencies (EA in England and Natural Resources Wales in Wales). The environment agencies regulate the disposal of radioactive wastes from NPPs. ONR's primary focus is the minimisation and safe management of radioactive wastes (and radioactive materials) at the NPP. There are joint interests between ONR and the environment agencies including the minimisation of radioactive wastes, and the management of higher activity radioactive wastes (HAW) and spent fuel. UK government policy is for these to be disposed of in a future Geological Disposal Facility (GDF).

419. A key aspect of GDA is that new NPPs should be designed and operated so that the risks of future decommissioning are minimised, so far as is reasonably practicable. ONR's assessment will include examination of whether the RP has sufficiently challenged its design for safe decommissioning, including features for facilitating decommissioning.

420. ONR also assesses the generic decommissioning strategy and preliminary decommissioning plan for the generic NPP design, taking account of relevant government policies and strategies. Government policy is for decommissioning to be carried out as soon after final shutdown as is reasonably practicable, taking into account all relevant factors. The design of a new NPP should not foreclose decommissioning strategies that can be carried out safely as soon as is reasonably practicable.

3.14.1 SCOPE FOR GDA

421. The RP is expected to apply its categorisation and classification scheme to all safety functions and SSCs within the scope of GDA. The number of SSCs within the scope of the NLR topic areas will depend on the design and the RP's judgment, but should include key SSCs that make significant contributions to safe management of radioactive wastes and spent fuel, and to the decommissioning of all key nuclear safety significant buildings and structures.

422. Key SSCs that are expected to form the part of the scope of GDA for management of radioactive wastes include the systems for management of gaseous, liquid and solid radioactive wastes, including systems/facilities for the accumulation and storage of such wastes where applicable.

423. The SSCs that are expected to form part of the scope of GDA for decommissioning include all key nuclear safety significant systems and buildings, including the reactor, fuel route, those containing a significant radioactive inventory (of waste and/or material) and relevant support facilities.

424. Conventional health and safety matters associated with decommissioning are reviewed, as appropriate during the GDA, by ONR's specialist conventional health and safety inspectors. The NLR assessment focuses primarily on aspects addressed by the Decommissioning SAPs and relevant matters relating to government policy and strategy on decommissioning.

425. The scope with respect to SFIS after removal from the spent fuel pool depends on decisions made by the RP but also needs to take account of government policy. The UK government's Base Case strategic assumption is the spent fuel from a new nuclear power station will be kept in interim storage on the site of the power station until the point at which it is disposed of in a GDF, and that the packaging of spent fuel will also be carried out on-site.

426. It may not be necessary for SFIS to be available at the start of reactor operations if the RP can demonstrate there is sufficient storage capacity in the spent fuel pool for a number of fuel cycles (and provide adequate storage for removal of all fuel from the reactor core as a result of an emergency). The precise scope of information required for SFIS will need to be agreed with the RP during GDA, but ONR expects this to include a justification for the feasibility of any proposals and a clear demonstration that future potential options for management of fuel throughout its full lifecycle are not being foreclosed.

DOCUMENTS SUBMITTED

427. For the agreed scope, the RP should submit documentation providing the safety case and relevant strategies. This should identify the key safety functional requirements for radioactive waste management, decommissioning and spent fuel management and should demonstrate these requirements can be fulfilled by means of the design and operation of the SSCs identified.

428. The number of and the level of detail in the documents submitted by RPs can vary, as can the approach taken to the structure of the safety case. Some RPs have found it useful to present the safety case using the claims, arguments, evidence approach. It is for the RP to decide the structure and content of the safety case.

429. The NLR topic areas have broader expectations relating to the management of radioactive wastes, spent nuclear fuel and decommissioning that are not met by consideration of safety functional requirements alone. These expectations are reflected in the list of documents that should be included within the scope of GDA to facilitate a meaningful assessment by ONR:

- Information on the radioactive waste and spent fuel inventory/source terms during normal operations, decommissioning and in accident conditions.
- Description of gaseous, liquid and solid waste management systems and their proposed operations.
- Key safety functional requirements for gaseous, liquid and solid radioactive waste management systems and, appropriate to the scope of GDA, for SFIS, and how these are adequately satisfied by the SSCs in the generic design.
- Relevant codes and standards for radioactive waste management, decommissioning and SFIS.
- Consideration of Operational Experience (OPEX) and RGP for radioactive waste management, decommissioning and SFIS.
- Demonstration of safe management of radioactive wastes (including HAW) and of long-term interim storage of spent fuel, including suitable and sufficient design features to support management:
    - Minimisation of generation (including the wastes arising from decommissioning).
    - Application of the waste management hierarchy.
    - Minimisation of accumulation.
    - Control and containment (including prevention of leakage and escape).
    - Characterisation and segregation.
    - Storage.
    - Condition monitoring and inspection.
    - Disposal using available and planned disposal routes (“disposability”).
- Demonstration of an adequately underpinned preferred option for SFIS, commensurate with the scope for GDA.
- A demonstration that non-fuel core components, which can be highly activated, are minimised, managed safely during operation and decommissioning of the generic design and can be disposed of using available or planned disposal routes in the UK.
- A radioactive waste management strategy (which may be addressed by means of an Integrated Waste Strategy) to meet the expectations of SAP RW.1, insofar as it is relevant to GDA.
- Demonstration that the generic design enables the risks of decommissioning to be minimised, so far as is reasonably practicable (design for decommissioning based on currently available technologies for dismantling and decommissioning, not on technologies that may become available in the future.

- A decommissioning strategy to meet the expectations of SAP DC.2, insofar as it is relevant to GDA.
- A Preliminary (also known as Initial) Decommissioning Plan to meet the expectations of SAP DC.4, insofar as it is relevant to GDA.
- Information on the proposed application of decontamination processes and techniques in the decommissioning of the generic design. Consideration of the need or otherwise for decontamination should take account of the overall need to justify the risks as ALARP.
- Demonstrations that the relevant risks are ALARP for:
  - Radioactive waste management.
  - Decommissioning.
  - Long term interim storage of spent fuel.

SAMPLING AREAS

430. ONR takes a "sampling" approach to assessment, targeting areas where hazards and risks are more significant, or the proposed approaches are particularly novel or contentious. The specialist inspector will decide the areas of documentation that ONR will sample. The primary objective is to seek confidence that the relevant risks associated with the generic design have been reduced to ALARP, although in the NLR topics assurance is sought that the generic design is compatible with relevant UK approaches for management of radioactive wastes, decommissioning and long-term interim storage of spent fuel.

431. The initial sampling strategy for assessment is a matter for the individual inspector but may consist of an initial "broad-brush" review of all the documents provided by the RP. The inspector would then carry out more detailed technical assessment of those topics which they consider to be significant in terms of hazard or risk, is otherwise important in terms of matters such as safe long-term management of nuclear liabilities, or where the information is not sufficiently clear to enable judgments to be reached. In such cases this may be lead to the inspector raising RQs and ROs, as appropriate.

432. The following list provides a number of areas on which the NLR inspector may focus, taking account of the key enforcement principles of proportionality, targeting and consistency:

- The safety case claims relating to radioactive waste management, decommissioning and long term interim storage of spent fuel.
- The relevance and applicability of the codes, standards and RGP claimed as being applied in the generic design.
- Multidisciplinary issues identified in the assessment such as the minimisation of radioactive waste (which fundamentally depends on the source term), the control and containment of radioactive waste and radioactive material (including spent fuel), and design for decommissioning.
- Assumptions relating to radioactive waste management, decommissioning and spent fuel management and whether they are consistent with relevant government policy.
- The accumulation and safe management of HAW. HAW is generally more hazardous than LLW and currently has no disposal route available in the UK, pending the availability of the planned GDF. It needs to be stored safely whilst on site to meet the expectations of the relevant SAPs and other regulatory guidance on HAW (see below), including the principle of passive safety. Assessment of information relating to the management of solid LLW may be more limited on the basis of proportionality and targeting.
- Safe management of non-fuel core components, noting some can be initially classified as High Level Waste (HLW) because of high levels of activation.

- Disposability of HAW and spent fuel is assessed by Radioactive Waste Management Limited, the organisation responsible for developing the planned GDF. The environment agencies regulate waste disposal. ONR's assessment is normally limited to ensuring that the RP has obtained disposability advice on HAW from RWM and from the Low Level Waste Repository (LLWR) on LLW. This provides confidence, appropriate to the scope and stage of GDA, that the relevant wastes and spent fuel are likely to be capable of being disposed of by means of existing and planned routes in the UK and the preceding management steps will be compatible with this objective.
- EIMT arrangements relevant to radioactive waste management, decommissioning and long-term interim storage of spent fuel.

3.14.2 BASIS FOR DECISION

433. The application of standards and guidance will form the basis for the judgments made in support of the inspector's recommendation on whether or not a Design Acceptance Certificate should be issued. The focus will be on whether the expectations in the relevant SAPs and ONR's TAGs are met and consideration of relevant government policies, strategies and guidance for the NLR topic area. Amongst the most significant of these include the Government's policy and strategy on the long-term management of solid LLW and the long-term management of HAW and spent fuel by means of geological disposal. The Funded Decommissioning Programme Guidance for New Nuclear Power Stations sets out the strategic "Base Case" assumptions made by government relating to radioactive waste management, decommissioning and management of spent fuel.

STANDARDS AND GUIDANCE

434. The standards and criteria normally adopted in any ONR assessment are:

435. The SAPs – There are specific groups of SAPs relating to radioactive waste management and decommissioning. Other SAPs of relevance include the control of nuclear matter (of particular relevance to management of spent fuel), containment and ventilation and maintenance and inspection. Not all of the SAPs are necessarily fully applicable to GDA, for example SAPs DC.7 on decommissioning organisation and DC.8 on the management system for decommissioning. The inspector needs to consider the applicability of SAPs to the assessment of generic design in planning the scope of the assessment.

436. TAGs, noting that other TAGs may also be of relevance:

- NS-TAST-GD-005 Revision 8 (Guidance on the demonstration of ALARP).
- NS-TAST-GD-024 Revision 5 (Management of Radioactive Materials and Radioactive Waste on Nuclear Licensed Sites).
- NS-TAST-GD-026 Revision 4 (Decommissioning).
- NS-TAST-GD-081 Revision 2 (Safety Aspects Specific to Storage of Spent Nuclear Fuel).

437. As with the SAPs not all of this guidance may be of relevance to GDA. This should be considered in planning the scope and depth of the assessment.

438. Other specific guidance considered during NLR assessment is "The management of higher activity radioactive waste on nuclear licensed sites - Joint guidance from ONR, EA, the Scottish Environment Protection Agency and Natural Resources Wales to nuclear licensees, Revision 2". The applicability of the guidance to GDA should be taken into account in planning the scope and depth of assessment as the guidance considers operational as well as design issues.

439. For IAEA guidance and standards and WENRA guidance, see the References section below.

ASSESSMENT PROCESS

440. The guidance listed above provides high level principles. The RP is expected to be able to demonstrate the relevant principles can be met by means of the generic design and other supporting information (evidence).

441. If the RP has relied upon current RGP in designing aspects of the NPP relevant to radioactive waste management, decommissioning and long-term interim storage of spent fuel. The assessment will be focused on its specific application to the generic design, in terms of the evidence provided. If the RP plans to apply processes/techniques/standards that are not considered to be RGP then it will need to demonstrate why adoption of RGP is not reasonably practicable in order to meet the legal duty that risks are reduced to ALARP.

3.14.3 INTEGRATION WITH OTHER TECHNICAL ASSESSMENT TOPICS

442. GDA requires the submission of a sufficiently developed generic safety case. Regulatory assessment of the NLR topic areas cannot be carried out in isolation, as there are often safety issues of a multi-disciplinary or multidisciplinary nature, in addition to the interests of the environment agencies.

443. Outputs from other discipline assessments may be required to reach an overall judgment on whether the risks associated with radioactive waste management, decommissioning and long-term interim storage of spent fuel are ALARP. It is important that there is good communication to ensure that the scope of work for each assessment discipline adequately recognises the interfaces and the submissions provided by the RP reflect the needs of all relevant disciplines.

444. The need for interactions with other assessment disciplines depends on the technical issues identified during assessment. However, there are some strong interactions between other disciplines and NLR specialists on the basis of ONR's regulatory experience. The following interactions are normally considered during the assessment of radioactive waste management, decommissioning and long-term interim storage of spent fuel but interactions with other disciplines can and do arise during the course of assessment:

- Chemistry – this takes an overview of the source term or radioactive inventory associated with reactor operations and the management of spent fuel in the spent fuel pool. Reactor chemistry, including material selection, is key to the generation and minimisation of radioactive waste.
- Radiation protection – this considers the minimisation of radiation doses to workers by means such as material selection, shielding and contamination control. Such measures also contribute to the minimisation of radioactive wastes and reduction of risks during decommissioning.
- Civil engineering – the civil engineering construction will have an influence on decommissioning and the techniques/methods that could be used to decommission the plant.
- Fuel and core – the design and performance of the fuel during reactor operation and during storage will have an impact on the generation of radioactive waste and the safety of storage of spent fuel.
- Mechanical engineering – this discipline assesses items important to safety (e.g. pumps and valves) and their ability to deliver key functions such as control and containment. Some components are important in minimising radioactive waste by preventing leakage and escape. Mechanical engineering is also

important in assessing risks associated with radioactive waste management, decommissioning and spent fuel management, e.g. movement of waste packages.

- Structural integrity – this assesses safety-related structural components and supports. The behaviour of such materials (e.g. corrosion) can contribute to radioactive waste arisings and affect the risks of future decommissioning and spent fuel management (e.g. neutron activation of components can affect the waste category and the method of decommissioning).
- Internal hazards – this discipline assesses hazards such as fire, explosion, flood, dropped loads, pressure part failure, and steam release etc. within the reactor buildings. This includes the adequacy of: the identification of hazards; prevention of hazards; and the protective barriers, segregation, separation, and active protection systems included in the design to provide mitigation in the event that such internal hazards should occur.
- Conventional safety and fire safety – This discipline considers aspects that might impact on non-nuclear safety, particularly during decommissioning.
- Human factors – These are important in decommissioning, when physical and engineering controls are being removed and risks can change over short time periods.

3.14.4 LESSONS LEARNED

445. Three GDA processes have been fully completed in GB to date. A number of lessons have been learned relating to NLR assessment. Early engagement on the scope of GDA for these topic areas is recommended. Lessons learned from previous GDAs and relevant operational experiences in GB are presented below.

