Office for Nuclear Regulation

ONR GUIDE			
Internal Hazards			
Document Type:	Nuclear Safety Technical Assessment Guide		
Unique Document ID and Revision No:	NS-TAST-GD-014 Revision 6		
Date Issued:	November 2019	**Review Date:**	November 2024
Approved by:	Geraint Williams	Deputy Professional Lead	
Record Reference:	CM9 Folder: 1.1.3.978. (2020/223342)		
Revision commentary:	Rev 5: This TAG revision is an extensive update to present ONR expectations on internal hazards more explicitly and broadly in the context of New Build, Existing Facilities and Advanced Nuclear Technologies. It should nevertheless be noted ONR regulatory expectations in the area of internal hazards have not changed. Rev 6: Updated Review Period		

TABLE OF CONTENTS

Published 11/19

1. INTRODUCTION

1.1 The Office for Nuclear Regulation (ONR) has established its Safety Assessment Principles (SAPs) [1] which apply to the assessment by ONR specialist inspectors of safety cases for nuclear facilities that may be operated by potential licensees, existing licensees, or other duty-holders. The principles presented in the SAPs are supported by a suite of guides to further assist ONR inspectors in their technical assessment work when making regulatory judgements and decisions. This Technical Assessment guide is one of these guides.

2. PURPOSE AND SCOPE

2.1 This Technical Assessment Guide (TAG) contains guidance to advise and inform ONR staff in the exercise of their regulatory judgment. In particular it explains the approach adopted by ONR in its assessment of safety submissions that relate to internal hazards that could have a detrimental effect on nuclear safety.

2.2 Internal hazards are those hazards to the facility or its structures, systems and components that originate within the site boundary and over which the dutyholder has control in some form. The term is usually limited to apply to hazards external to the process, in the case of nuclear chemical plant, or external to the primary circuit in the case of power reactors. 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 amongst many others.

2.3 This revision is a significant re-write and reorganisation of the previous TAG in the interest of increased clarity. ONR's fundamental approach towards internal hazards has been established for some time and remains unchanged, but experience from using the previous TAG, especially on new build projects, has shown that some aspects of internal hazards would benefit from more explicit presentation within our guidance. Particular areas in which additional clarity has been provided have been on the hazards associated with pressure part failure, combined and consequential hazards, and on interactions with other ONR assessment disciplines.

2.4 This internal hazards TAG is intended to apply across all stages of a facility's lifecycle, including design, construction, commissioning, operation, decommissioning etc.

3. RELATIONSHIP TO LICENCE AND OTHER RELEVANT LEGISLATION

3.1 The following set of licence conditions are seen as the key conditions for which compliance may be most affected by internal hazards:

- Licence Condition 7: Incidents on the site - *the licensee shall make and implement adequate arrangements for the notification, recording, investigation and reporting of incidents occurring on the site*. This includes those arising from the occurrence of internal hazards and their combination with external hazards. Records of the above should be kept in line with Licence Condition 6.
- Licence Condition 9: Instructions to persons on the site - the instructions should provide explicit information on how to deal with internal hazards and how site personnel are best protected. These instructions may require cross-referencing to specific operating instructions and limits for some hazards, for example fire and flooding.
- Licence Condition 11: Emergency arrangements – Emergency arrangements should include consideration of the conditions which may exist in an incident either arising from an internal hazard, or from one in which internal hazards may develop during the progression of the incident.

- Licence Condition 14: Safety documentation - *the licensee shall make and implement adequate arrangements for the production and assessment of safety cases consisting of documentation to justify safety during the design, construction, manufacture, commissioning, operation and decommissioning phases of the installation*. It is from this licence condition that the requirement for safety cases arises, and therefore for internal hazards to be considered.
- Licence Condition 15: Periodic review - *the licensee shall make and implement adequate arrangements for the periodic and systematic review and reassessment of safety cases*. It is from this licence condition that ONR expects the review and reassessment of safety cases to address internal hazards.
- Licence Condition 20: Modification to design of plant under construction - this licence condition requires that a modification to the design of plant under construction is assessed taking due account of all relevant internal hazards.
- Licence Condition 22: Modification or experiment on an existing plant - this licence condition requires that a modification or experiment on an existing plant is assessed taking due account of all relevant internal hazards.
- Licence Condition 23: Operating Rules – this licence condition requires that the licensee shall, in respect of any operation that may affect safety, produce an adequate safety case to demonstrate the safety of that operation and to identify the conditions and limits necessary in the interests of safety. These conditions may be set to prevent internal hazards from materialising, or to reduce the severity of internal hazards should they materialise e.g. avoid high operating pressures giving rise to pipe whip or energetic jet impacts on plant upon loss of pressure boundary failures.
- Licence Condition 28: Examination, Maintenance, Inspection and Testing (EIM&T) – this licence condition requires that the licensee make and implement adequate arrangements for the regular and systematic examination, inspection, maintenance and testing of all plant which may affect safety which would include a number of systems installed to protect and against internal hazards e.g. automatic fire suppression systems and flood detection and trip systems.

3.2 Other relevant legislation for internal hazards include the following:

- Dangerous Substances and Explosive Atmospheres Regulations (DSEAR) 2002.
- Regulatory Reform (Fire Safety) Order 2005.
- Fire (Scotland) Act, 2005 and Fire Safety (Scotland) Regulations 2006.
- Pressure Systems Safety Regulations (PSSR), 2000.
- Lifting Operations and Lifting Equipment Regulations (LOLER), 1998.
- Control of Major Accident Hazards Regulations (COMAH), 2015.

3.3 There are Approved Codes of Practice (ACOPs) associated with both DSEAR 2002 and PSSR 2000:

- Dangerous Substances and Explosive Atmospheres, Approved Code of Practice and Guidance L138 (2nd edition), published 2013 [2].
- Safety of Pressure Systems, Pressure Systems Safety Regulations 2000 Approved Code of Practice L122 (2nd edition), published 2014[3].
- Safe Use of Lifting Equipment, Lifting Operations and Lifting Equipment Regulations 1998, Approved Code of Practice and Guidance, L113 (2nd edition), published 2014 [4].

3.4 These ACoPs have been approved by the Health and Safety Executive (HSE) with the consent of the Secretary of State. They give practical advice on how to comply with the law. It should be noted that ACoPs have a special legal status [5]. If a dutyholder decides not to follow the relevant provisions of the ACoP, it will need to show that it

has put in place equally effective means of complying with the law. It should however also be noted that compliance with these ACoPs for a relevant application in a nuclear context does not mean that all legal responsibilities have been complied with.