- Radioactive waste management policies, strategies, practices (e.g. classification of radioactive wastes) and disposal routes can vary substantially from country to country. This means that a “generic” design for radioactive waste management systems and processes based on practices in a particular country or region may not be suitable for use in GB.
- It is important to identify potential gaps/differences between GB policies, practices, etc. and the “generic” design in these topic areas as a result of the differences between GB practices and the country in which the design was developed. They could result in the need to challenge the design and ultimately for the RP to modify or even redesign the plant to comply with ONR expectations and practices. This is not necessarily a matter of concern with respect to the feasibility of achieving acceptable levels of nuclear/radiological safety, but risks to workers and the public still need to be demonstrated to be ALARP.
- Care needs to be taken where RP’s may refer to radioactive waste operational data from other countries, as the circumstances from which that data was collated may not be representative of the conditions that will apply in GB.
- It is important to gain assurance that the relevant safety case claims, arguments and evidence made by the RP are consistent with those made in submissions to other disciplines. Previous experience has found inconsistencies between submissions made on the topics of decommissioning and management of radioactive wastes compared to submissions made to the chemistry topic area for example in relation to surface treatment methods and the intended scope of chemical decontamination.
- ONR would expect the key constraints for radioactive waste systems to be identified and justified in terms of both normal operations and reasonably foreseeable events or deviations from the expected condition, to allow subsequent detailed design and operational delivery of the various treatment stages to be bounded and confirmed as suitable. The RP should define the full

range of anticipated feeds into the radioactive waste management systems, consistent with the Source Term. It is important for the generic case to be clear on its use of 'best estimate' and/or 'design basis' data, when and how this data will practically apply and for how long related challenges will be imposed on the radioactive waste systems.

- Generic safety cases have to accommodate unavoidable uncertainties. In such instances ONR expects that a precautionary approach should be applied. The generic case should provide assurance that the technical viability of the intended strategy for managing radioactive wastes is not dependent on potentially optimistic assumptions on how the reactor will perform in practice. ONR therefore targets those parts of the generic case that may be vulnerable to 'cliff-edge' effects in the event that underpinning assumptions prove to be incorrect. This includes consideration of radioactive wastes for which the final waste categorisation is uncertain.
- The RP will need to demonstrate the design (and associated documentation) is consistent with relevant government policies and strategic assumptions, and that the plant is capable of producing radioactive wastes that can be disposed of by existing and/or planned routes available in the UK. Key strategic assumptions include the storage of spent fuel pending planned disposal in the GDF (i.e. spent fuel is assumed not to be reprocessed) and the long-term storage of HAW and spent fuel pending the availability of the GDF. These assumptions affect a range of aspects of the design such as the assumed design life of radioactive waste storage facilities and waste packages.
- The RP is expected to demonstrate that HAW arising from the operation of the generic design can be managed safely across the lifecycle of the wastes. This may be achieved by means of preparation of a Radioactive Waste Management Case (RWMC, as described in the Joint Guidance for the management of higher activity radioactive wastes).
- The regulation of the accumulation of radioactive waste by ONR does not appear to be well understood in comparison with the understanding of the regulation of disposal of radioactive wastes by the environment agencies. The RP needs to demonstrate that the accumulation of radioactive wastes can be minimised, primarily be demonstrating that the radioactive wastes produced can be disposed of by available or planned routes. Accumulated wastes need to be stored safely. Early engagement with the organisations responsible for disposal of radioactive wastes is recommended.
- The documentation of the options assessment processes used in making decisions is important in these topic areas, in the context of ONR's non-prescriptive goal setting regime. Understanding the reasons for decisions made and the options that have been considered in reaching the decision is valued by ONR in its consideration of whether risks have been reduced to ALARP. These areas are also known to be of particular interest to stakeholders. There should be clear linkages to any consideration of hazards and identification of design features incorporated to minimise risks SFAIRP. RPs have typically presented arguments that overemphasise the back-end of the waste management process (disposal), with insufficient consideration of waste avoidance, minimisation, generation and conditioning, such that a holistic consideration has not always been provided.
- The disposal of radioactive wastes is regulated by the relevant environment agency and the RP needs to demonstrate that Best Available Techniques (BAT) are being applied. Experience of previous GDAs has indicated that it has been difficult for RPs to understand that it is also necessary to demonstrate that the risks associated with radioactive waste management are reduced to ALARP. Some of the expectations in these topic areas, for example the minimisation of radioactive wastes, are relevant to ALARP as well as BAT and

need to be adequately addressed in safety as well as environmental documentation.

- The RP should provide evidence of an adequately integrated approach to ALARP and BAT and demonstrate the application of both ALARP and BAT for the generic design. ONR's TAG on ALARP recognises the possibility for conflict in the different regulatory application of ALARP and BAT in nuclear safety and environmental protection. The TAG states it is important that adequate weighting is given to health and safety aspects during optioneering studies carried out to establish BAT so that an overall ALARP solution that balances health, safety and environmental aspects is reached in an optimised manner. This is of particular relevance to radioactive waste management, spent fuel management and decommissioning because disposal of radioactive wastes is the ultimate outcome of the application of the systems and processes. ONR's NLR specialists work closely with their counterparts in the environment agencies to ensure that ALARP and BAT are appropriately integrated.
- Management of non-fuel core components. Experience of reactor operations and other GDAs indicate that managing these wastes can be challenging because of high radiation levels resulting from activation in the reactor core and because they may not be readily accommodated in operational waste management processes (e.g. storage and packaging). It is important that these components are included in the overall radioactive waste inventory and that the quantities expected during operation are understood by the end of GDA. These wastes will need to be stored safely and converted into a passively safe form prior to disposal in the planned GDF.
- The codes and standards used should be relevant and applicable to the processes and SSCs selected relating to radioactive waste management, decommissioning and spent fuel management.
- The radioactive waste and spent fuel inventory/source terms should include information on characterisation, the basis of any assumptions made, the sources of the information used to derive the inventories/ source terms and uncertainties in measurements/ estimates.
- In recent years the UK has identified some radioactive wastes that can present particular challenges in developing strategies for their management:
    - "Boundary" wastes are defined as radioactive wastes at or close to waste classification limits), particularly those on the boundary between low level waste and HAW. The RP should identify any potential boundary wastes, and demonstrate their arisings can be minimised and managed safely across their lifecycles.
    - "Problematic" wastes are defined as those radioactive wastes for which no defined management route is either available or currently planned in detail, or for which existing solutions are sub-optimal. These do not include HAW for which disposal to the GDF using established waste processes and packages are planned. The RP should identify any potential problematic wastes, and demonstrate their arisings can be minimised and managed safely across their lifecycles.
- Assessment of Integrated Waste Strategy (IWS) documents indicates that such documents may not always meet the expectations of Safety Assessment Principle RW.1 because they are typically high level summaries of waste strategies, used as vehicles for communication with stakeholders. Additional underpinning evidence may be needed to make an adequate demonstration. The underpinning of justification of the chosen options described in the IWS, by means of strategic options studies and consideration of ALARP (and BAT), is of particular importance.
- The demonstration that the generic design enables safe decommissioning should not be based solely on good practice principles but should include evidence of how the design has been challenged and how the principles have

been implemented in the generic design. Information should be presented on the dismantling of large items such as the reactor pressure vessel and steam generators, other major modules and primary devices as well as on the dismantling of buildings/structures. The demonstration should take account of relevant Operational Experience (OPEX) and RGP in decommissioning.

- An important aspect of the decommissioning strategy is justifying the proposed timing of decommissioning, taking account of the expectations and relevant factors in SAP DC.3. This aspect is important in relation to government policy on new build, which assumes that decommissioning will be carried out promptly after cessation of reactor operations. The RP needs to be familiar with relevant government guidance (Funded Decommissioning Programme Guidance for New Nuclear Power Stations). It is also important not to foreclose options for future decommissioning.

3.14.5 REFERENCES

446. IAEA guidance and standards (this list is not exhaustive):

- IAEA Fundamental Safety Principles: Safety Fundamentals SF-1, IAEA, Vienna, 2006
- General Safety Requirements Part 5: Predisposal management of radioactive waste, No. GSR Part 5, IAEA, Vienna, 2009
- General Safety Requirements Part 6: Decommissioning of Facilities, No. GSR Part 6, IAEA, Vienna, 2014
- Specific Safety Guide No.15 Storage of Spent Nuclear Fuel, SSG-15, IAEA, Vienna 2012
- Specific Safety Guide No.40 Predisposal Management of Radioactive Waste from Nuclear Power Plants and Research Reactors, SSG-40, IAEA, 2016
- Storage of Radioactive Waste, Safety Guide, WS-G-6.1, IAEA, Vienna, 2006
- Specific Safety Guide No. 47 Decommissioning of Nuclear Power Plants, Research Reactors and Other Nuclear Fuel Cycle Facilities, SSG-47, Vienna, 2018
- Design Lessons Drawn from the Decommissioning of Nuclear Facilities, IAEA-TECDOC-1657, IAEA, Vienna, 2011

447. WENRA guidance:

- Safety Reference Levels for existing reactors, WENRA, September 2014,
- Reactor Harmonisation Working Group report on Safety of new NPP designs, WENRA, March 2013
- WENRA Report on Treatment and Conditioning Safety Reference Levels, 2018
- Decommissioning Safety Reference Levels, version 2.2, WENRA, 2015
- Waste and Spent Fuel Storage Safety Reference Levels, version 2.2, WENRA, 2014

3.15 PROBABILISTIC SAFETY ANALYSIS

448. PSA is an integrated, structured, logical safety analysis that combines engineering and operational features in a consistent overall framework.

449. It is a quantitative analysis that provides measures of the overall risk to the public that might result from a range of faults (for example, failure of equipment to operate, human errors, or hazards such as fires).

450. PSA enables complex interactions (for example between different systems across the reactor) to be identified and examined and it provides a logical basis for identifying any relative weak points in the proposed reactor design.

451. Other terms such as probabilistic safety assessment (PSA) used by the IAEA and probabilistic risk assessment (PRA) used in the USA, are equivalent.

3.15.1 SCOPE OF THE ASSESSMENT

452. During GDA, it is expected that the RP submission includes a fully documented full scope PSA, covering all the relevant sources of radioactivity, all relevant initiating events (IEs) (including internal and external hazards) and all operation modes. The outcomes of the hazards prioritisation will determine the level of detail of the different hazards PSAs. It is considered RGP that fully documented PSAs (in line with the PSA TAG) are provided for internal fire and flood, seismic and external flood with a level of detail in line with the level of development of the generic design.

DOCUMENTS SUBMITTED

453. The number and the level of detail in the documents submitted by the RP can vary. The following is considered RGP:

- A dedicated chapter in the top-tier safety case report (SC Head Document).
- A PSA summary report referenced in the top-tier safety case report.
- Individual reports for each of the PSA tasks (or sub-tasks, when appropriate, such as individual systems reports).
- The PSA computer model (including input parameter data bases, result files and other relevant documentation).
- The complete task files, including relevant references, should be made available to ONR upon request.
- A document database that identifies the relevant documentation supporting the PSA.
- A PSA project plan, including:
  - A complete list of the PSA objectives, applications and definition of the requirements of the PSA to fulfil these.
  - Identification of the various procedures used to support the development of PSA tasks and PSA applications.
  - The PSA quality assurance and quality assurance procedures followed in the development of the PSA.

KEY ASSESSMENT TOPICS AND ASSESSMENT APPROACH

454. The ONR inspector will typically start the review by ensuring that the technical foundations of the PSA are adequate, including the following:

- There is a clear description and justification of the PSA methods and techniques (including relevant PSA tasks procedures) used in the development of the level 1, level 2 and level 3 PSA. The ONR inspector should expect the PSA methods and techniques, and their application in practice, to meet international good practice. When assessing the adequacy of the methods some in-depth spot checks of models and data may be required to ascertain that those methods and techniques have been adequately applied.
- There is a clear description of the processes used to support the development of the PSA and PSA applications and justification that these processes and their implementation by the RP meet RGP. The ONR inspector expects to see reasonable justification to show the following:
  - The PSA is based on robust and traceable processes in which all details of the PSA, including explicit and implicit assumptions, modelling techniques, etc. are fully checked, documented and recorded.

- Adequate processes have also been used to ensure high quality of the inputs from other teams into the PSA and adequate substantiation of related aspects of the PSA.
- The PSA reflects the NPP design being assessed by ONR and is updated, as appropriate, and following an adequate process, to reflect design modifications during GDA.
- The PSA assumptions are captured, tracked and reviewed when further information becomes available. There should be a process to enable these assumptions to be transferred to the safety case supporting future stages of the NPP development and then reviewed as necessary. For example, review and update of assumptions may be needed during completion of the systems' detailed design, during construction and decisions on equipment location, cable routing and hazard protection strategies, during the development of operational and emergency procedures, technical specifications, maintenance schedule, etc.
- The PSA is integrated into the design process (for example the PSA provides input to the development of design modifications, operational and emergency strategies and procedures, safety classification of SSCs, etc.)
- The PSA is used to support the demonstration that the level of risk is ALARP.

- The PSA has a robust basis and the scope of the PSA covers all the relevant sources of radioactivity, all relevant IEs, and all operation modes. In order to consider this point, the ONR inspector can choose to undertake, early in GDA, detailed reviews of some specific aspects of the PSA considered to be key technical foundations, for example:
  - Identification and grouping of IEs.
  - Prioritisation of internal and external hazards for the PSA.
  - PSA reliability data analysis such as data for IEs frequencies, component failure probabilities and unavailabilities, common cause failure (CCF) probabilities, etc.
  - Scope of the success criteria analysis for the PSA.
  - Scope of the severe accident analysis for the level 2 PSA.
- The PSA results that represent the level of risk of the NPP meet regulatory expectations.

455. If the ONR inspector is satisfied that the outcomes of the review of the technical foundations of the PSA are broadly adequate to move to the next step of assessment, a detailed review of the PSA models and data, and the underlying supporting analyses may be conducted on a sampling basis against the PSA TAG (see below).

SAMPLING AREAS

456. The above section provides a description of the scope of the assessment usually carried out in GDA. During the detailed review, the ONR inspector may decide to adopt a sampling approach in some areas. It is important to note that the full PSA submission needs to be provided by the RP, independently of the sampling approach undertaken by the ONR inspector.

457. The ONR inspector will normally assess each of the main technical areas considered essential to produce a full scope PSA in line with the PSA TAG. A good understanding of each technical area of the PSA would then enable an overall judgement to be made regarding the adequacy of the PSA.

458. The detailed review often includes a representative sample of fault trees, event trees, supporting analysis and reliability data. The sampling should cover all type of systems

such as front line and support systems, C&I, electrical, water / air, systems, etc. It should also cover all types of IEs that can occur in the reactor being assessed, such as transients, LOCAs, anticipated transients without scram, etc. This is key to ensuring that the review addresses the thermal-hydraulic behaviours of the reactor in a comprehensive manner.

459. The sampling needs to be done in a focussed, targeted and structured way with a view to revealing any specific or generic weaknesses in the PSA. For example, the event tree and success criteria analyses behind the analysis of faults such as Steam Generator Tube Ruptures have often been included in the scope of the detailed review because of the complexity of this type of scenario.

460. The ONR inspector may also decide to inspect the process and implementation records used in the development of PSA or for PSA applications. The review of the adequacy of the various codes, and how they have been used to support the PSA, may involve an inspection of verification and validation records or other supporting documentation such as input decks.

3.15.2 BASIS FOR DECISION

STANDARDS AND GUIDANCE

461. ONR's SAPs [1] constitute the regulatory principles against which duty holders' safety cases are judged. SAPs FA 10 to 14, and the following TAGs are key to the assessment of PSA:

- NS-TAST-GD-030 – PSA.
- NS-TAST-GD-063 – HRA.

462. ONR expectations for an acceptable PSA outlined in the SAPs and TAGs are generally consistent with international standards and guidance, such as IAEA level 1 and level 2 PSA standards, Nuclear Energy Institute (NEI) Peer Review Process Guidance and the American Society of Mechanical Engineers (ASME) PRA standards (see list of references).

463. It is accepted that for a less mature design, the level of detail of the PSA will be commensurate with the level of detail of the design. The PSA TAG provides clear expectations regarding the use of assumptions for aspects of the facility not yet available or under development.

464. The ONR inspector will also review whether the PSA results meet SAP NT.1 Targets 7 to 9 (see section 2.2). The assessor should bear in mind that all the plant damage states will need to be considered to allow comparison with SAPs Target 9 and Target 8 (>1000 mSv). In addition, to allow comparison with SAPs Targets 7 and 8 (<1000mSv), in addition to the level 1 PSA sequences leading to non-success states (for example core damage or fuel damage), captured as plant damage states in the level 2 PSA, the success states from the level 1 PSA as well as non-reactor or non-fuel pool faults outside the scope of a typical PSA will also need to be considered.

EVALUATION OF THE IMPORTANCE OF SHORTFALLS

465. In previous GDAs, to evaluate the importance of the findings in the various PSA technical areas, a Risk Gap Analysis (RGA) was conducted. This was a complex task but in some cases it was essential to consolidate the regulatory decision at the end of GDA PSA assessment. The RGA consisted of a series of sensitivity analyses that when possible (and reasonable) were combined. RGAs have been undertaken by

ONR's TSC or by the RP (in which case they should be included in the scope of the ONR inspector's review).

3.15.3 INTEGRATION WITH OTHER TECHNICAL ASSESSMENT TOPICS

466. Due to the nature of the PSA, the ONR inspector needs to recognise that the assessment should include consultation with inspectors in other topic areas; also, other inspectors may seek input from the PSA as discussed below.

467. These interactions help to prevent assessment gaps, duplications and inconsistencies, and, therefore, they are key to the success of GDA. Examples of these interactions are:

- Human factors: this provides input to the assessment of the PSA's HRA. In addition, the PSA provides input to the identification of the human-based safety claims, human failure events (HFEs) and evaluation of their importance to overall risk. The ONR inspector should be attentive to how the RP has managed the PSA and HF interface during the development of the PSA, as HRA supporting information may have been developed in parallel to the PSA and there may be inconsistencies between the model and the analyses.
- Fault studies: this provides input to the assessment of the level 1 PSA success criteria. In addition, the PSA and fault studies topic areas should cooperate to gain confidence in the completeness of the list of initiating events identified for a facility. The RP's PSA modelling will be an input to the initiating event frequencies identified in the fault schedule.
- Severe accident analysis: this will provide input to the assessment of the level 2 PSA. An important area of interface is the identification of the scope of confirmatory analyses.
- Structural integrity: this provides input to the assessment of, for example, the containment structural analysis (metallic parts) for the level 2 PSA. Structural integrity will also provide input to the assessment of the external hazards PSA (regarding fragilities of metal components).
- Civil engineering / external hazards: this provides input to the assessment of the containment structural analysis for the level 2 PSA and to the external hazards PSA regarding definition of hazards' magnitudes and frequencies, and fragilities of structures.
- Internal hazards: this provides input to the review of the internal hazards prioritisation and PSA to ensure, for example, that assumptions in the model are aligned with the design and operational procedures and that the list of internal hazards considered is complete.
- Radiological protection: this provides input to the assessment of the level 3 PSA.

468. In addition to the above, throughout GDA there will be interactions between PSA and all the other technical disciplines. Many of these interactions are of an informal nature, but they are essential to ensuring consistency across the reviews of the various technical aspects of the safety case. For example, the PSA often incorporates detailed modelling of the C&I, electrical and mechanical systems' relevant failure modes (including software), common cause failures, etc. The interfaces between PSA and C&I, electrical engineering and mechanical engineering are key to ensuring that the PSA adequately reflects the design of those systems, including failure modes, reliability data and assumptions. The PSA discipline also provides input to the engineering reviews in those areas regarding claims, failure modes, dependencies and evaluation of the importance of the individual systems to the overall risk. In past GDAs, the interface between PSA and C&I has been particularly important and the PSA has

provided information on vulnerabilities in the design that was used to check the completeness of the C&I design requirements.

469. It is therefore important to stress that the PSA results can be used to support the assessment in other technical areas. PSA results and risk importance rankings provide useful insights to understand the risk significance of the faults, SSCs and operator actions, which can help inspectors in other topic areas to target / focus their assessment.

3.15.4 LESSONS LEARNED

470. There have been three GDAs completed in GB and as a result there are a number of lessons learned for new GDA inspectors and for the RPs, many of these (not all) are relevant to these three GDAs.

- Partial scope PSAs do not provide the full picture of the risk and distort the risk profile and importance of SSCs. Any decisions made with a partial scope PSA (such as design modifications) may not be optimal. The missing parts may potentially represent higher risk than the existing parts and may substantially impair a proper understanding of the risk. For example, lack of, or limited, PSA for internal hazards can have an important impact on the risk profile. In addition, for modern NPPs with low core damage frequencies (CDF), the percentage contribution of the risk associated with external hazards can be much higher than for older NPPs (even dominant).
- It is worth assessing in detail the list of IEs as reviews often find that important IEs are missing and / or wrongly grouped.
- Very low CDF / Large Release Frequency (LRF) may be an indication of gaps / shortfalls in the PSA or in the data derivation. The ONR inspector may choose to inspect the process and records underpinning the derivation of data, if ONR is not familiar with the data sources used.
- Model simplifications, for example omission of components or component failure modes based on low probability, which were considered acceptable in PSAs for old NPPs (where CDFs may have been around 1E-4/yr) are no longer justified for modern reactors (with CDFs < 1E-6/yr).
- Reviewers often find that the modelling of pre-accident HFEs (misalignments and miscalibrations) is incomplete, or the pre-accident HFEs are left out of the models altogether, which is not acceptable.
- Reviewers often find issues with the treatment of dependencies between human errors; treatment of human dependencies is often optimistic, which may lead to substantial underestimation of the risk.
- The potential for misdiagnosis needs to be evaluated and the HFEs modelled in the PSA as appropriate; this is often found lacking during PSA reviews.
- The modelling of the containment isolation is often found to be too simplified and missing dependencies. Similar issues have been found with other systems credited in the level 2 PSA.
- Equipment survivability issues are often missed in level 2 PSAs.
- Holistic treatment of hydrogen phenomena is often lacking in the level 2 PSA, including the consideration for hydrogen combustion outside containment if / where appropriate.
- It is often useful for the ONR inspector to discuss with the RP early in the review:
    - The adequacy of the processes to develop and use the PSA, including how the PSA will be used to inform, and will reflect, design development (including design changes), the demonstration of ALARP and the process to capture and review assumptions, as it is likely that assumptions will become key issues to follow up after GDA.

Establishing these processes early helps the RP to record evidence in an adequate way from the beginning, avoiding inefficiencies and iterations.

- The quality of the documentation and production of a documentation map / list of the references and submission dates. Documentation is as important as the PSA model but reviewers often find parts of the PSA documentation to be poor or lacking. Traceability of the PSA model and data to design documentation, supporting analyses, and other supporting documents, is essential.
- In some cases the RP may need to translate documents, such as document input decks, which will need time to prepare. Identifying these early can help efficiency.
- The RP's PSA capability and capacity. The RP may sometimes benefit from acquiring additional support at early stages of the GDA, if the RP is not sufficiently familiar with ONR's expectations and RGP in PSA. This will avoid inefficiencies and repetitions in any work that needs to be developed during GDA.

3.15.5 REFERENCES

- IAEA - Safety Standard – Specific Safety Guide SSG-3 Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants (http://www-pub.iaea.org/MTCD/publications/PDF/Pub1430_web.pdf)
- IAEA - Safety Standard – Specific Safety Guide SSG-4 Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants (http://www-pub.iaea.org/mtcd/publications/pdf/pub1443_web.pdf)
- NEI- PRA Peer Review Process Guidance, NEI 00 02 (2000)
- NEI- Process for Performing Follow on PRA Peer Reviews using the ASME PRA standard, NEI 05-04 (2008)
- PRA standards issued in the US by the American Nuclear Society (ANS) and the American Society of Mechanical Engineers (ASME):
  - ASME/ANS RA-Sa-2009, "Addenda to ASME/ANS RA-S-2008 Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Application"
  - ANS/ASME-58.22-2014, "Requirements for Low Power and Shutdown Probabilistic Risk Assessment" (Trial use)
  - ASME/ANS RA-S-1.2-2014, "Severe Accident Progression and Radiological Release (Level 2) PRA Methodology to Support Nuclear Installation Applications" (previously ANS/ASME-58.24) (Trial use)
  - ASME/ANS RA-S-1.5, "Advanced Light Water Reactor PRA Standard" (Draft)

3.16 RADIOLOGICAL PROTECTION

471. The focus of radiological protection in GDA is on occupational exposure of staff on site from all pathways, public exposure off site from direct radiation shine during normal operations and exposure of staff during post-accident recovery operations.

472. In GDA, ONR radiological protection leads on:

473. Occupational exposures to staff arising from:

- Normal operations from commissioning through to decommissioning.
- Airborne discharges e.g. noble gas release (Ar-41).
- Handling, processing and accumulation of radioactive waste.
- Leakage and escape of radioactive materials.
- Post-accident recovery.

474. Doses to Public

- Direct gamma and neutron shine from normal operations on-site.

475. Aspects outside the scope of this guidance:

- EA leads on public exposures from all discharge routes and environmental impact.
- Radiological consequence analysis for faults identified by level 3 PSA is carried out by Radiological Protection specialists, but this is not covered by this guide.
- A Radiological Protection Inspector may examine the criticality analysis for the Spent Fuel Pool. The adequacy of reactivity control in the reactor needs to be looked at by fault studies and fuel and core.

3.16.1 SCOPE FOR GDA

476. Radiological protection applies through all phases of the facility lifetime; design, construction, commissioning, operation and decommissioning and all modes of operation; start-up, hot stand-by, shutdown, transient, anomalous, fault and accident.

477. The main focus for radiological protection is risks that will arise from normal operations rather than from fault conditions. Therefore, issues such as justification for radiological doses to workers and the public, the adequacy of engineering controls (such as material selection or radiation shielding) and measures to control radioactive contamination are the focus during design assessment.

478. It should be noted that good use of operational experience (OPEX), including data, from relevant existing plants is of key importance in producing the radiological protection safety case. This is particularly true of areas such as source term, radiological dose assessment and demonstration that doses to workers and the public are ALARP.

479. Radiological Protection has input into fault consequences, but does not lead on these issues.

AREAS FOR ASSESSMENT AND DOCUMENTS SUBMITTED

480. These include but are not limited to the following, which also indicates where key documents will be required:

- Source term - understanding the hazard to assess against by use of OPEX and calculation tools and showing it has been minimised. This includes radioactive sources that are part of the design and sources arising from reactor operation.
- Containment design - control radioactive material and prevent movement into the operational environment, this includes ventilation.
- Shielding design – demonstration that the design provides adequate protection against radiation hazard by use of OPEX and calculation tools.
- Designation of areas – identify and designate risk level for each room/area, engineered controls where required to restrict access.
- Exposure Assessment of Workers - radiological dose, internal and external components to workers, highest dose tasks including routine and breakdown maintenance, assessment of equipment reliability arguments using OPEX where available.
- Exposure Assessment of the Public - external direct radiological exposure to members of the public using OPEX where available.
- Post-accident accessibility – minimise the exposure to workers acting to mitigate accident consequences.

- Instrumentation – use of instrumentation provided for radiation protection purposes in the design of the plant.
- Waste handling and decommissioning – minimise exposure to workers for all operations at all stages of lifecycle.
- The RP's approach to ALARP as applied to occupational exposure and public exposure due to direct radiation shine, with a particular focus on the tasks contributing most to occupational exposure using OPEX where available.

3.16.2 BASIS FOR DECISION

481. For radiological protection, this will be primarily against UK Law. For radiation protection, the Ionising Radiations Regulations 2017 (IRR 17) are the main legal requirements. Detailed references to IRR 17 and references to other guidance documents including IAEA guidance and standards and WENRA guidance are provided in the References section below.

482. TAGs (http://www.onr.org.uk/operational/tech_asst_guides/index.htm) give additional detailed guidance to inspectors. A number of TAGs provide the principle expectations of ONR regarding radiation protection. These are:

- NS-TAST-GD-002 "Radiological Shielding".
- NS-TAST-GD-004 "Fundamental Principles".
- NS-TAST-GD-005 "Guidance on the demonstration of ALARP (As Low as Reasonably Practicable)"NS-TAST-GD-038, "Radiological Protection".
- NS-TAST-GD-041 "Criticality Safety".
- NS-TAST-GD-043 "Radiological Analysis Normal Operation".
- NS-TAST-GD-045 "Radiological Analysis Fault Conditions".

483. Additional Guidance can be obtained from TIGs e.g. ONR-INSP-GD-054 "The Ionising Radiations Regulations 2017.

484. SAPs are written as guidance for ONR inspectors and hence are a useful reference source for RPs (http://www.onr.org.uk/saps/saps2014.pdf). Parts of the SAPs of particular relevance to Radiological Protection in GDA are as follows:

485. Fundamental Principles

- FP.3 Optimisation of protection.
- FP.4 Safety assessment.
- FP.5 Limitation of risks to individuals.
- FP.6 Prevention of accidents.
- FP.7 Emergency prep. & response.
- FP.8 Protection of present & future generations.

486. Radiological Protection

- RP.1 Normal operations (Planned exposure situations).
- RP.2 Fault and accident conditions (Emergency exposure situations).
- RP.3 Designated areas.
- RP.4 Contaminated areas.
- RP.5 Decontamination.
- RP.6 Shielding.
- RP.7 Hierarchy of control measures.

487. Engineering Principles : Key Principles

- EKP.1 Inherent Safety.

- EKP.2 Fault Tolerance.
- EKP.3 Defence in Depth.
- EKP.4 Safety Function.
- EKP.5 Safety Measures.