3.5 In addition to the above licence conditions, regulations and ACoPs, there are numerous standards and guidance documents relating to the design, commissioning, operation and maintenance of safety systems for nuclear plant which may be affected by or are designed to prevent, control or mitigate internal hazards. Additionally, for scenarios involving fire, explosion, and dangerous substances, there are likely to be overlaps with the Control of Major Accident Hazards (COMAH) Regulations 2015 on nuclear sites that fall within these Regulations due to the size and nature of their inventories.

3.6 Standards and guidance relevant to each internal hazard in turn are referred to in Section 5. These are provided as examples of approaches which may be considered Relevant Good Practice by ONR for specific applications and situations, and should not be taken as the only acceptable way to demonstrate that the risks have been reduced to As Low As Reasonably Practicable (ALARP).

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

SAPs

4.1 ONR SAPs include an expectation that safety cases provide an analysis of normal operation, potential faults and accidents, in the context of the facilities' engineering design and operational provisions to demonstrate that risks from the facilities have been reduced to ALARP. This means that safety cases need to be informed by a systematic identification of internal hazards and their combinations as documented in SAP EHA.1 and EHA.14.

4.2 Hazard identification involves a review of the facility design and of the site context. For plant that has been operating, it will be informed by a review of the plant condition. It may also include insights from event tree analysis. Hazard identification exercises are generally undertaken early on in the design process, throughout design development and should consider all operational states including commissioning, operations and decommissioning. The aim is to ensure that the site and plant layouts eliminate or minimise the potential for detrimental effects should hazards materialise, and by commencing an identification process early enough for there to be flexibility to adapt the designs. Hazard identification exercises should be informed by reviews of relevant Operational Experience (OPEX). They should also be periodically reviewed to ensure that the status of the plant remains understood and operates within the design constraints, particularly after modifications to plant or structures.

4.3 Having identified the hazards, it is necessary to characterise the hazard ranges, loads and demands that would be placed upon the facilities. Expectations on Internal Hazard characterisation are summarised in EHA.6 of ONR SAPs [1].

4.4 In line with EKP.3, *nuclear facilities should be designed and operated so that defence in depth against potentially significant faults or failures is achieved by the provision of multiple independent barriers to fault progression.* This includes consideration of internal hazards as initiating events and as threats to safety measures. EKP.5 expects measures to be identified to deliver the required safety functions and these should be resilient to hazards.

4.5 Demonstration that the risks from hazards have been reduced to ALARP can be done by adopting inherently safe approaches, attention to site and plant layouts, good engineering standards and design, keeping inventories of hazardous (e.g. combustible

and toxic) materials to a minimum, and thereafter through good safety management practices.

4.6 In line with the hierarchy of safety measures in the SAPs (EKP.5) guidance, the safety assessment should demonstrate that threats from internal hazards are either removed or minimised. The latter may be done by showing that items important to safety (i.e. safety systems and safety related items) are protected by safety features e.g. nuclear safety barriers that withstand the hazard loadings, or designed to withstand the challenges of the hazards, and by the provision of safety systems which respond to mitigate the radiological consequences of fault sequences. Note that the reference to "items" includes Structures, Systems and Components (SSCs).

4.7 The hazards from all facilities and activities that the operator might reasonably need to undertake on the site during the life of the facilities need to be considered, including those associated with construction, commissioning, inspection, maintenance, testing, decommissioning etc.

4.8 Detailed knowledge of the plant and site layout is required for an internal hazards assessment to appropriately capture challenges to nuclear safety from both individual and combined hazards. This applies to facilities nearing commissioning or during operations. Multi-facility sites generally require appropriate interface arrangements to deal with the potential knock-on or domino effects from materialisation and spread of internal hazard effects. These may be interfaces within the site management structure of a single licensee company, or cooperation between several licensees.

4.9 Expectations in all the above areas are explicitly documented in the suite of SAP Engineering Principles, and particularly in the ELO (Layout), EKP (Key Engineering Principles), ECS (Safety Classification and Standards), EDR (Design for Reliability), ESS (Safety Systems) and Fault Analysis (FA.1-9) series. In the context of design and operation of nuclear chemical process the Chemical Engineering SAPs EPE 1-3 are also relevant. Relevant SAPs are discussed, for each internal hazard in turn in section 5.

WENRA and IAEA

4.10 The objective of the Western European Nuclear Regulators Association (WENRA) [5] is to develop a common approach to nuclear safety in Europe by comparing national approaches to the application of the International Atomic Energy Agency (IAEA) safety standards. The Reference Levels (RLs), which are primarily based on the IAEA safety standards, represent good practices in the WENRA member states and also represent a consensus view of the main requirements to be applied to ensure nuclear safety. Section 4 of NS-TAST-GD-005 identifies the WENRA RLs as Relevant Good Practice (RGP) for existing civil nuclear reactors.

4.11 It should be noted that ONR SAPs are intended for both existing and new facilities whereas the WENRA Reactor Safety Reference Levels are principally intended for existing reactors. WENRA has nevertheless published a report on safety of new NPP designs considering lessons from the Fukushima Dai-ichi accident [6] which has been considered in this TAG. Similarly, WENRA also has safety reference levels for radioactive waste treatment and conditioning [7] and radioactive waste disposal facilities [8] which, in the context of internal hazards, align with the IAEA guidance considered in this TAG. It is recognised that, therefore, WENRA and IAEA documents considered in this TAG are focused on nuclear reactor power plants and so do not have the same broad scope intent of the SAPs and this TAG.

4.12 The WENRA reference levels were re-issued in 2014 to primarily update them with lessons learned from the Fukushima Dai-ichi accident and insights from the EU stress

tests. Key expectations in this version were the revised expectations on natural hazards and combination of events.

4.13 As part of this TAG rewrite, ONR has reviewed the WENRA reference levels and IAEA Safety Standards referenced within, NS-G-1.7 [9] and NS-G-1.11[10], and concluded that expectations in the area of internal hazards remain aligned with the SAPs and this TAG. Specifically, WENRA RLs Issue S: Protection against Internal Fires are addressed in Section 5, as RL text has been mapped with ONR expectations in the SAPs and TAGs. ONR expectations in the area of combined hazards are also aligned with the WENRA reference levels (2014) and these have been made more explicit in the revised Section 5 of this guide.