488. Accident Management and Emergency Preparedness

- AM.1 Planning and Preparedness.

489. Numerical Targets and Legal Limits

- NT.1 Assessment against Targets.
- NT.2 Time at Risk.
- NT.3 Applying the Targets.

490. The SAPs set numerical targets. Targets 1, 2 and 3 are the most relevant for Radiological Protection. It should be noted that these are linked to the legal dose limits in IRR 17.

491. A combination of fault studies, PSA and radiological protection disciplines will also be looking at proportionate consideration of targets 5 and 6 within GDA. The level of effort required will be informed by the novelty of the design. An overview of all numerical targets is given in the cross cutting section of this document.

3.16.3 INTEGRATION WITH OTHER TECHNICAL ASSESSMENT TOPICS

492. Integrated working is vital both for regulators and the RP to ensure the GDA process delivers a design where risks are ALARP and is efficient and effective.

- Chemistry leads on the source term topic due to the importance of plant chemistry in controlling source term. As occupational exposure is strongly related to source term, radiological protection works closely with chemistry on this topic.
- Mechanical engineering and radiological protection cooperate in assessing the mechanical and radiological properties of reactor materials and in the ventilation design topic.
- Structural integrity and radiological protection cooperate in assessing the structural and radiological properties of reactor materials.
- Human factors provide input into the application of IRR 17 in areas such as access control.
- Civil engineering provides input to the radiation shielding aspects of the radiological protection assessment.
- Nuclear liabilities provide input into the ALARP justification for waste, spent fuel and decommissioning strategies.
- C&I provide input into areas such as monitoring, warning devices and alarms.
- The radiological protection assessment provides input to the public exposure from direct shine aspects of the EA's environmental assessment.
- Radiological protection provides input into the radiological consequences assessment of fault studies, PSA and severe accident analysis (SAA).

3.16.4 LESSONS LEARNED

- RPs need to be aware of the need to provide a safety case for operational radiological protection and not just focus on the risk to the public from reactor fault conditions. RPs require competent staff and an adequate strategy & plan in place in order to deliver the radiological protection aspects of the safety

case. An important element of this is a thorough demonstration that radioactive source terms are ALARP, including reference to RGP at comparable plants.

- Note also that a generic approach to ALARP based around the requirement to reduce risk to the public from fault conditions cannot necessarily be applied to occupational radiological protection of workers during normal operations. This is because a suitable ALARP process for occupational exposure needs to enable assessment of the viability of options involving minor changes, such as the route of a single pipe or service conduit or the measurement range of one instrument, that result in small but worthwhile reductions in occupational exposure.
- Sufficient emphasis must be placed on the need to control radioactive contamination in the workplace and hence reduce internal radiation exposures to levels that are ALARP. It is also important to note that some radioactive isotopes such as tritium and those in the actinide series contribute very little to external radiation, but can be significant contributors to internal radiation and so must not be overlooked when defining source terms.
- The hierarchy of controls (IRR 17 regulation 9(2)) needs to be demonstrably applied to both the control of worker access and the need for worker access to high radiation dose rate areas of the plant.

3.16.5 REFERENCES

493. Ionising Radiations Regulations 2017 (IRR 17) Approved Code of Practice and Guidance (L121):

- Document L121 includes ACOP and statutory Guidance on practical implementation of the regulations (http://www.hse.gov.uk/pubns/priced/l121.pdf). All aspects of these regulations will apply to NPP operation hence are relevant for GDA, however regulations of particular note are identified in the next section.
- Document L121 features the absolute legal requirements of IRR 17, accompanied in each section by appropriate elements of the ACOP and Guidance. The ACOP has special legal status. If a RP complies with the ACOP, then legally they are deemed to have met the requirements of the law. Guidance, which is identified separately, represents what the regulator considered to be good practice when complying with the law.

494. Notable IRR 17 Regulations for GDA:

495. As stated in the previous paragraph, all aspects of IRR 17 are of relevance to GDA; however there are some regulations that are of particular note for GDA as follows:

- Regulation 2 – Interpretation
  This regulation gives definitions of terms (such as “dose” and “external radiation”) used throughout IRR 17.
- Regulation 3 – Application
  This regulation defines where (what types of premises) and to what (what sort of activities) IRR 17 apply.
- Regulation 9 - Restriction of exposure
  This is one of the key parts of IRR 17 and contains far more supporting text (ACOP and Guidance) than any other individual regulation. It includes the absolute legal requirement to restrict doses So Far As Is Reasonably Practicable (SFAIRP), introduces the concept of hierarchy of controls and gives specific examples of the use of engineering controls and safety features and warning devices. It also describes the use of dose constraints for occupational exposure and for members of the public in addition to other requirements.
- Regulation 12 – Dose Limitation

This regulation defines legal dose limits for various classes of employee and members of the public.

- Regulation 17 - Designation of controlled or supervised areas
  This regulation gives the criteria for the official designation of areas where work with radiation is taking place.
- Regulation 19 – Additional requirements for designated areas
  This regulation states some of the minimum requirements for areas that have been designated as a result of Regulation 17 requirements. This includes specification of requirements for physical demarcation of the areas, control of access and changing and washing facilities.
- Regulation 20 – Monitoring of designated areas
  This regulation includes requirements for monitoring equipment, including installed monitoring equipment required in response to knowledge of the radiological environment.
- Regulation 28 - Sealed sources and articles containing or embodying radioactive substances
  This regulation places duties on employers regarding the design, construction maintenance and testing of any article containing or embodying a radioactive substance.
- Regulation 30 - Regulation 30 Keeping and moving of radioactive substances
  This regulation places duties on employers regarding suitability of storage and receptacles for radioactive substances.
- Regulation 31 - Notification of certain occurrences
  This regulation gives levels at which employers must notify ONR where losses, releases or spills of radioactive material have taken place.
- Regulation 32 – Duties of manufacturers etc. of articles for use in work with ionising radiation
  This regulation places legal responsibilities on designers, manufacturers and suppliers to ensure that articles supplied for work with ionising radiation restrict exposure SFAIRP.

496. Use of RGP to address IRR17 Regulation 9 Requirements:

- For Radiation Protection in GDA, RGP can be a standard, practice or design that controls risk or dose to the extent that it has been judged and recognised by ONR as satisfying the legal requirement for doses and risks to be reduced SFAIRP.
- New designs, as a minimum, should meet the standards set by RGP. The level of safety of a new design must be no less than a comparable facility already working or being constructed in GB or somewhere else in the world. This requires designers to be outward looking, not just referencing corporate and national knowledge and experience.
- In practice, representative metrics such as dose per year, dose per outage/task or dose per GWh generated can be used to identify specific measures which have been adopted to reduce dose and thus can be regarded as RGP.
- Further where OPEX from previous plant type operation has identified specific radiological issues, means of addressing these issues would be regarded as RGP.
- Examples of RGP can be found in publications by international organisations such as IAEA (e.g. Radiation Protection Aspects of Design for Nuclear Power Plants. Safety Guide No. NS-G-1.13, IAEA 2005 http://www-pub.iaea.org/MTCD/publications/PDF/Pub1233_web.pdf), WENRA and NEA.
- The Health and Safety Executive document “Reducing Risks, Protecting People” (R2P2) is used by inspectors as an assessment guide and is also a good reference source.

3.17 SAFEGUARDS

497. Nuclear safeguards are independent measures to verify that States comply with their international non-proliferation commitments not to divert qualifying nuclear materials (plutonium, uranium and thorium), from their civil nuclear programmes, to non-peaceful end-uses.

498. ONR's safeguards role includes working to ensure that UK safeguards are met in a proportionate manner, and this will remain the case following UK withdrawal from the Euratom Treaty. The legislative framework for safeguards implementation in the UK will be significantly different, with ONR having the role of the State System for accountancy and control of nuclear materials (SSAC) instead of the European Commission, but there will continue to be requirements for the provision of safeguards information early in the design process for new facilities or projects. Further information on current UK safeguards arrangements can be found on the ONR website. Information on development of the UK safeguards regime to be in place after the UK has left the Euratom Treaty is available at the gov.uk website.

499. There is extensive experience to the effect that, just as for other regulatory areas, early consideration of safeguards requirements for any new build project (known as safeguards by design (SBD)) has benefits for all stakeholders (as noted in the IAEA documents listed in the safeguards references section 3.17.4). Examples of these benefits include minimising the risk associated with project scope, schedule, budget and licensing; and in reducing the cost of safeguards implementation to the operator, the national SSAC and the IAEA safeguards inspectorate (e.g. there have been instances where safeguards requirements have had to be either retro-fitted or been considered late in a project's development and have posed significant and costly challenges to implement).

500. Operators setting-up new facilities should provide preliminary information to ONR (the national safeguards authority) as soon as the decision to construct or authorise construction has been taken. This information (known as preliminary Basic Technical Characteristics, BTCs) should specify the facility's owner and operator, its purpose and location, the nuclear materials involved and the facility capacity and throughput, and the expected commissioning date.

501. The information is in turn declared to the international safeguards inspectorates (the IAEA and at present also the Euratom inspectorate), and is the basis for engagement with RPs and prospective operators to understand UK safeguards requirements and expectations as a basis for demonstrating how those requirements will be met.

502. Further detail should be provided no later than 200 days prior to the start of construction using the full BTC template (an example the template for a new reactor facility is included at Appendix 1).

3.17.1 SCOPE FOR GDA

503. The main areas of safeguards interest for new types of nuclear facility are for the RPs to:

- Define and agree nuclear materials accountancy and control and safeguards (NMAC&S) arrangements for the new facility, including the process and timeline for specifying and installing any surveillance, monitoring and other safeguards equipment that may be required as part of verification by the international safeguards inspectorates.
- Ensure all statutory safeguards reporting requirements (e.g. for reporting as set out in Safeguards Regulations) are met.

DOCUMENTS SUBMITTED

504. During GDA, it is expected that the documentation submitted by the RP will need to demonstrate their understanding of safeguards requirements at the generic (international/national) level and how they will be accommodated in the generic design. This includes demonstrating an understanding of the requirements:

- Arising from the UK's international commitments and national safeguards legislation.
- For the accountancy, control and reporting of nuclear material inventories and flows at the facility. Under future UK safeguards regulations this will include submission to ONR of an initial Accountancy and Control Plan (ACP).
- For supporting on-site safeguards inspections, by ONR safeguards and as necessary the international safeguards inspectorates, for physical inventory verification and facility design verification (e.g. which may include incorporating provision for containment and surveillance measures and transmission of safeguards data for use by the international inspectorates in their verification) and future ONR inspections (e.g. against the facility ACP).

505. GDA documentation and processes should ensure that, as the design for any particular facility matures into the delivery of a specific nuclear reactor site the designer/operator will need to ensure that:

- Safeguards requirements for their particular facility and its inventory of nuclear material develop in line with the design/construction programme by:
  - Ensuring there is effective oversight of the transfer of safeguards information from the GDA into the subsequent licensing and construction processes.
  - Increasing the detail of the safeguards and NMAC in line with the reactor development.
  - Setting safeguards within the overall company organisational structure and detailing roles and responsibilities within the operator's hierarchy.
  - Identifying and implementing appropriate training to support and deliver the NMAC processes.
- Safeguards provisions remain suitably robust to meet the safeguards requirements by demonstrating:
  - An understanding of how safeguards requirements at the site/facility level are met, in particular in the areas of:
    - Nuclear material accountancy and control
    - Safeguards reporting/verification
  - Delivery to the required timescales of:
    - Preliminary design information.
    - Pre-construction BTC information.
    - An ACP when required by future UK regulations.
    - How safeguards related documentation will be incorporated within the overall site documentation strategy.

3.17.2 BASIS FOR DECISION

506. Although safeguards requirements are currently not a formal part of the GDA process, experience has shown that early consideration of safeguards requirements for any new build project (not just reactors) has benefits for all stakeholders. Discussion towards, and outline agreement of, suitable safeguards arrangements, will include proportionate incorporation of the requirements described in existing safeguards guidance documents (e.g. references 3 and 4). ONR will be producing its own guidance on expectations for safeguards assessment generally, for production of future ACPs and

for future ONR inspections to assist implementation of the UK safeguards regime to be in place after the UK has left the Euratom Treaty. Until that guidance is available the national and international guidance listed in the references of this chapter should inform the assessment of the RP arrangements for nuclear materials accountancy and control and safeguards.

507. Important indicators of successful safeguards engagement will include the RP having demonstrated that the following has been considered:

- Minimising risks to the project associated with ensuring safeguards compliance.
- Optimising the effectiveness and efficiency of safeguards implementation by the operator, the national safeguards regulator and the international safeguards inspectorates.

508. Positive safeguards assessment by ONR will depend on what steps the RP has taken to acknowledge and incorporate safeguards requirements early in the design and construction phases of the project. Factors in this assessment will include the extent to which there has been:

- Early and ongoing constructive engagement between RP, designer, future operator and builder (if different from the operator), and the safeguards authorities both nationally and internationally.
- Provision of a preliminary BTC submission, and demonstration of how these will be updated as more detailed technical information on plant design and operation becomes available.
- Description of NMAC arrangements and, when required by UK legislation, an initial ACP.
- Evidence provided to show that safeguards arrangements to enable verification by the international safeguards inspectorates have been consider in the design and build phases from the start.

3.17.3 INTEGRATION WITH OTHER TECHNICAL ASSESSMENT TOPICS

509. SSCs required for accounting and control of nuclear material interact with, or can be part of, facility arrangements relating to safety and security. In order to ensure that safeguards requirements are being incorporated early in the design, the RP is expected to ensure effective interaction between relevant disciplines process to also identify early any possible areas of synergy or contrasting requirements.

510. This interaction should be initiated between the leads of the topics within the GDA process. In particular those disciplines associated with SAPs ENM 4 and 8, which are concerned with nuclear material materials accountancy and control (NMAC), a fundamental requirement for the successful safeguards implementation.

511. Similarly is also anticipated between safeguards and security (e.g. security and systems to identify theft of nuclear material, supporting SyDP6.1 and Categorisation for Theft and SyDP6.3 physical protection system design - from the SyAps referenced in section 3.17.4 will be relevant to NMAC arrangements).

512. In addition to NMAC, RPs and operators need to make provision for on-site verification by the international safeguards inspectorates. This verification can cover the nuclear materials accounts and associated supporting documentation, physical access to verify the nuclear material against the reported inventories in the safeguards reports; and the facility infrastructure compared to the Basic Technical Characteristics declarations (so called design information verification). All of these activities will benefit from early consideration as part of the facility design and build process. Any requirements for

incorporating safeguards equipment into the facility design and build may also require interactions with civil engineering and mechanical engineering disciplines.

513. Certain facility types, for example bulk processing facilities (fuel manufacture, enrichment, reprocessing etc.) or reactors using novel fuel types, may require the RP to provide for facility-specific safeguards features as part of the final agreed safeguards approach (e.g. these features may range from space for independent safeguards measurement or monitoring equipment and the associated infrastructure, to laboratory services that may be staffed by international regulators).

514. Examples of other ONR topic areas that could be involved include:

- Chemistry: sampling of nuclear material for accountancy or independent safeguard analysis/verification.
- C&I: Integration of safeguards equipment.
- Civil and mechanical engineering: for installation of safeguards equipment for containment/surveillance and remote data transmission.
- Organisational and human factors: for instance how safeguards staff are incorporated in the overall organisation structure – safeguards specific training and SQEPs.

3.17.4 REFERENCES

- Control Of Processes Involving Nuclear Matter (SAP – ENM. 1 TO 8) NS-TAST-GD-023
- SyAPs – ONR Security Assessment Principles, http://www.onr.org.uk/syaps/
- Guidance on International Safeguards and Nuclear Material Accountancy at Nuclear sites in the UK 2010 Edition, Revision 1 (http://www.onr.org.uk/safeguards/accountancy.pdf)
- International Safeguards in Nuclear Facility Design and Construction. IAEA Nuclear Energy Series NP-T-2.8 (https://www-pub.iaea.org/books/iaeabooks/10361/International-Safeguards-in-Nuclear-Facility-Design-and-Construction)
- International Safeguards in the Design of Fuel Fabrication Plants. IAEA Nuclear Energy Series No. NF-T-4.7 (https://www-pub.iaea.org/books/iaeabooks/10746/International-Safeguards-in-the-Design-of-Fuel-Fabrication-Plants)
- International Safeguards in the Design of Nuclear Reactors. IAEA Nuclear Energy Series NO. NP-T-2.9 (https://www.iaea.org/publications/10710/international-safeguards-in-the-design-of-nuclear-reactors)

3.17.5 QUESTIONNAIRE FOR THE DECLARATION OF THE BASIC TECHNICAL CHARACTERISTICS OF A QUALIFYING NUCLEAR FACILITY

515. This questionnaire has been taken from the Euratom Safeguards Regulations and draft UK Nuclear Safeguards Regulations.

516. Annex I-A. REACTORS

IDENTIFICATION OF THE QUALIFYING NUCLEAR FACILITY

517. Name, location, owner, operator, purpose and type of operation, detailed layout of the facility, detailed reactor data (power, fuel type, enrichment, coolant, moderator, thermal output)

GENERAL ARRANGEMENTS AT THE QUALIFYING NUCLEAR FACILITY, INCLUDING THOSE RELATING TO MATERIAL USE AND ACCOUNTANCY, CONTAINMENT AND SURVEILLANCE

518. Description of qualifying nuclear material

- Use of qualifying nuclear material.
- Outline drawings of fuel assemblies, fuel rods/pins, fuel plates.
- Method of identifying individual assemblies, rods/pins, plates.
- Other qualifying nuclear material used in the qualifying nuclear facility.

519. Flow of qualifying nuclear material

- Flow sheet showing: points where qualifying nuclear material is identified or measured; material balance areas and inventory locations used for material accountancy; and the estimated range of nuclear material inventories at these locations under normal operating conditions.
- Expected nominal fuel cycle data: core: loading, burn-up.
- Forecast of throughput and inventory, and of receipts and shipments.

520. Handling of qualifying nuclear material

- Layout of the fresh fuel storage area, drawings of fresh fuel storage locations, and description of packaging.
- Drawings of transfer equipment for fresh and irradiated fuel, including refuelling machines or equipment.
- Drawings of reactor vessel showing location of core and openings in vessel; description of method of fuel handling in vessel.
- Number and size of channels for fuel assemblies and control devices in the core.
- Spent fuel storage area.
- Coolant flow diagrams as required for heat balance calculations.

ACCOUNTANCY AND CONTROL OF QUALIFYING NUCLEAR MATERIAL

521. Accountancy system

- Description of accountancy and control system for qualifying nuclear material (describe item and/or mass accountancy system, including assay methods used and assessed accuracies, supplying specimen blank forms used in all accountancy and control procedures).

522. Physical inventory

- Description of; procedures, scheduled frequency and methods for operator's physical inventory taking (both for item and/or mass accountancy, including main assay methods and expected accuracy); access to qualifying nuclear material in the core and to qualifying nuclear material which is irradiated and outside the core; expected radiation levels.

OTHER INFORMATION RELEVANT TO APPLICATION OF SAFEGUARDS

523. Organisational arrangements for material accountancy and control.

524. Information on the health and safety rules which have to be observed at the qualifying nuclear facility, and with which the inspectors must comply.

3.18 SECURITY

525. The objective of this document is to provide guidance to security inspectors and RPs on ONR's expectations for GDA within the security discipline.

526. This topic-specific guidance is to provide clarity on key areas of interest to ONR during GDA in each of the disciplines and is not intended to replace the TAGs.

3.18.1 SCOPE FOR GDA

527. The expectation for GDA is that the RP will submit a GSR to ONR which describes the security features of the reactor technology being assessed. Importantly, it should document the categorisation of Nuclear Material (NM) and Other Radioactive Material (ORM) from both theft and sabotage in order to determine the protective security outcomes and applicable security postures to be applied. Similarly, it should also identify and characterise equipment or software utilised on the premises in connection with activities involving NM/ORM in order to determine the cyber security outcomes and applicable cyber security postures to be applied. It is therefore important that inspectors carry out their assessment recognising that the security arrangements detailed in the GSR must be able to meet regulatory expectations, in respect of the Security Assessment Principles (SyAPs) Fundamental Security Principles (FSyPs), in order that a future site-specific security plan can be developed.

DOCUMENTS SUBMITTED

528. The number and the level of detail in the documents submitted by the RP can vary.

529. The following is considered RGP:

- A Preliminary Security Report; this may form a part/chapter of the PSR and is the first document to be provided within GDA.
- A GSR outline structure document that may explain a 'tiered' approach with the GSR at Tier 1 and other supporting documents at Tier 2.
- Generic plant layout document to a level of detail that includes the fabric of the building and access routes.
- A Vital Area Identification methodology and subsequent study that uses the UK Design Basis Threat (DBT).
- A Cyber Risk Assessment that explains how nuclear technology and specifically Computer Based Systems Important to Nuclear Safety (CBSIS) will be protected. Identification and categorisation of Operational Technology and Information Technology should allow a RP to design an effective cyber protection system.
- Finally a GSR that summarises the VAs and operational technology that need to be protected within a high level concept of operations that outlines how security risks are designed-out and remaining risks might be mitigated by designing-in security commensurate with the maturity of the design. The GSR should then inform, in sufficient detail, any future licensee in the development of a Site Security Plan.

KEY ASSESSMENT TOPICS

530. In conjunction with ONR Security Informed Nuclear Safety (SINS) team, the security inspector will typically start the review by ensuring that the RP has a technical understanding of the VA methodology as expanded above, to inform the development of the VAI study, upon which much of the protective security architecture will be designed for the purposes of GDA. The inspector should ensure that the RP has

identified all relevant FSyPs and Security Delivery Principles (SyDPs) and effective processes are in place to achieve key principles including:

- Secure by Design - The underpinning aim should be an inherently secure design, consistent with operational purposes and where security has been considered from the initial design stage.
- The Threat - Protection systems should be designed evaluated and tested using the state's (DBT).
- The Graded Approach - Protection systems should be based on a graded approach, taking into account the categorisation for theft or sabotage of NM/ORM, and the consequence of compromise of any Sensitive Nuclear Information (SNI).
- Defence in Depth - Protection systems should reflect a concept of several layers and methods of protection, preferably independent of each other, that have to be overcome or circumvented by an adversary and ensure appropriate mitigation of security events should prevention fail.
- Security Categorisation - The security functions to be delivered at a dutyholder's site and facilities, in all modes of operation, should be identified and then categorised based on their significance with regard to security.
- Security Classification - SSCs that have to deliver security functions should be identified and classified on the basis of those functions and their significance to security.
- Codes and Standards - SSCs that are important to security should be designed, manufactured, constructed, installed, commissioned, quality assured, maintained, tested and inspected to appropriate codes and standards.

SAMPLING AREAS

531. The above section provides a description of the scope of the assessment usually carried out in GDA. During the detailed review, the security inspector may decide to adopt a sampling approach in some areas. The sampling needs to be done in a focused, targeted and structured manner with a view to revealing / identifying any specific or generic security weaknesses.

532. The security inspector will (normally) assess each of the main technical areas considered essential to produce a full scope GSR in line with the Security GDA TAG.

- Assessing the RP's arrangements for managing security to confirm that they have the appropriate strategic enablers in place to support the development of a high quality GSR.
- Assess the format, layout and proposed contents list of the GSR.
- Assess the application of the VAI methodology.
- Validate those VAs and their categories that have been identified.
- Examine overarching security claims and general "defence in depth" security measures.
- Confirm the identification of Computer Based Systems Important for Safety (CBSIS).

3.18.2 BASIS FOR DECISION

STANDARDS AND GUIDANCE

533. ONR's SyAPs constitute the regulatory principles and expectations against which duty holders' security arrangements are assessed. Civil Nuclear Security (CNS) has produced a number of TAGs to support security assessment, but the following TAGs are key to GDA assessment

- CNS-TAST-GD-11.1 (Rev 0) Security Assessment in GDA.
- CNS-TAST-GD-7.3 (Rev 0) Protection of Nuclear Technology & Operations.
- CNS-TAST-GD-7.1 (Rev 0) Effective Cyber and Information Risk Management.
- CNS-TAST-GD-6.2 (Rev 0) Target Identification for Sabotage.
- CNS-TAST-GD-6.3 (Rev 0) March 2020 Physical Protection System Design (Official-sensitive).

534. It is accepted that for a less mature design, the level of detail of the GSR submitted during the early phases of the review (e.g. the fundamental step) will be commensurate with the level of detail of the design. The GSR should address the expectations of SyAPs and the security outcomes based on the categorisation of the design in respect of theft and sabotage (including cyber-attack). CNS TAGs provide clear guidance on ONR expectations. Further guidance and standards can be found in the References section below.

3.18.3 INTEGRATION WITH OTHER TECHNICAL ASSESSMENT TOPICS

535. It is recognised that during GDA there will be a need to consult with other ONR inspectors as part of the security assessment process. Similarly, other inspectors will seek input from security. These interactions are important and every effort should be made to identify cross cutting topic areas between security and other technical areas.

536. Also, it should be noted that the interactions between security and some technical areas will need to be formalised since aspects of the assessment in those areas constitute formal inputs to the security assessment. Close consultation is often associated with:

- Internal hazards.
- External hazards.
- C&I.
- Fault studies.

Security may also interact with other disciplines, such as: conventional fire, human factors and safeguards.

3.18.4 LESSONS LEARNED

537. There have been three GDAs completed in GB and as a result there are a number of lessons learned for new GDA inspectors and for the RPs.

- Early establishment of processes for the production, storage and transmission of SNI is vital to facilitate the smooth exchange of GDA information. This will require the involvement of ONR CS&IA inspectors, BEIS and Cabinet Office (coordinated by ONR).
- Early establishment of security vetting requirements (particularly for foreign RPs) to facilitate handling and production of protected material and information.
- Foreign RPs may not always be familiar with the process for the identification of VAs and early discussion with SINS inspectors may avoid potential delay or misunderstanding.
- The UK DBT is protected SECRET UK/US Eyes Only. Consequently the RP may require the services of a UK based design engineering consultancy company to support the VAI work.
- The adequacy of the processes to develop and use the VAI study, to inform design development (including design changes). Establishing these processes early helps the RP to record evidence in an adequate way from the beginning, avoiding inefficiencies and iterations.

3.18.5 REFERENCES

- Prevailing UK DBT
- IAEA - Nuclear Security Series No. 13. Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Rev 5)
- IAEA - Nuclear Security Series No. 4. Engineering Safety Aspects of the Protection of Nuclear Power Plants Against Sabotage

3.19 SEVERE ACCIDENT ANALYSIS

538. Consistent with the principle of defence of depth, ONR has an expectation that events more severe than those considered within the design basis are managed through the provision of equipment and procedures that can control or mitigate the consequences. For GDA, this means that beyond design basis events with plant damage states where the potential consequences are severe should be considered in the safety case.

539. This consideration needs to be a complementary mix of deterministic and probabilistic analysis. The topic area ONR has considered under the heading of “severe accident analysis” is predominately focused on the deterministic portions of the RP’s safety case demonstration. Level 2 and Level 3 PSA will consider the probabilistic aspects.

3.19.1 SCOPE FOR GDA

540. ONR’s technology neutral SAPs define a severe accident as:

“those fault sequences that could lead either to consequences exceeding the highest off-site radiological doses given in the BSLs of Numerical Target 4 (i.e. 100 mSv, conservatively assessed) or to an unintended relocation of a substantial quantity of radioactive material within the facility which places a demand on the integrity of the remaining physical barriers. A substantial quantity of radioactive material is one which if released could result in the consequences specified in the societal risk Target 9.”

541. In the specific context of a new NPP being considered in GDA, severe accident analysis can be considered consistent with the IAEA (Ref SAA.1) and WENRA (Ref SAA.2) expectations for deterministic analysis of design extension conditions associated with core damage (so called ‘DEC-B’ analysis). There are several objectives for the analysis undertaken by the RP, including:

- Demonstrate an understanding of phenomena and risks.
- Demonstrate defence in depth.
- Identify performance and environmental qualification requirements for equipment.
- Identify mission times and stocks of inventories.
- Demonstrate learning from Fukushima and other accidents.
- Support PSA modelling.
- Inform emergency procedures.
- Demonstrate that risks are ALARP.
- Demonstrate that large or early releases have been practically eliminated.

IDENTIFICATION OF PLANT DAMAGE STATES AND ASSOCIATED PHENOMENA

542. Using a combination of engineering judgement, analysis, historic experience and RGP (and in close collaboration with the PSA topic area), the RP should identify appropriate plant damage states and sequences for deterministic analysis. These sequences should be selected to represent all the main physical phenomena associated with extensive fuel damage. All operating modes of the reactor should be considered, as

well as any other facilities or activities that have the potential for a severe accident, for example the spent fuel pool.

543. The plant damage states and associated phenomena identified will be technology and design dependent. For the design being considered, some phenomena may be claimed to be physically impossible; the RP should substantiate such assertions with appropriate analysis, discussion and potentially with reference to experimental results and research. Plant damage states and sequences with the potential to challenge the containment, resulting in a risk of a large or early radioactive release should be subject to particular attention, including the following accident categories:

- Prompt reactor core damage and consequent early containment failure, such as from failure of a large pressure-retaining component or uncontrolled reactivity accidents.
- Early containment failure, such as highly energetic direct containment heating, large steam explosion or explosion of combustible gases.
- Late containment failure such as basemat penetration or containment bypass during molten core concrete interaction, long term loss of containment heat removal or explosion of combustible gases.
- Containment bypass due to leakage, consequential failures or open containment states.
- Significant fuel degradation in a storage fuel pool and uncontrolled releases.