4.14 IAEA guidance relevant to internal hazards can be found within:

- SF-1, “Fundamental Safety Principles: Safety Fundamentals” [11];
- NS-G-1.7, “Protection against Internal Fires and Explosions in the Design of Nuclear Power Plants” [10];
- NS-G-2.1, “Fire Safety in the Operation of Nuclear Power Plants” [12];
- NS-G-1.11, “Protection against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants” [9];
- SSR-4 Safety of Nuclear Fuel Cycle Facilities [13].
- SSR-2/1 Safety of Nuclear Power Plants: Design [14];
- SSR-2/2 Safety of Nuclear Power Plants: Commissioning and Operation [15].
- SSG2 Deterministic Safety Analysis for Nuclear Power Plants [16].
- SSG-15 Storage of Spent Nuclear Fuel [17].

4.15 The guidance for internal hazards contained in the above IAEA documents is addressed in the UK approach to regulation of nuclear facilities.

5. ADVICE TO INSPECTORS

General

5.1 The overall objective of ONR SAPs for internal hazards is to minimise their effects on the facilities, particularly to ensure that they do not adversely affect the reliability of safety systems designed to perform essential safety functions, and that the potential common cause failures caused by the materialisation of internal hazards have been adequately addressed.

5.2 Items important to safety (i.e. safety systems, structures and components, SSCs, and safety-related systems) should be either protected against the hazards i.e. by appropriate use of segregation, redundancy, diversity and separation, or qualified to withstand the effects of the hazards. ONR SAPs EDR.2 applies in this regard.

5.3 In achieving this objective, the SAPs expect a comprehensive and systematic approach to identifying the internal hazards which may individually challenge the facilities, and to consider those hazards in combination with any consequential, concurrent or independent hazards and/or faults which may arise in that context and in combination with the most onerous conditions. Internal hazards may be inherent to the facilities normal operation e.g. generation of flammable materials, or generated as a consequence of plant fault or external hazards. Internal hazard effects may include local effects (e.g. from fire, flooding, pipe whip, jet impact, etc.), global effects (e.g. pressurisation of compartment, humidity, temperature, etc.) and the subsequent plant and equipment failures which may result from them, including related hazards.

5.4 The SAPs also expects the hazards to be characterised in the context of the challenges they will pose to the plant. Hazard characterisation may involve a wide range of tools including correlations, models, computer codes etc. Inspectors should

expect appropriate validation and verification of any such models to be available in line with ONR SAPs (AV.2, AV.3 and AV.4). ONR expectations for the validation of computer codes and calculation methods further explained in a separate TAG (NS-TAST-GD-042; [18]).

5.5 In line with IAEA guidance, ONR expects a "defence-in-depth" approach to be applied to internal hazards, and this approach should be in line with the expectations detailed within EKP.3. That is, for each internal hazard that cannot be practically eliminated, the following approach is applied (in order of preference):

- Prevent the hazard from occurring;
- Limit the severity of the hazard should it occur;
- Limit the consequences of the hazard should it occur and be severe.

5.6 Inspectors should expect safety cases to recognise the unmitigated consequences from hazard scenarios, and these to be used to define the appropriate engineering and managerial provisions. The safety case should also demonstrate how the defence-in-depth philosophy has been applied to each internal hazard and identify the appropriate control measures which should be classified and defined according to their significance in ensuring that nuclear safety functions continue to be delivered.

5.7 Generally, for internal hazards that cannot be completely eliminated or prevented, the severity of the hazard can be reduced by a number of means. This can be done by favouring benign materials, fluids and operating envelope e.g. limiting combustible or flooding source inventories, operating at lower pressures and temperatures etc.

5.8 Limiting the consequences of hazards can be preferably ensured by good plant layout principles (ELO.4), and by protecting the plant from the hazard loadings. The latter should be generally achieved by the provision of robust passive barriers which withstand the maximum credible loadings and segregate safety systems that allow the continued delivery of nuclear safety functions..

5.9 The nuclear safety consequences of hazards can also be limited by ensuring that equipment important to safety withstands the hazard loadings e.g. by suitable qualification to the specific dynamic and environmental conditions of the hazard, ensuring sufficient separation or shielding. Approaches based entirely on hazard distances or heavily reliant on SSC qualification may be challenging to support in the absence of suitable segregation.

5.10 As part of the assessment of safety cases, inspectors should ensure that safety functions that may be impacted by internal hazards (individual hazards or in combination) have been allocated an appropriate safety category (e.g. A, B or C) and SSCs that have to deliver those functions have been given an appropriate safety classification (e.g. 1, 2 or 3), clearly identifying their role in ensuring nuclear safety (ECS.1 and ECS.2). Further guidance on categorisation and classification is given in another ONR TAG (NS-TAST-GD-094). Categorisation of safety functions and classification of SSCs as informed by hazard analyses in turn informs judgements on the choice of safety measures (number, type, classification and level of substantiation) in line with their role in delivering defence-in-depth.

5.11 Avoiding or reducing the number of highest reliability components (sometimes referred in GDA as High Integrity Components (HIC), Highest Safety Significance (HSS) or Very High Integrity (VHI) is a key consideration in structural integrity and, generally all engineering specialisms. These are items for which gross failure leads to highly undesirable consequences and therefore this is an onerous route to a safety case with additional measures beyond normal practice i.e. in nuclear codes and standards expected to either discount the failure or infer that the failure frequency has been reduced to a very low value. However, in addition to the above, these components

need to be located, segregated or designed to be demonstrably resilient against all credible internal hazards which may materialise in the vicinity. This is because code compliance may not include transient loads resulting from the effects of hazards.

5.12 Inspectors should expect safety cases to demonstrate that due consideration has been given to the potential for cliff-edge effects, where small changes in the case within reasonable bounds of uncertainty and plausible states would lead to more severe consequences. They should also expect safety cases to consider the effects of internal hazards across the accident sequences, from the most frequent initiating events and design basis analysis, through to severe accident analysis. This is because internal hazards do not only play a role as event initiators or as triggers of consequential hazards, but can also place indirect demands or loadings on SSCs credited to perform with a defined level of reliability within the sequences. The level of substantiation of safety measures should be consistent with the safety categorisation and classification, and in line with their role in delivering defence-in-depth.