IDENTIFICATION OF SSCs

544. Regardless of what has occurred for the facility to get into a degraded state, the expectation for a modern NPP is that there is design provision so that it can be placed in a safe and stable condition with radiological consequences mitigated to ALARP.

545. The SSCs included in the design for severe accidents could vary greatly from one reactor technology to another. All reactor technologies considered in previous GDAs have adopted different approaches, for example on the extent of claims made on active or passive SSCs, or fixed and mobile equipment. However, the design provision needs to consider the fundamental safety functions of reactivity, cooling and containment.

546. The RP's submissions should facilitate interactions with ONR on:

- The independence of the identified severe accident SSCs from other levels of defence of depth which are likely to have already failed or been bypassed.
- The appropriateness of the classification applied to the identified severe accident SSCs.
- The qualification of the identified severe accident SSCs to deliver the required functions in conditions expected to be experienced during the severe accident.
- The sizing of the SSCs such that they are sufficient to deliver the identified safety functions.
- The time required to initiate the SSCs recognising the complexity/difficulty of operation.
- The support systems needed to initiate and maintain the operation of the SSCs (for example, C&I, AC and DC power, heat sinks etc.)
- The mission times and stock requirements (e.g. water, fuel, DC power) for severe accident SSCs and their associated support systems.

ANALYSIS TECHNIQUES

547. The RP's submission should include analysis of severe accident scenarios to support claims made in the safety case such as:

- The reactor can be brought into a state where the containment functions can be maintained in the long term.
- The SSCs (e.g. the containment) and procedures are capable of preventing a large radioactive release or an early radioactive release, including containment bypass.
- Control locations remain habitable to allow performance of required staff actions.

548. Acceptance criteria will need to be established by the RP for this analysis, including radiological criteria and technical criteria for aspects such as containment integrity and hydrogen concentration. A best-estimate approach should normally be followed for the analysis, and acceptance criteria are likely to be relaxed compared to DBA. However, where uncertainties are such that realistic analysis cannot be performed with confidence, a conservative approach should be adopted. IAEA's guidance on deterministic analysis (Ref. SAA.4) is a useful for reference on analysis methods.

549. Predictions of the timings for key events in the progression of a severe accident are another outcome from analysis. It is usual for unmitigated analysis to be performed initially, before the same scenario is run again crediting the performance of severe accident SSCs. This analysis is important for informing emergency arrangements and providing credibility for claimed operator actions. It is unrealistic to expect uncertainties in timings to be eliminated, but the sensitivity of the recommended operator actions, design provisions and PSA results to such uncertainties should be considered.

550. For the light water reactors considered in GDAs to date, extensive use of the MAAP computer code has been made by the RPs. ONR has undertaken limited independent confirmatory analysis of a sample of scenarios using the MELCOR code. ONR does not prescribe what codes the RP should use, nor is it committed to one particular code for its independent confirmatory analysis. However, the use of MAAP by the RP and MELCOR by the regulator is consistent with practice in other countries, and therefore can be helpful for leveraging insights for overseas assessments.

551. In previous GDAs, both ex-vessel and in-vessel accident management strategies have been put forward by RPs, and ultimately accepted by ONR. The two "rival" strategies each have significant uncertainties associated with them, remain areas of on-going research, and attract both support and criticism in the severe accident community. Whichever option is favoured by the RP, it should expect to receive significant regulatory attention from ONR.

552. As with all analysis models used in support of safety cases, ONR should assess the verification and validation provided by the RP against the principles set out in SAPs AV.1 to AV.8 (Ref. SAA.3). For some phenomena, credit can be taken for the extensive benchmarking and worldwide research that has gone into codes like MAAP. However, the applicability of a code, or a module of a code, to the reactor design and plant damage state in question needs to be justified. Some phenomena will be very design specific or will be an area of significant physical or analytical uncertainty. In these cases, the RP's evidence will be strengthened by reference to actual accident experience or test rig data.

553. Although codes like MAAP and MELCOR have the capability to model a wide range of phenomena, there may be phenomena which require additional modelling, such as hydrogen modelling with computational fluid dynamics methods. This is acceptable, but these methods also need to be appropriately verified and validated, and may attract additional regulatory attention (depending on the significance of the results to the safety case).

554. Undertaking independent confirmatory analysis has been a valuable method for ONR to gain additional insights into the RP's analysis. It can reveal the impact of user effects and model sensitivities on key claims in the analysis. The ability of RP to supply data and explain modelling assumptions (compared against ONR's TSC's choices) is a good way to form a view on its quality control and analysts' experience.

555. Whilst ONR may choose to undertake its own independent confirmatory analysis through TSCs, it is important to recognise that it is the RP's analysis that needs to demonstrate the safety of the reactor. The objective of ONR's analysis is to gain confidence in what the RP has done and probe for areas where additional substantiation may be needed; it is not intended to replace or rival what the RP has done.

EMERGENCY ARRANGEMENTS AND PROCEDURES

556. There is no expectation in GDA that the RP provides detailed emergency arrangements or procedures. These will be a matter for a future licensee. However, appropriate principles and assumptions for accident management need to be put forward, with a strategy for how these will be developed into arrangements and procedures that are consistent with RGP. Requirements and constraints for future arrangements that follow from the GDA safety case (whether that is from deterministic or probabilistic analysis) should be identified. In previous GDAs, the generic procedures or examples from other similar plants have been useful to ONR.

ALARP AND PRACTICAL ELIMINATION

557. Demonstrating that the supplied severe accident design provision reduces risks to ALARP, and that it would be grossly disproportionate to do more will be a challenging but vital part of the RP's submission.

558. The nature of severe accidents is such that additional design features are likely to be expensive but they would only be called upon for very low frequency scenarios. Cost-benefit analysis techniques may therefore be of limited value in decision making. RGP has a role to play, however it is not always clear what this looks like in areas of high uncertainty and technology-specific approaches. Decisions and choices made in previous GDAs do not necessarily apply to a new reactor technology going through GDA.

559. The learning from the Fukushima Daichi accident did re-baseline what constitutes RGP (both in terms of design provision and analysis methods). Updated guidance and design improvements implemented into operating facilities should inform judgements on what can and should be done; something that has been successfully implemented elsewhere must have been practicable and judged by at least one organisation not to be grossly disproportionate. In some cases, it will be reasonably practicable to provide greater levels of resilience and defence-in-depth on a new power plant still being designed, than it is with an existing facility with a limited operating life. However, it may also be possible to achieve higher levels of safety on a new plant with alternative approaches (perhaps more elegant and cheaper) through innovative design and analysis.

560. The results of PSA and comparisons against core damage frequency, large release frequency and SAPs numerical targets 8 and 9 will provide valuable context for ALARP judgements made by both the RP and ONR. However, there may still be ALARP improvements that could be made after the PSA evaluation has been exhausted. For example, it is still possible to optimise instrumentation, situational awareness, ease of deployment, etc. even if these factors are not modelled in the PSA.

561. It has become RGP for new reactor designs to 'practically eliminate' large or early releases. This expectation is set out in IAEA guidance (Ref SAA.1), WENRA guidance (Ref SAA.2) and ONR's SAPs (Ref SAA.3). Ref SAA.1 provides a high level and unquantified definition of what these releases are:

- An 'early radioactive release' in this context is a radioactive release for which off-site protective actions would be necessary but would be unlikely to be fully effective in due time.
- A 'large radioactive release' is a radioactive release for which off-site protective actions that are limited in terms of lengths of time and areas of application would be insufficient for the protection of people and of the environment.

562. It also defines practical elimination as "physically impossible for the conditions to arise or if these conditions could be considered with a high level of confidence to be extremely unlikely to arise".

563. Practical elimination is a relevant concept for the designers when they are at the early stages of developing their reactor technology. Key decisions on how high levels of nuclear safety will be achieved will have probably already been made long before the RP submits its design for GDA. In the GDA submissions to ONR, it is expected that the RP will put forward claims, arguments and evidence for both the phenomena and scenarios that it claims to be impossible in the design, and those which are extremely unlikely because of the engineering provision. This may require early design choices and historic interactions with overseas regulators to be re-examined and explained.

564. At the point at which the design has reached sufficient maturity to enter a full-scope GDA, the demonstration of practical elimination should be wide ranging and multi-faceted. The nature of the demonstration to show practical elimination with a high degree of confidence can and should vary based on the scenario in question, but may comprise one or more of the following:

- Arguments for the existence of multiple levels of defence in depth, demonstrated through DBA, PSA, and analysis of design extension conditions.
- Where the event bypasses all intermediate lines of defence and proceeds straight to a severe accident, DEC-B analysis is expected to be the basis of arguments for why the provided design provision is sufficient to ensure there is a margin to large or early releases.
- Manufacturing methods, quality, code compliance and inspection arguments may be made for incredibility of failure claims (for example for catastrophic reactor pressure vessel failure).
- Analysis and argument will be needed to justify claims of physical impossibility.

565. It is highly unlikely that all scenarios that could result in large or early releases will be shown to be physically impossible. So there will remain a theoretical possibility that the engineered provision to prevent large or early releases will fail. This should be recognised in the (Level 2 and 3) PSA. ONR does not set a frequency threshold for what is acceptable for these sequences (for practical elimination) but the RP should complement its deterministic arguments (showing the effectiveness of the successful operation of claimed measures) with a probabilistic consideration of the residual risk from a large or early release.

566. Practical elimination arguments are needed for all radioactive hazards and activities on the NPP site with the potential for large or early releases. This includes shutdown reactor modes and the spent fuel pool, which can be associated with an open containment (or even no containment). Scenarios in these operating modes and facilities cannot be dismissed on frequency grounds. Deterministic arguments based on the robust defence-in-depth and large margins to failure are likely to be credible,

complemented by probabilistic arguments which put the likelihood of a large or early release in the wider context of the overall risk for the NPP.

POST-FUKUSHIMA LESSONS LEARNED

567. The accident at Fukushima Daiichi in 2011 prompted wide ranging reviews of nuclear safety with implications for most topic areas, and with notable significance for the severe accident topic area. Previous GDAs commenced before or shortly after the Fukushima accident, and therefore ONR placed specific actions on RPs to review their designs against the then still emerging lessons contained in sources such as: HM Chief Inspector of Nuclear Installations Final Report (Ref.SAA.5), European Nuclear Safety Regulators Group Stress Tests (Ref. SAA.6) and the IAEA Director General's Report (Ref. SAA.7).

568. In the recent years, the lessons identified have been consolidated into revised ONR and international guidance, as well as industry practice. ONR inspectors will be looking to gain confidence that the RP has appropriately taken into account relevant learning from Fukushima (and earlier accidents such as Three Mile Island or Chernobyl). The level of confidence gained through the review of initial submissions and interactions with the RP should inform what additional information is requested. If the RP can show that its design and safety case has been benchmarked against the latest guidance, nothing further may be required. However, if no mechanism for review and incorporation of learning is evident, an explicit demonstration against the notable Fukushima reports may be required.

DOCUMENTS SUBMITTED

569. The main claims for severe accidents and a summary of the supporting substantiation should be reported in the top level safety submission (expected to be the PCSR or equivalent head document) provided during the GDA. This almost certainly will be in its own section/chapter, or at least clearly demarcated from the main fault studies and PSA sections.

570. ONR inspectors will need to sample supporting documentation, for example analysis reports, details of severe accident SSCs, and descriptions (and associated validation evidence) for the computer codes and modelling methods used.

571. It is important that the engineering requirements coming from severe accident analysis are reflected in the relevant engineering sections of the PCSR or equivalent safety case document and supporting engineering references (i.e. descriptions of functional and qualification requirements should not be restricted to design basis scenarios if a SSC has role to play in severe accidents).

3.19.2 BASIS FOR DECISION

572. The starting point for ONR's assessment will be the FA series of SAPs (notably FA.15, FA.16 and FA.25), together with the expectations set out in the associated TAG (Ref SAA.8). The modelling submitted by the RP will be assessed against the AV series of SAPs (Ref SAA.3).

573. As discussed above, the RP needs to demonstrate in its submissions why it is satisfied it has reduced risks to ALARP, and ONR needs to reach a judgement of the adequacy of this demonstration. ONR's judgements should be informed by the guidance to inspectors provided in NS-TAST-GD-005 on ALARP (Ref SAA.9), and the report on risk informed regulatory decision making (Ref SAA.10).

574. The deterministic severe accident analysis undertaken by the RP will have a significant contribution to make to its Level 2 and Level 3 PSA modelling. However, the PSA results will also have an important role to play in providing context and a framework for ONR judging the adequacy of presented severe accident ALARP arguments. Therefore, the RP needs to link the relevant sections of its safety case together, and ONR's inspectors in the two areas will work in close cooperation.

575. Severe accident modelling will always be an area of high uncertainty. ONR inspectors should not expect the same level of conservatism and confidence as can be provided in other areas of the safety case, and should not expect the RP to resolve technical issues that have evaded others. However, the highest expectations of quality, along with a recognition and allowance for uncertainty are still to be expected. It needs to provide and use the best information possible to inform the design and future emergency arrangements, but should not be a research project.

576. ONR will be looking for evidence that the RP has suitable experience to run analysis codes, that the codes are being applied appropriately for its reactor design, that any limitations in aspects of the modelling are understood, that the RP is able to interpret the results, and that it has an appreciation of any residual uncertainty in the predictions.

577. Whilst ONR inspectors will take a sampling approach, it is likely all the high level claims made in the top level safety submission (expected to be the PCSR or other safety case document) will be considered and the overall risks / ALARP claims for the NPP taken into account. A selective "deep slice" approach can be taken to look at the detailed evidence, for example to form a view on the credibility of the overall analysis by just considering a small number of plant damage states. The sampling approach will be informed by a range of factors such as engineering judgement, past experience, uncertainty in phenomena, significance of phenomena to the safety case and work is assessed in other topic areas.

3.19.3 INTEGRATION WITH OTHER TECHNICAL ASSESSMENT TOPICS

578. As discussed in preceding sections, both the RP's work and ONR's assessment in the severe accident topic area will need to be undertaken in close cooperation with the PSA topic area.

579. It is expected that deterministic analysis of design extension conditions without significant fuel damage (DEC-A) will be considered as part of the fault studies topic area due to the similarity of the codes and methods used, while DEC-B type scenarios will be assessed in the severe accident topic area. To demonstrate that large or early releases have been practically eliminated, claims and arguments made in the severe accident topic area are likely to take credit for demonstrations of the effectiveness of defence-in-depth measures considered in the fault studies area.