5.13 Inspectors should also expect that the measures providing protection against hazards are subject to an appropriate maintenance regime (with appropriate operating and maintenance instructions). This applies to passive measures as well as active ones. The integrity and reliability of barriers, penetrations and detection and alarm systems should be demonstrated.

5.14 Inspectors should expect the deterministic and probabilistic data used in the analysis to be justified. Licensees should place the greater emphasis on deterministic means of demonstrating safety. However, probabilistic arguments may be of some use when assessing proportionality and on optimising the effectiveness of measures, consistent with ALARP principles. In such cases, estimates of failure probabilities and consequences should be shown to be commensurate with the age and condition of the plant and equipment.

5.15 Internal Hazards as a discipline interface with most other ONR disciplines. For example:

- Fault Studies forms a key interface with internal hazards in the consideration of event initiators, fault sequences, consequences and defence-in-depth, taking note of SAPs FA.3, FA.6, FA.7 and FA.8.
- Severe Accident Analysis. The assessment of severe accident characterisation and measures is normally considered by Severe Accident Analysis specialists and not internal hazards inspectors. However, internal hazards inspectors should liaise with Severe Accident Analysis specialists to ensure that safety cases adequately consider internal hazards as initiators.
- Probabilistic Safety Analysis (PSA). Internal hazards inspectors should liaise with Probabilistic Safety Analysis inspectors in the assessment of internal hazards as initiating events in the PSA, and in how the consequences and plant responses to hazards have been modelled and credited.
- External hazards can cause internal hazards and therefore internal hazards inspectors should liaise with External Hazards specialists in the assessment of hazard combinations.
- Structural integrity forms a key interface in the considerations of break locations and categorisation / classification of pipework and equipment in relation to a number of internal hazards, particularly pipe whip and jet impact, and flooding, spray and steam releases as well as highest reliability claims.
- Internal hazards inspectors should also liaise with process engineering and chemistry specialist inspectors in their consideration of hazards to SSCs posed by the process (during normal and abnormal conditions).
- Where there are time dependant actions (for example, claims made on valve isolation or impacts to protection systems), Inspectors should liaise with the

relevant specialists e.g. Human Factors and Control & Instrumentation / Electrical Engineering.

- Where claims of withstand capability are made on structures, the civil engineering design should include all internal hazards loadings and demonstrate that the loads from hazards are within the scope of the civil engineering design substantiation. Other key interfaces with Civil Engineering include fire barrier design (EKP.2 and 5), consideration of good plant layout principles (ELO.4) to cite two examples.
- Where hazards have the potential to impact not only nuclear plant and SSCs but also people, internal hazards inspectors should liaise with Life Fire Safety and Conventional Health and Safety inspectors. This is particularly important for sites whose inventories fall within the remit of COMAH, and for which Conventional Safety specialists should be approached for advice. Similarly, where conventional and fire safety hazards may impact on nuclear plant and SSCs, those specialists should liaise with Internal Hazards specialists.

Specific considerations associated with pipework system failures

5.16 Inspectors should particularly note that whilst partial failures [e.g. in line with the Leak Before Break (LBB) concept] may feature as part of safety cases, it is expected that good design practice would be followed to ensure that the plant can accommodate the consequences of gross failure, and reliance on highest integrity plant is to be considered only when all avenues to improve the structural integrity case have been exhausted and none are deemed to be reasonably practicable. This is primarily relevant to internal flooding, pipe whip and jet impact hazards.

5.17 In the above hazard context, licensees' safety cases generally consider a system to operate in High Energy mode when the pressure is equal or greater than 2.0 MPa and/or the operating temperature is 100º C or greater in the case of water, according to [9] or equivalent. Whilst there are systems which may be operating in high energy mode during short periods of time e.g. during testing, inspectors should expect to see that failures are postulated in the most onerous initial operating state (SAP para. 631 and FA.7), e.g. in high energy mode. The short duration of the mode of operation (e.g. operating in high energy mode for 1% or 2% of the operating times) should not be used to exclude the most onerous failures from the safety case (see SAP NT.2 and SAP para. 759-767). The ONR inspector should carefully consider the deterministic and probabilistic arguments made when making a judgement on whether the risks from the operations in question have been reduced to ALARP.

5.18 Where bounding arguments are made on that hazards associated with high energy pipework failure bound consequences of the failure in operating states with lower stored energy, inspectors should seek evidence that those effects are comparable and not overly simplified e.g. a "moderate energy" pipe with larger bore holding a larger inventory can pose a more significance flooding or steam release / humidity challenge than higher energy pipes. Similarly the consequences of failures of moderate energy pipework should not be limited to consideration of partial failures.

5.19 Inspectors should expect to see failures postulated in locations as follows:

- Terminal ends (welds, fixed points to supported plant components, large pipework which is restrained by supports suitably designed to withstand the dynamic loads from pipework movement in the postulated pipe whip scenarios);
- Locations with high stress, high fatigue usage factors or where operational experience suggests that there may be a higher likelihood of degradation and hence failure e.g. dissimilar metal welds.

- Locations where failure would give rise to bounding consequences in terms of impact on SSCs e.g. other high energy pipework and components.

5.20 The above approach is partly based on US practice [33] and based on the above, it is expected licensees and requesting parties will review the piping systems and identify limiting locations by postulating failures where appropriate at terminal ends, weld locations, points of high stress and fatigue usage, and at all locations where failure would give rise to bounding consequences on SSCs and hence the delivery of safety functions.

5.21 It may be appropriate to rationalise the list of scenarios prioritising sets of bounding / challenging scenarios which should capture worst case consequences from the system/ pipework under consideration. However, inspectors should ensure that potential failure points are not excluded on low stress or fatigue usage levels alone, and the worst case failure locations are identified and analysed proportionately.

5.22 There should also be a demonstration of adequate safety measures to prevent hazard progression and sufficient control of radiological hazards at all times in line with SAPs EKP.2, EKP.5. Hazards arising from systems which are not continuously energised or in use should be postulated in the worst operational state and/or least control (mode of operation with the highest energy). The worst operational state may also relate to the conditions of neighbouring plant or of protective or mitigative measures e.g. maintenance / 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.

5.23 The following subsections provide advice to inspectors on the application of these general expectations to each internal hazard in turn.

Fire

5.24 Fires result from the oxidation of combustible materials (fuel) in the presence of an oxidiser (typically oxygen from air) and are initiated by ignition sources, which provide the initial energy required for the exothermic process of combustion to start.

5.25 Fires generate flames, heat, smoke and other combustion products, all of which have the potential to damage SSCs delivering safety functions in nuclear plant and to prevent normal operation and actions needed to maintain nuclear safety. The expectations regarding fire hazards to life (flame impingement, heat, toxic products of combustion, loss of visibility for escape and firefighting) are within the scope of "conventional" fire safety and are not presented in this TAG.

5.26 A basic safety requirement in ONR SAPs, WENRA RLs and IAEA guidance documents is to engineer defence-in-depth, as described in section 4 above. Generally speaking, inspectors should expect defence-in-depth to be reflected in the hierarchy of measures adopted in the design of the facilities against fire hazards. Good engineering design in this area should show how precedence has been given to fire prevention (e.g. minimisation of combustible inventories) and how the design ensures that fires, when they occur, do not lead to unacceptable consequences. This involves limiting the severity of any fires (e.g. by early detection and extinguishing, the provision of suitably rated fire barriers that prevent fire spread). For any severe fires which do arise, the consequences on nuclear safety relevant SSCs should be limited by design (e.g. by provision of redundant safety measures in segregated fire compartments). An important example is by arranging that redundant safety measures should be located in fully segregated fire compartments. This is referred to as the "fire containment approach". The fire containment approach is the preferred approach to fire protection [10]. Generally, the expectation is that fire barriers should be rated to withstand

combustion of the entire fire load in the compartment, both in terms of fire intensity and resistance rating (duration).

5.27 Even though the fire containment approach does not require fire suppression or extinguishing systems to limit the effect of the fire to the single set of redundant equipment, and therefore to allow safety functions to be provided; nevertheless there are occasions where Inspectors should look for active fire suppression systems. IAEA guidance [10] specifically indicates that this may be appropriate in areas of high fire load, but ONR inspectors should also look for such systems in areas where there is the potential for fire spread should fire doors fail or be left open, or where a fire could continue burning for an extended period, which would go outside the resistance rating for elements of the fire containment boundaries. The need for such provision may form part of ONR judgement on hazard resilience or form part of a licensee's overall ALARP argument.

5.28 Where the fire containment is not practical due to conflicts with other plant design requirements, an alternative fire protection method, the "*fire influence approach*", could be adopted. This involves separation of redundant items or safety systems important to safety into separate fire cells, where a mixture of passive building elements, distance and active fire suppression may be necessary for adequate separation. Adequate fire cell separation could be achieved using an appropriate combination of limited combustibles, local passive fire barriers, shields, cable wrap, cable conduits, separation by distance and fire detection and suppression systems. The "*fire influence*" approach should be designed to offer an equivalent fire protection to the physical segregation provided by fire barriers, including by the active fire protective measures described. It should be noted that modifications or facility upgrades can bring specific challenges to the fire influence approach, as hazard management relies on continued availability of multiple measures and good control of transient loads to ensure the effectiveness of each measure individually and in combination is not compromised.

5.29 A series of key expectations on hazard identification, analysis and measures specific to fire hazards are documented in the sections below. These recommendations arise from a number of sources, including IAEA guidance and WENRA RLs. Inspectors should however note that this TAG is not meant to comprehensively capture all expectations for fire safety. Other good practice guidance, documents, including all of their recommendations, should be considered as part of the fire assessment as appropriate.

Fire Sources

5.30 Fires can start at any time and at any location which contains permanent or transient combustible inventories, providing an ignition source of sufficient energy is present. Consequently, inspectors should expect that these locations, together with the combustible inventories (nature, quantity and properties of materials and substances present) are suitably identified (EHA.14).

5.31 The safety case should provide reference to surveys or studies of combustible substances, which should be systematic and demonstrably complete. The survey should include solids (for example: furniture, waste, oily rags, metal fines, dusts and powders, wooden scaffolding, electrical equipment, combustible insulation and cladding), gases (for example: methane, Liquefied Petroleum Gas [LPG], compressed flammable gases, hydrogen, propane), liquids (for example: petrol, acetone, paint thinners, methanol, fuel oil, hydraulic fluids, lubricating oils), vapours. Transient fire loads that could be introduced either during construction, maintenance etc. should also be identified.

5.32 In addition, good engineering practice should be adopted in the design and layout of the facilities (ELO.4) and this should be apparent in fire and ignition source identification records. Examples of good engineering practice include:

- Non-combustible, fire-retardant or self-extinguishing construction materials, electrical cabling and working fluids should be used wherever it is reasonable to do so (EHA.17).
- The quantity of combustible materials, including in process and storage, should be minimised and controlled (EHA.13).
- The location of combustible inventories in the vicinity of items important to safety should be identified and documented. This should also include the routing of combustible inventories in relation to safety items, e.g. to consider the path of a combustible liquid or gas. Similarly any ignition sources should be documented.
- Storage facilities should be segregated from areas containing safety-related plant and equipment by spatial or physical barriers. They should be fitted with suitable fire detection and suppression facilities so far as is reasonably practicable (EHA.16). Fire detection and suppression systems should be adequately reliable (ERL.1).
- Sufficient procedures and controls should be put in place to ensure that the level of combustibles, both fixed and transient, within a compartment do not exceed the design fire load and potentially increase the threat to nuclear safety.
- Any processes involving or producing combustible or explosive gases should take place in well ventilated areas segregated by suitable barriers from items important to safety.
- Bunds, drip trays and flange shields should be provided to control and contain any leakage of combustible or flammable liquids as well as any potential fire initiators
- Ignition sources (e.g. hot surfaces, flames and hot gases, mechanically generated sparks, electrical apparatus, exothermic reactions (chemical), spontaneous ignition, static charge) should be eliminated so far as is reasonably practicable. The control of ignition sources should minimise the likelihood of ignition of combustibles. Only suitable electrical equipment such as that specified in relevant standards should be used in areas where flammable vapours may exist. Such areas should be classified accordingly. Adequate risk assessments are required in areas where there are dangerous and explosive substances present under the requirements of DSEAR Regulations [2] and other relevant regulations. Notwithstanding this, it should be recognised that meeting the requirements of DSEAR may not go far enough if the potential fire or explosion could affect plant or building structures related to the nuclear safety of the facility.

5.33 It should be noted that all combustible inventories, including transient and protected combustible loads (e.g. cables in conduits) can contribute to a fully developed fire and the overall fire load. Consequently, a basis of design that provides for a fire that involves all available combustibles within a fire compartment is a good starting point in demonstrating resilience against fire hazards and should be expected during the hazard identification stage.