580. There will need to be cooperation with the civil engineering and structural integrity topic areas when considering containment and reactor pressure vessel design requirements and resilience in severe accidents. This will also consider arguments on the likelihood of a catastrophic failure of the spent fuel pool.

581. Where active measures are claimed, C&I systems need to be available to actuate and monitor them. It is important that they are not compromised by earlier failures that resulted in an initiating event escalating to a severe accident, and they also need to be qualified to work in the environmental conditions expected. There will therefore need to be close integration between the C&I and severe accident topic areas. Similar interfaces will be needed with the mechanical engineering area.

582. Given that definitive emergency procedures, final control room design, manning levels and site-specific deployments of emergency equipment are outside of scope of GDA, detailed human factors assessment of severe accident operator claims cannot be undertaken. However, a proportionate consideration by the human factors discipline is likely to be necessary to ensure that any claims made on operators in response to severe accidents are credible.

583. Extreme external hazards such as seismic events have the potential to initiate severe accidents and to compromise the ability of claimed systems to respond during the management of the resulting plant damage state. Margin analysis beyond the GSE design basis is now an expectation in the external hazards area and therefore is likely to be reported outside of the severe accident portion of the safety case. However, there does need to be clear links between the external hazards and severe accident areas, regardless of where different aspects are reported.

584. To understand how the fuel fails in a severe accident, how the released inventory can relocate from the reactor or spent fuel pool to the environment will require interactions with the chemistry, fuel and core and radiological protection topic areas.

3.19.4 LESSONS LEARNED

585. The following list details some additional specific pieces of learning from earlier GDAs:

- Thought needs to be given to what can be done in GDA compared to site specific analysis undertaken at a later date. Emergency procedures/arrangements, layouts etc. will be matters for a future licensee. However, arguments to substantiate or expand upon in a site-specific safety case can be put forward in GDA. Some assumptions on mobile equipment or operator actions will be taken will need to be made in GDA, even if final design choices are not made.
- The need to demonstrate Practical Elimination is now established in the SAPs and international guidance. Whilst there are international initiatives to develop further guidance, there are no algorithms or systematic set of requirements to follow. The RP should review available information and precedents, and develop approaches and criteria that are appropriate for its technology, and discuss these with ONR.
- Major design features which are either fundamental to accident management strategy or are notable by their absence will inevitably attract a lot of regulatory attention. For example, if core catchers, in-vessel retention, passive autocatalytic recombiners or filtered containment venting are part of the approach, the RP will need to demonstrate their effectiveness. If they are not included, the RP can expect to be asked to explain why they are not part of their strategy (given that others have considered them to be RGP) and demonstrate why it would be grossly disproportionate or be of no benefit to nuclear safety to include them.

3.19.5 REFERENCES

- SAA.1 IAEA, Safety of Nuclear Power Plants: Design, SSR-2/1, Revision 1
- SAA.2 WENRA RHWG, Safety of new NPP designs, March 2013
- SAA.3 Safety Assessment Principles for Nuclear Facilities, 2014 Edition, Revision 0
- SAA.4 IAEA, Deterministic Safety Analysis for Nuclear Power Plants, SSG-2, Revision 1
- SAA.5 Japanese earthquake and tsunami: Implications for the UK nuclear industry - Final Report, HM Chief Inspector of Nuclear Installations
- SAA.6 European Nuclear Safety Regulators Group (ENSREG) Stress Tests

- SAA.7 IAEA Director General's Report on the Fukushima Daiichi Accident
- SAA.8 ONR, TAG - Severe Accident Analysis, NS-TAST-GD-007, Revision 3
- SAA.9 ONR, TAG - Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable), NS-TAST-GD-005, Revision 9
- SAA.10 ONR, Risk informed regulatory decision making, June 2017

3.20 STRUCTURAL INTEGRITY

586. ONR's structural integrity assessment covers the engineering assessment of the integrity of metallic and non-metallic structures and components. Structural integrity 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 techniques.

587. In ONR, the structural integrity discipline primarily considers the confinement safety function associated with pressure boundary components, internal structures in these components, and other support structures. ONR's structural integrity assessment therefore includes the design, construction, operation, maintenance and decommissioning of a wide range of structures and components.

588. The emphasis in structural integrity assessment is placed on reducing risk at the design stage. In particular, by influencing improvements, where appropriate, in the design provisions for achieving structural integrity along with developing the RP's understanding of ONR's expectations. In addition, the most safety significant and life limiting structures and components often fall within the remit of the structural integrity discipline.

589. ONR's approach to structural integrity in some areas is likely to be philosophically different to approaches employed by experienced RPs. These areas are outlined below.

3.20.1 SCOPE FOR GDA

590. For structural integrity, the RP should identify the structures and components within the scope of GDA. Typically these include, but are not necessarily limited to, pressure vessels, boilers, pressure parts, tanks, coolant circuits, pipework, core support, pumps, valves, storage tanks, and the freestanding metal shell of pressure retaining containment structures. The scope of structural integrity assessment may also include metal pressure boundary penetrations and metal linings of concrete containment, but not the concrete structures as a whole, which are assessed by ONR's civil engineering discipline.

591. The principal means of identifying the level of structural integrity demonstration is via a process of establishing the effects of the consequences of gross failure on the delivery of nuclear safety functions, which informs the classification of SSC. ONR's assessment is based on the consideration of the consequences (direct and in-direct) of postulated gross failures rather than partial failures as gross failure usually represents the limiting situation. ONR has some specific expectations for structural integrity, which are, in part, derived from precedents in GB. These expectations are unique and are often unfamiliar to RP's. These include the concept of highest reliability structures and components. The identification of structures and components for which the RP claims highest reliability is fundamental to informing the scope and rigour of ONR's assessment (Section 2).

DOCUMENTS SUBMITTED

592. The RP's documentation, justifying the structural integrity of structures and components, should provide the safety case that links the integrity provisions to the safety significance, design and construction, and safety management arrangements. It is expected to include the following:

- The safety functional requirements of the structures and components.
- Demonstrations of the application of the categorisation and classification adopted in the wider safety case to structures and components. This should accommodate and take cognisance of structural integrity matters such as: the consequences (direct and indirect) of postulated gross failures; defence in depth provisions; reliability claims; including the identification of highest reliability claims.
- The consideration of interactions between structural integrity and other disciplines, in particular, fault studies and internal hazards to underpin structural integrity classification and chemistry for materials selection.
- A demonstration that the structural integrity provisions in codes and standards for design, construction and inspection are suitable and sufficient i.e. they have an adequate basis and are applied appropriately. If these are not demonstrably suitable and sufficient, the submissions should include the measures to be taken.
- The design philosophy for structures and components, including design principles, descriptions, loadings, design codes and standards, materials, construction, inspection, testing, and operating limits.
- The design provisions for access and design for inspectability along with the strategies for inspections during manufacture, pre-service and in-service.
- The basis for confidence in achieving the design intent, including specifications, standards, arrangements for manufacture, design documentation and design control arrangements.
- Limits and conditions for operation – The basis for establishing a set of limits on operation which will inform the operating envelope consistent with the nuclear safety case and the design and manufacturing provisions for structures and components.
- The design provisions for ageing management, including materials surveillance, archiving arrangement, component replacement strategies, and decommissioning.
- The plant layout in sufficient detail to allow the inspector to understand potential areas of interaction between structural integrity and other topic areas e.g. internal hazards.
- The basis of the safety case including the additional measures beyond normal practice defined in codes and standards that will underpin highest reliability claims for structures and components.
- The basis for the avoidance of fracture demonstrations for highest reliability including provisions for the integration of defect tolerance assessment, with conservative material properties, and high reliability manufacturing inspections.
- A demonstration that the risks for nuclear and conventional safety are reduced ALARP.

593. ONR expects that there is suitable and sufficient evidence to infer that the level of structural integrity demonstration is commensurate with the importance of the structure or component to nuclear safety. The structural integrity classification process and the linkage to the assignment of appropriate design, construction and inspection codes are therefore important. In addition, if the RP claims highest reliability, ONR expects additional measures beyond normal practice i.e. the provisions of established nuclear design, construction and inspection codes.

594. ONR does not prescribe how a structural integrity case is presented. The structural integrity case for Sizewell B set a precedent for the inference of high levels of structural integrity. The case comprised two aspects:

- 'Achievement of integrity' based on compliance with an established design, construction and inspection code (supplemented with additional measures in design, quality assurance, materials and inspection).
- 'Demonstration of integrity' with the emphasis on showing defect tolerance with the support of validated (qualified) inspections.

595. For GDA, several RPs have used a multi-legged style structure as a means of showing conceptual defence in depth as advised by the UK Technical Advisory Group on the Structural Integrity of High Integrity Plant (TAGSI), (Bullough et al, see topic area References). This is merely a matter of presentation. The key point is that the RP needs to provide sufficient evidence, to show an adequate understanding of ONR's expectations, along with a basis for confidence that the inference of high levels of structural integrity is achievable during licensing. In particular, there should be provision for additional measures above normal practice to underpin highest reliability claims with the avoidance of fracture demonstration, a prominent expectation in GDA.

596. The number and the level of detail in the documents submitted by the RP can vary. However, previous RPs have found an approach based on a claims, arguments and evidence structure a useful means of presenting the linkage between the provisions for structural integrity and the safety case.

SAMPLING AREAS

597. It is seldom possible, or necessary, to assess a safety case in its entirety, therefore sampling is used to target the areas scrutinised and to improve the overall efficiency of the assessment process. Sampling within the structural integrity discipline is based on a proportionate and targeted approach with the focus on structures and components whose consequences of postulated gross failure are significant e.g. highest reliability claims and safety significant SSC.

598. For GDA, initially a "broad brush" review of all the documents provided by the RP may be undertaken followed by a more in depth "deep dive" review of topics that are significant with respect to reducing risks or are less clearly explained in the RP's safety case.

599. The structural integrity inspector will decide the areas of design that ONR will sample. ONR will seek confidence that the structural integrity provisions are commensurate with RGP. In general, RGP comprise those standards for controlling risk, judged and recognised by ONR, as satisfying the law, when applied appropriately. For structural integrity, RGP includes, for example: established nuclear design, construction and inspection codes such as the ASME Section III (and related code sections) and RCC-M. However, as mentioned above, for highest reliability, additional measures above normal practice are expected. RGP may also include approved codes of practice, IAEA standards, and WENRA reference levels etc.

600. The following list provides a number of areas that the structural integrity inspector will usually assess:

- The overall approach to structural integrity, including multi-discipline and cross-discipline interactions with other topic areas.
- Structural integrity claims on structures and components, including highest reliability claims.
- The proposed codes and standards.

- Materials testing and surveillance activities with the emphasis on structures and components underpinned by highest reliability claims and safety significant SSC.
- The structural integrity safety case strategy, including the approach to providing the beyond design code compliance justifications for highest reliability claims.
- The basis for an avoidance of fracture justification in support of highest reliably claims.
- Design summaries for the main metallic structures and components.
- Manufacturing, pre and in-service inspection (examination) and testing strategies.
- Access and design for inspectability.
- Materials selection and manufacturing (including fabrication) techniques along with the identification of through-life degradation mechanisms and an outline of the mitigation strategies to underpin the design life.
- Design documentation along with the provisions for design control.
- ALARP considerations for structural integrity.

3.20.2 BASIS FOR DECISION

STANDARDS AND GUIDANCE

601. The standard and criteria relevant to ONR's structural integrity assessment include:

- SAPs – SAPs EMC.1 to EMC.34 cover the Integrity of Metal Structures and Components, with SAP EMC.1 to EMC.3 invoked for highest reliability and the collective SAP EMC series covering design, manufacture, inspection, operation, monitoring, and analysis relevant to GDA. Other SAPs, related to the safety case, categorisation and classification, ageing and degradation, along with maintenance and inspection may inform the structural integrity assessment.

- TAGs:
  - NS-TAST-GD-016 Integrity of Metal Structures, Systems and Components.
  - NS-TAST-GD-005 Guidance on the demonstration of ALARP.
  - TAST-GD-051 The purpose, scope and content of safety cases
  - TAST-GD-067 Pressure Systems Safety.
  - NS-TAST-GD-094 ONR-TAST-GD-094 Categorisation of Safety Functions and Classification of Structures, Systems and Components.

- For IAEA guidance and standards and WENRA guidance, see the References section below.

ASSESSMENT PROCESS

602. In common with the other engineering disciplines, ONR expects a robust demonstration of physical defence in depth in the plant design. ONR's assessment is therefore based on the provision of measures for structural integrity that are consistent with the potential consequences of postulated gross failure. ONR expects a rigorous understanding of the consequences of postulated gross failure of SSC on the delivery of safety functions. This includes the consideration of both direct and indirect consequences. Direct consequences arise from the loss of flow, heat sink or containment e.g. LOCA, whereas indirect consequences arise from missiles, pipewhip, jets, over pressurisation, flooding and adverse environmental conditions etc.

603. If there are no engineered means of providing physical defence in depth via measures to prevent, protect or mitigate the consequences (direct and indirect) of a postulated

gross failure or a low failure frequency needs to be inferred, the safety case rests on avoiding the occurrence of the initiating event i.e. a highest reliability claim (to discount gross failure). A highest reliability claim is effectively a sub-set of the IAEA and WENRA concept to 'practically eliminate' large or early releases for new reactors (Section 3.20.5). Notably, practical elimination is defined as "physically impossible for the conditions to arise or if these conditions could be considered with a high level of confidence to be extremely unlikely to arise", (Ref. 1, Section 3.20.5) A typical example for a PWR with a large core inventory would be the gross failure of the Reactor Pressure Vessel.

604. However, in GB, a highest reliability claim is an onerous route to a safety case because the low failure frequency expected goes beyond what may be inferred from the actuarial statistics relating to the failure frequencies for the gross failure of pressure vessels and piping designed and constructed to high standards.

605. ONR therefore expects a demonstration of integrity based on sound engineering provision with measures over and above normal practice defined in nuclear codes and standards. Taken together these measures provide conceptual defence in depth. In addition, these structures and components need to be monitored, inspected and maintained through-life to maintain confidence that gross failure can be discounted. These expectations derive in part from precedents, in particular, the recommendations of the Light Water Reactor Study Group (Section 3.20.5) and the conclusions of the Sizewell B public inquiry relating to the integrity of PWR vessels (Section 3.20.5). Typically for highest reliability these additional measures include:

- Material selection and specification with tighter control of composition.
- The use of proven, well understood and approved manufacturing processes.
- The use of proven materials including a plan for direct fracture toughness testing of representative materials in manufacture and through-life via a material surveillance strategy for structures and component that may be affected by the environment, e.g. irradiation embrittlement.
- Fracture analyses with a target margin established by custom and practice, of typically 2.0, between the limiting defect size and defects that could be present in the component accounting for in-service growth i.e. an avoidance of fracture demonstration using an elastic-plastic approach beyond, for example, the fracture assessment used in established design codes.
- High reliability NDT performed during manufacture. The straight application of codes and standards is not expected to provide the required level of reliability, consequently additional measures are required, such as the development of NDT procedures that are qualified against specific objectives.
- Where appropriate high reliability in-service NDT.
- Design for inspectability, wherever possible, designs should promote the effectiveness of the NDT performed during manufacture and in-service.
- A basis for confidence that the design intent is achievable and that there is provision for the organisations involved to develop an intelligent customer capability during licensing along with provision for the development of arrangements for third party inspection surveillance of the design and manufacturing activities.