5.34 The results of the fire hazard identification process should be documented to provide a basis for the hazard characterisation stage. In particular, fire hazards to items important to safety that may arise due to the failure of barriers and escalating fires

should be identified. ONR assessors should seek assurance on the completeness and coverage of the hazard identification methodology.

Fire Hazard Analysis

5.35 Fire hazard analysis aids the design process and is ultimately used to demonstrate the adequacy of the engineered safeguards in place to prevent unacceptable consequences to nuclear safety.

5.36 Inspectors should expect safety cases to demonstrate that suitable fire consequence analysis methods and models have been applied to estimate the severity of fire hazards (EHA.1, EHA.5, EHA.6) and that the outputs from fire and ignition source identification have been taken forward for analysis.

5.37 The potential for fire initiation and growth and the possible consequences on items important to safety should be determined as part of the fire hazard analysis with the following key purposes:

- Determine consequences to SSCs and their defined withstand criteria, determine if further separation, isolation and redundancy is required (EDR.2, ESS.18);
- Determine the performance requirements of fire safety measures (e.g. fire barriers, suppression systems, passive fire protection applied to structures etc.);
- Specify the capability and capacity of the fire detection systems and any other active fire protection provisions;
- Justify the adequacy of ”fire influence” provisions in place;
- Test fire hazard identification and design substantiation assumptions and limitations;
- Determine consequential effects from fires– e.g. flooding, explosion, drop loads etc.

5.38 As part of their assessment, inspectors should evaluate that the analysis approach adequately addresses the inherent uncertainty associated with fire initiation and progression, and any reliance placed on the reliability of fire protection or fire mitigation measures. On this basis, inspectors should expect that appropriately conservative base assumptions have been used to develop the deterministic case, for example:

- The analysis captures the outcome of worst case scenarios (e.g. there is no effective active fire protection, ventilation remains available either due to the continued operation of forced systems and/or natural ventilation via openings etc.). Sensitivity studies may be required to establish the worst case scenario;
- Generally, it should be expected that at least as a starting point, the analysis will be based on complete burn-out of all combustible loads including any protected loads (e.g. cables in conduits, cable wrap etc.) within the compartment;
- All SSCs in the fire compartment are lost in the fire unless they are suitably qualified;
- Fire analysis during maintenance operations, outages etc. should be developed and take into account the worst permitted configuration i.e. availability of fire barriers, status of doors and hatches connecting different fire compartments etc.

5.39 It is expected that the fire analysis should clearly identify the fire compartments within the design and how these relate to the “safety divisions” (i.e. how safety systems are structured into redundant trains). It should also document the effects of fire scenarios on the nuclear safety relevant barriers and plant taking into account the most challenging plant state. Typical features of adequate fire analysis generally include the following:

- For each compartment, the scenarios identified to present the most significant threat to the fire compartment barriers. There should be a clear auditable trail showing, for example, that the scenarios have been defined taking into account the effect of multiple relevant variables e.g. combustible load, ventilation rates (natural and mechanical), room height, areas, geometry etc. ONR’s expectations on Ventilation system design and performance are outlined in the Ventilation TAG (NS-TAST-GD-022) [20].
- Fire modelling of compartment-wide (global) fires can be used to generate time-temperature profiles and/or other key representative parameters of the fire.
- The time-temperature profiles generated can then be evaluated against recognised standard fire curves which are relevant to the plant design and construction materials (e.g. BS EN 1363-1 [19] for a three-hour fire duration). The objective of the global fire effects modelling is to demonstrate that all fire scenarios are within standard fire curves relevant to the design, and therefore that the claimed barrier response is not compromised in the event of a fire.
- Substantiation of claimed barriers can be undertaken using acceptance criteria. The acceptance criteria may take the form of a minimum barrier thickness or other parameters representing the claimed fire resistance of the barriers. This can be extracted from standards relevant to the barrier design and fire conditions e.g. those specified in BS EN 1992-1-2 [21] for reinforced concrete barriers under a three-hour fire. Detailed structural analysis and/or fire testing may be required to substantiate bespoke barrier designs or complex fire scenarios. Further design development to reduce fire loading could also be needed.
- Inspectors should expect that appropriate sensitivity analysis has been undertaken to show that there are sufficient safety margins. This should address uncertainty inherent to the design and the fire analysis. Pessimistic estimates in parameter values (e.g. ventilation rates, combustible inventories, characteristics of rooms) and fire behaviours within reasonable bounds of uncertainty should not lead to cliff-edge effects exceeding the capacity of protection measures.
- Specific to the “fire influence” approach, inspectors should expect any claims on sufficient separation of SSCs by distance to be substantiated with evidence such as consequence analysis results showing sufficient margins with conservative assumptions. This is particularly relevant when any such claims play a primary role against common cause failure of multiple SSCs delivering the same fundamental safety function (EDR.3).
- Similarly, any claims on “no fire spread” between combustible inventories should be supported by evidence e.g. due consideration of flame impingement and/ or heat transfer between inventories. In particular claims specific to cables such as on cable trays, metallic conduits, minimum distances between cable raceways, flame-retardant cables, should be supported with appropriate evidence.
- Inspectors should expect that the fire analysis remains valid throughout the life of the plant. Findings from plant commissioning activities, plant

modifications etc. may result in change to key assumptions invalidating the analysis presented. For example, conduits that may not be a part of the original design could have been added, or fire protective measures could have been found not to be conforming to expectations (e.g. intumescent paints, fire resistant seals).

(NB. this is not intended as an exhaustive list of requirements, inspectors should apply their judgement on proportionality and reasonable practicability according to the specific plant design and balance of fire protection features).

5.40 Fire effects can concentrate on specific areas of the plant or protection features. These are commonly referred to as local fires and typically arise from ignition of highly localised fuel loadings (e.g. oils, lubricants, fuels, densely packed cabling mounted on or placed near fire barriers). They pose a different challenge to the design than that posed by global fires as heat from the fire (and flame impingement) is focused on specific features e.g. structural members, a fire barrier panel or fire door. Pool fires are a typical example of fire scenarios which can result in significant localised effects.

5.41 Inspectors should expect the fire analysis to clearly identify the locations and fire sources e.g. hydrocarbon inventories where local fires are credible and could pose a significant challenge. Some of the typical features of pool fire analyses include:

- Calculation of fire burning characteristics (e.g. heat release rate, fire duration, flame height and pool area) using for example empirical correlations or combustion models within Computational Fluid Dynamics (CFD) packages as appropriate.
- Evaluation of fire generated conditions and effects on structures (ECE.6, ECE.12). Generally, the analysis leads to temperature – time profiles which can be compared to a hydrocarbon fire curve for a pool fire (e.g. BS EN 1363-2 [22]).
- Design features providing a level of protection or a potential threat to SSCs should be identified, e.g. reinforced concrete (RC) structures local to a fire source or smoke plume. Design substantiation may involve calculation of the maximum temperature rise of the back face of the barrier (to demonstrate, for example, that there are no negative effects on SSCs on the other side of the barrier). It may also involve calculating the temperature rise on the first layer of steel reinforcement and comparing these to maximum allowable values given in standards.
- Appropriate justification should be provided for areas containing localised high inventories other than oils/ lubricants such as cables, and for construction materials and techniques which may differ from those captured in barrier performance standards.
- Computer fire model limitations, assumptions, error margins should be made explicit and sources of uncertainty identified and provided for in the design.

Fire Safety Measures

5.42 The overall design of the facility should evidence that fire vulnerabilities have been addressed using the output from the fire analysis. This is often the result of an iterative process in which consequence analysis is revisited as the design and location of SSCs delivering safety functions is optimised. It also results in the specification of fire resistance for barriers and/or passive fire protection to meet a required level of resilience.

5.43 Some common characteristics of design features and considerations in the design of safety measures against fire include the following:

- Fire barriers should be designed to provide the fire resistance as required by the fire analysis.
- Penetrations (e.g. doors, dampers, cable and pipework penetrations and etc.) on divisional / fire barriers[1] should be avoided where practicable. If this is not feasible, then the location of penetrations in fire barriers should be optimised to prevent spread of fire and should be designed to at least the same level of fire resistance as the fire barrier. The penetrations should be readily identifiable and maintained at suitably frequent intervals to ensure the appropriate level of reliability.
- Fire dampers should be provided in ventilation ducts that penetrate fire barriers to prevent the transmission of fire and smoke. Consideration should be given to the means of initiation and the potential for the transmission of smoke and the acceptability of this should it occur. The ventilation system integrity should be maintained despite possible filter fires or any other fire or explosion hazards.
- Where dampers are installed in divisional / fire barriers appropriate consideration to single failure criterion should be given and this may require installation of fire dampers in series (EDR.4).
- In forming their judgement on the adequacy of fire dampers, inspectors should be satisfied that they are not only designed, but also adequately installed, maintained and inspected.
- Fire doors on divisional/ compartment barriers should be avoided so far as is reasonably practicable. If included, inspectors should consider whether the design has given due consideration to the potential value of lobby configurations (with two fire-rated doors in series between fire compartments for defence-in-depth) and that the doors withstand all relevant internal hazard loadings according to the expected level of performance of the barrier.
- Appropriate door monitoring systems, of appropriate safety classification levels and alarming to an appropriate staffed location may be reasonably practicable, particularly across nuclear safety barriers of the highest nuclear significance.
- Where structural steelwork forms part of a divisional or compartment barrier, or provides a support function to the barrier, consideration should be given to the need to provide passive fire protection depending on its safety function, the severity of fire effects and consequences of failure.
- If fire barriers are to be of a bespoke design or made of materials outside the scope of existing standards additional evidence will be necessary. This may include, for example, fire performance results. As an example, modular barriers formed by combinations of steel plates and/ or steel and reinforced concrete should be designed to provide the same level of fire resistance as the appropriate standard fire barrier would achieve. Performance specifications for fire detection, active fire suppression systems and passive fire barriers should be shown to be appropriate to their duty and environment. Consideration should be given to the functional importance of the plant area, the type and possible magnitude of fire, pertinent characteristics of the location, and existence of substances that may be stored in the area and which could come into contact with fire suppressants.

[1] A divisional fire barrier is a nuclear significant fire barrier which provides the physical segregation between two redundant safety trains.

- The fire detection, alarm and extinguishing systems should be provided commensurate with the fire hazard scenarios stipulated in the safety case and should be appropriately categorised and classified (EHA.16).
- The consequences of flooding from the operation or failure of water, foam or gas based fire suppression systems should be assessed as appropriate and it should be shown that active fire suppression systems are designed and located so that any spurious operation does not impair the functional capability of SSCs or compromise life safety.
- Possible consequences of firefighting water run-off from water-based fire suppression systems should be considered in the design. The measures adopted to control firewater run-off (e.g. use of drains) should ensure that contaminated water is not released into the environment or to areas in which it may pose a hazard to people or the facilities.

5.44 The number, type and level of substantiation of the above safety measures should be aligned with the categorisation of safety functions and classification of SSCs, according to their role in delivering defence-in-depth.

5.45 In order to ensure the operability of the fire protection measures, procedures shall be established and implemented. They shall include inspection, maintenance and testing of fire barriers (and penetrations such as doors, cable and pipe conduit seals, heating, ventilation and air conditioning ducts and dampers), fire detection and extinguishing systems (WENRA RL S5.1). Due consideration should be given to fire protection during modifications and upgrades of facilities, including during the implementation of the modification or upgrade when the fire hazard load may change and similarly the status of and plant reliance on specific SSCs. It is ONR's expectation that WENRA RLs S6 (fire-fighting organisation) will also be implemented, including:

- Adequate arrangements for controlling and ensuring fire safety, as identified by the fire hazard analysis.
- Written emergency procedures clearly define the responsibility and actions of staff in responding to any fire in the plant shall be established and kept up to date.
- A fire-fighting strategy shall be developed, kept up-to date, and trained for, to cover each area in which a fire might affect items important to safety and protection of radioactive materials.
- When reliance for manual fire-fighting capability is placed on an offsite resource, there shall be proper coordination between the plant personnel and the off-site response group, in order to ensure that the latter is familiar with the hazards of the plant.
- If plant personnel are required to be involved in fire-fighting, their organization, minimum staffing level, equipment, fitness requirements, and training shall be documented and their adequacy shall be confirmed by a competent person.