606. Whilst it will not be possible to provide a deterministic consequence case for gross failure (direct or indirect) a nominal failure frequency may be inferred for the purposes of probabilistic safety assessment. These expectations may result in differences with international practices, where leak before break (LBB), partial failure type claims (e.g. Dt/4) or concepts such as break preclusion or no break zones may be invoked. RPs should note that LBB or partial failure claims are not, generally, accepted by ONR as providing an adequate means to discount gross failure and ONR expects that

consequence analyses are provided, or if that is not possible, a highest reliability claim would be expected. In addition, whilst the application of break preclusion or no break zone concepts may include some additional provisions above normal practice these may need to be supplemented with further measures to underpin a highest reliability claim.

607. In contrast, for structures and components where highest reliability is not invoked, there needs to be a robust consequences case. For these structures and components, 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 ALARP, meeting the requirements of recognised design codes and standards may need to be supplemented e.g. the additional manufacturing controls, inspection and surveillance activities to ensure the integrity of Reactor Internals.

608. As part of the demonstration of a robust consequence case the scope and location of postulated pipe breaks may differ from international practice. ONR considers that the location of pipe breaks may be informed, but not constrained, by international practice. Thus, ONR expects that the location of pipe breaks should take cognisance of several factors: stress levels, cyclic stress levels, degradation mechanisms, OPEX, and the consequences of failure for adjacent SSCs important to safety.

609. The guidance described above provides high-level principles. In GDA the codes and standards proposed by the RP for the design, construction and inspection of structures and components are considered by ONR. 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 (Section 4) then, ONR will focus on both the basis of the approach and its application. The aim is to establish that the proposed codes and standards provide structural integrity provisions which are consistent with RGP.

610. 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.

3.20.3 INTEGRATION WITH OTHER TECHNICAL ASSESSMENT TOPICS

611. GDA requires the submission of an adequate, coherent and holistic generic safety case. Regulatory assessment of the structural integrity safety case must therefore be carried out with appropriate interactions with other disciplines.

612. The following interactions usually inform the structural integrity assessment:

- Fault studies (FS) – Interactions with fault studies are required to inform the categorisation of safety functions and the classification of SSCs. The fault studies inspector provides advice on the structural integrity claims needed to support the overall safety case for the plant.
- Internal hazards (IH) – Structural integrity assessment provides input to the missile generation, pipe-whip and internal flooding aspects of the internal hazards assessment. The results of the RP's internal hazard assessments (e.g. consequence assessments and barrier substantiation) inform the structural integrity and plant classifications.
- Chemistry (C) – The reactor chemistry, radiation protection and mechanical engineering disciplines provide input to the material selection and the assessment of potential through-life degradation aspects of the structural Integrity assessment.

- Civil engineering (CE) – Interactions with the civil engineering topic are required, normally, relating to metallic components in containment or confinement design. Civil engineering structures often provide support to structures and components considered within structural integrity (e.g. the reactor pressure vessel).
- Management for safety and quality assurance (MSQA) – Interactions with MSQA disciple are important in the assessment of the RP's proposals for the procedural control of design and manufacture of structures and components, including the plans to develop arrangements for third-party surveillance of the design and manufacture for highest reliability structures and components.

Structural integrity may also interact with other disciplines, such as: human factors, nuclear liabilities, probabilistic safety analysis and severe accident analysis.

3.20.4 LESSONS LEARNED

613. There have been three GDAs completed and as a result there are a number of lessons learned to inform new GDA inspectors and RPs. For ease of presentation these are listed under general and highest reliability below:

GENERAL

- ONR expects a robust demonstration of physical defence in depth in the plant design with consideration of the worst case consequences (direct and indirect) of postulated gross failures of SSC in the design. Thus, where structures and components whose gross failure may have previously been excluded through the application of LBB, partial failure (e.g. DT/4), or break preclusion type concepts ONR expects an explicit consideration of the consequences of postulated gross failure.
- The GB approach to categorisation and classification is often unfamiliar to RPs. ONR expects a link between the plant SSC classifications and the structural integrity provisions primarily based on the significance of the potential loss of the safety functional requirements following the postulated gross failure of SSCs. In addition, the relationship between the nuclear pressure vessel design code class and the overall safety categorisation and classification for structures and components may need specific consideration depending on the safety functional requirements, for example the structural integrity provisions for the safety injection system accumulators.
- Achievement of compliance with an appropriate nuclear or non-nuclear design, construction and inspection code may not meet RGP even outside of highest reliability applications. For example with reactor internals additional measures including inspection and surveillance activities may supplement the code provisions to mitigate through-life degradation mechanisms.
- Similarly, the application of the design and construction code in its country of origin needs to be considered and individual countries may supplement the design and construction codes with further provisions e.g. use of the ESPN order in France. In consequence, adaptation documents may be required to allow for appropriate use of the design and construction code in the UK, and the principles for these documents need to be established in GDA.
- In considering the design for access and inspectability it may be necessary to go beyond code requirements and improve the design to achieve an ALARP position.
- Design codes and standards change with time, hence the design submitted to GDA should consider if the design standards represent RGP.

HIGHEST RELIABILITY

- A highest reliability claim is an onerous route to a safety justification with an attendant high burden of 'proof' expected in design and through-life. Highest reliability claims therefore attract significant regulatory scrutiny and assessment. A principal aim is to establish with the RP whether it is reasonably practicable to avoid the highest reliability claim via consequence analyses or design improvements.
- In situations where it is not reasonably practicable to provide defence in depth in the design against a postulated gross failure or where the failure frequency needs to be very low ONR expects a highest reliability claim as the basis for discounting gross failure. This is an onerous route to a safety case attracting a high burden of 'proof'. ONR expects measures beyond normal practice i.e. compliance with an established nuclear design, construction and inspection codes.
- Where the RP discounts gross failure by invoking a highest reliability claim a demonstration is expected to show that such structures and components are not unduly challenged by the consequences of postulated gross failure of other SSC e.g. the internal hazards arising from pipewhip and missiles.
- In GDA, ONR expects an avoidance of fracture demonstration for a sample of the limiting locations in highest reliability structures and components. This demonstration integrates a conservative defect tolerance assessment with readily achievable lower bound material properties, including plans for fracture toughness testing of parent and weld materials, together with a basis for confidence in the achievement of qualified manufacturing inspections to reliably reject defects of structural concern. The approach involves the RP exercising sound engineering judgement with appropriate balances being struck between the inputs to the avoidance of fracture demonstration. RPs have benefited from engaging GB expertise to progress their avoidance of fracture demonstrations.
- A key expectation relevant to highest reliability and safety significant SSC is to limit the number and length of welds. However, recent OPEX also highlights the need for an appropriate balance between eliminating or reducing weld volumes and either avoiding defects or achieving adequate material properties in large thick section forgings.

614. In addition early engagement with the RP on the areas below is recommended:

- Scope of the structural integrity assessment for GDA (e.g. reactor design, containment, spent fuel transport and storage etc.)
- Design, construction and inspection codes for the range of structural integrity classifications and discussion of ONR's expectations and RGP.
- Defect assessment methodologies and discussion of ONR's expectations and RGP.
- Identification of novel design features or concepts including materials, construction techniques and assessment methods.
- Identification of through-life degradation mechanisms and mitigation strategies to reduce risk.

3.20.5 REFERENCES

615. Examples of GB Approaches to Structural Integrity Demonstration

- Bullough R., et al, 'The demonstration of incredibility of failure in structural integrity safety cases,' International journal of pressure vessels and piping, Vol. 78, No. 8, pp. 539 552, 2001
- Geraghty J E, 'Structural integrity of Sizewell B - The way forward,' Nuclear Energy, Vol. 35, No. 2, pp. 97 103, 1996

- Sizewell B Reactor Pressure Vessel, Special Issue of Nuclear Energy, Vol. 31, No. 6, pp. 409 453, 1992
- An Assessment of the Integrity of PWR Pressure Vessels, Summary Report, Second Report by a Study Group Under the Chairmanship of Dr W Marshall, United Kingdom Atomic Energy Authority,1982
- An Assessment of the Integrity of PWR Pressure Vessels, Addendum to the Second Report of the Study Group, since 1982 under the Chairmanship of Professor Sir P Hirsch, United Kingdom Atomic Energy Authority, April 1987
- Sizewell B Public Inquiry. Report by Sir Frank Layfield. Volume One Part I, HMSO, London. ISBN 0 11 411575 3

616. IAEA Standards and Guidance

- IAEA – Safety Standards: Safety of Nuclear Power Plants: Design, Specific Safety Requirement Series No. SSR-2/1, (Rev 1), 2016
- IAEA – Safety Standards: Fundamental Safety Principles Series No. SF-1, 2006
- IAEA – Safety Standards: Safety of Nuclear Power Plants: Seismic Design and Qualification for Nuclear Power Plants Series No. NS-G-1.6, 2012
- IAEA - Safety Classification of Structures, Systems and Components in Nuclear Power Plants, No.SSG-30, May 2014
- The relevant guidance from IAEA standards as discussed in Appendix A2 of ONR-TAST-GD-016

617. Other National and International Guidance

- WENRA RHWG, Safety of new NPP designs, March 2013
- The relevant guidance from WENRA reference levels as discussed in Appendix A1 of ONR-TAST-GD-016
- R6 – Assessment of the Integrity of Structures Containing Defects, Revision 4, EDF Energy Nuclear Generation Ltd.
- The American Society of Mechanical Engineers (ASME) Boiler and Pressure Vessel Code
- RCC-M. Design and Construction Rules for Mechanical Components of PWR Nuclear Islands. 2007 Edition. Published by the French Association for Design, Construction and In-Service Inspection Rules for Nuclear Island Components – AFCEN, Paris
- RSE-M. In-Service Inspection Rules for Mechanical Components of PWR Nuclear Islands, RSE-M, 2010 edition+2012 addendum, 2010, 2012, AFCEN
- European Methodology for Qualification of Non-Destructive Testing. Third Issue. ENIQ Report No. 31 EUR 22906 EN, August 2007
- ENIQ Recommended Practice 2. Strategy and Recommended Contents for Technical Justifications, Issue 2. ENIQ Report No.39. EUR 24111EN-2010, June 2010

Office for Nuclear Regulation

Interfaces

4 INTERFACES

618. Each topic area within GDA both influences and is influenced by other GDA topic areas. The inspector for each topic area therefore needs to work closely with inspectors in other topic areas, both in consultation with those inspectors and in the provision of information to those inspectors.

619. One of the lessons learned from previous GDAs has been that “silo working” needs to be avoided by both ONR and the RP. Inspectors need to coordinate their assessment work across those topic areas with which their area interfaces in order to perform an adequate assessment of the overall design within GDA. This applies equally to the RP, and the interfaces should also be evident within the RP’s safety case.

620. The following table displays the key interfaces visually. They are also described in the text provided for each topic area in the previous section of this document.

GDA DISCIPLINE INTERFACE TABLE	Chemistry	Civil Engineering	Control and Instrumentation	Conventional Fire	Conventional Health and Safety	Electrical Engineering	External Hazards	Fault Studies	Fuel and Core	Human Factors	Internal Hazards	Mechanical Engineering	Nuclear Liabilities	Probabilistic Safety Analysis	Radiological Protection	Safeguards	Security	Severe Accident Analysis	Structural Integrity
Chemistry								×	×	×		×	×	×	×	×		×	×
Civil Engineering				×	×		×	×		×	×	×	×	×	×	×		×	×
Control and Instrumentation				×		×	×	×		×	×	×		×	×	×	×	×	
Conventional Fire		×	×			×				×	×		×				×		
Conventional Health and Safety		×								×	×	×	×						
Electrical Engineering			×	×			×	×		×	×	×		×					
External Hazards		×	×			×		×		×	×	×		×			×	×	
Fault Studies	×	×	×			×	×		×	×	×	×		×	×		×	×	×
Fuel and Core	×							×		×			×					×	
Human Factors	×	×	×	×	×	×	×	×	×		×	×	×	×	×	×	×	×	×
Internal Hazards		×	×	×	×	×	×	×		×		×	×	×			×		×
Mechanical Engineering	×	×	×		×	×	×	×		×	×		×	×	×	×		×	×
Nuclear Liabilities	×	×		×	×				×	×	×	×			×				×
Probabilistic Safety Analysis	×	×	×			×	×	×		×	×	×			×			×	×
Radiological Protection	×	×	×					×		×		×	×	×				×	×
Safeguards	×	×	×							×		×					×		
Security			×	×			×	×		×	×					×			
Severe Accident Analysis	×	×	×				×	×	×	×		×		×	×				×
Structural Integrity	×	×						×		×	×	×	×	×	×			×	

References

5 REFERENCES

621. Specific references for each of the technical topic area in chapter 3 of this report are provided within that topic area's section of the report, as are the references for the safety case topic. General references used elsewhere in the report are listed here.

[1]. Safety Assessment Principles for Nuclear Facilities. 2014 Edition. Revision 0 www.onr.org.uk/saps/saps2014.pdf

[2]. Technical Assessment Guides www.onr.org.uk/operational/tech_asst_guides/index.htm

[3]. New nuclear reactors: Generic Design Assessment Guidance to Requesting Parties. ONR-GDA-GD-001 Revision 3. ONR. September 2016* www.onr.org.uk/new-reactors/ngn03.pdf

[4]. New Nuclear Power Plants Guide to the Nuclear Regulators' Approach. NGN01 Revision 0. September 2013* www.onr.org.uk/new-reactors/ngn01.pdf

[5]. Process and Information Document for Generic Assessment of Candidate Nuclear Power Plants. Environment Agency. Version 3. October 2016* www.gov.uk/government/publications/assessment-of-candidate-nuclear-power-plant-designs

[6]. Licensing Nuclear Installations. 4th edition: January 2015 www.onr.org.uk/licensing-nuclear-installations.pdf

[7]. IAEA Safety Classification of Structures, Systems and Components in Nuclear Power Plants, No.SSG-30, May 2014

[8]. IAEA Application of the Safety Classification of Structures, Systems and Components in Nuclear Power Plants, IAEA-TECDOC-1787, 2016

[9]. DECC (now BEIS), National Policy Statement for New Nuclear (EN-6), July 2011

*These guidance documents are currently being updated, new versions will be published in due course.