Explosions

5.46 Damaging Vapour Cloud Explosions (VCEs) arise from the ignition of flammable gases or vapours (used or generated during normal operation or under fault conditions) in confined or congested conditions which result in acceleration of the flame front to produce significant overpressure effects. Depending on the subsonic or supersonic characteristics of the flame progression, explosions can involve deflagration and/or detonation phenomena, respectively, with the latter having more destructive effects. Deflagrations can progress to detonation (commonly known as deflagration to detonation transition, DDT) depending on plant geometry. Blast waves from deflagration or detonation events interact with surrounding SSCs including nuclear safety barriers and can lead to failure due to blast waves directly, or impact by entrained debris / missiles

5.47 Other explosions hazards relevant to nuclear facilities may include dust explosions, or Boiling Liquid Expanding Vapour Explosions (BLEVEs). BLEVEs arise from the sudden release and quasi-instantaneous explosive expansion of superheated liquids held under pressure as the pressure boundary fails catastrophically. Apart from blast effects, BLEVEs also involve significant thermal effects (fireballs) when the fluid released has flammable characteristics.

5.48 In the UK, explosion hazards fall within the scope of the Dangerous Substances and Explosive Atmospheres Regulations 2002 (DSEAR) [2]. An explosive atmosphere is defined in DSEAR as a mixture of dangerous substances within air, under atmospheric conditions, in the form of gases, vapours, mist or dust.

5.49 In the assessment of nuclear safety cases, inspectors should expect explosion hazards to be eliminated so far as is reasonably practicable e.g. by substitution of flammable gases or vapours for non-flammable alternatives (EKP.1, EHA.13). Where the hazard cannot be avoided, and subject to reasonable practicability, measures should be provided to prevent accumulation of flammable gas releases, for example adequate ventilation (to prevent flammable concentrations in air), control of ignition sources and the potential consequences minimised by design.

5.50 Inspectors should be satisfied that SSCs important to safety are adequately protected from the explosion effects by, for example, suitably qualified barriers. The safety case should give consideration to the need for redundancy and segregation in the design and layout of these items important to safety (EDR.2, ESS.18) and any barriers providing protection should be rated to withstand the explosion loads.

Explosion Sources

5.51 Inspectors should expect the safety case to systematically document the explosion sources identified according to EHA.1 and 16, alongside with clear descriptions of inventories, flammability / explosivity properties, storage and operating conditions (pressure, temperature), locations etc. Typical explosion sources which may be present in nuclear plant include:

- Flammable gases such as hydrogen either generated by the process (e.g. radiolytic) or stored at site (e.g. for hydrogen injection, generator cooling, or calibration purposes). Hydrogen must be treated with particular care as it has a wide flammability range (with a Lower Explosive Limit (LEL) at 4% in air to a Upper Explosive Limit (UEL) at 75% also in air, very low ignition energy, and hydrogen explosions can be very severe. Different flammability ranges apply in other atmospheres (e.g. in the presence of inert gases such as nitrogen or in steam / oxygen-rich environments).
- Also at some sites, propane and butane are burned to supply heat for carbon dioxide and nitrogen vaporisation and should be considered as credible explosion sources.
- Non-flammable but combustible, high flash point fluids at ambient temperature and pressure can give rise to flammable vapours upon contact with high temperature surfaces.
- Oil mist clouds, which are formed when high flash point fluids such as fuels, oils or lubricants are released from a pressurised system and atomise to a flammable volume can be a significant explosion source.
- Fluids stored at pressure e.g. steam, high pressure non-combustible gases, or when phase changes occur within a confined space (e.g. rapid phase transitions), can give rise to significant overpressures. These are commonly known as physical explosions or non-combustible internal blasts.

- High Energy Arcing Faults (HEAF) associated with high voltage electrical panels / switchgear or high energy transformers, result in a rapid release of energy in the form of heat and mechanical force and should also be identified. Other potential sources are electrical batteries terminal boxes and power cables.
- Highly exothermic reactions and pyrophoric materials may also give rise to significant overpressures. Their possible occurrence in the nuclear plant context should be considered as appropriate.
- Any movement of explosive materials or gases by vehicular transport or pipeline on the site should be taken into consideration in the hazard identification studies.

5.52 In the case of flammable gases, an explosion can take place within the storage container or as a result of a leak. When considering flammable gases transferred or contained in vessels or pipelines, care must be exercised in the selection of the release location, gas accumulation and location of the explosive atmosphere as this may be different to the actual storage location.

5.53 As in the case of other internal hazards, a systematic compartment-by-compartment survey of substances / plant which may give rise to explosions is a key step in developing a robust safety case.

Explosion Hazard Characterisation

5.54 Following the identification of explosion sources, inspectors should expect the safety case to include the results of an explosion hazard analysis. This should characterise, for the sources identified, the consequences of explosions (including relevant parameters such as maximum overpressure and impulse, as appropriate), which are in turn used in the design of the plant and protective / mitigative measures.

5.55 Whilst dutyholders may use any analysis methods and modelling tools that they consider appropriate (e.g. the multi-energy model, CFD codes or even bespoke or empirical models to characterise Vapour Cloud Explosion hazards), inspectors should check that the models are applicable to their intended use, that they are verified and validated within the intended modelling envelope, and any assumptions / data have been considered appropriately (AV.2, AV.3 and AV.4).

5.56 Generally, and as advice to inspectors, the following points represent conservative assumptions / indicators of adequate explosion modelling:

- The analysis is based on unmitigated worst case scenarios (e.g. a stoichiometric concentration of the flammable substance is assumed, ventilation is unavailable to disperse the flammable mix etc.). A number of sensitivity studies may be required to establish the worst case scenario.
- Full bore rupture of pipelines/ pipework carrying / containing combustible gases (or non-combustible gases at pressure) have been considered.
- Chronic accumulation of gases / vapours / stable mists to reach flammable concentrations at the release point or elsewhere in or outside process have been considered.
- The ventilation and substance behaviour assumptions used to derive explosive concentrations (e.g. potential for persistence, stratification) and the time to reach those concentrations are conservative.
- The overpressure levels associated with the reflective shock wave, pressure piling etc. have been considered.

- The potential acceleration of the flame fronts in deflagration events to reach supersonic speeds and detonation has been adequately considered in line with actual plant geometry and configuration.
- The potential interaction of blast waves with plant have been adequately considered included the potential for significant blast waste reflections which may compound the direct effect of the blast.
- Conservative voltage thresholds and fault currents have been selected and justified for HEAF events.
- All SSCs within an appropriate hazard range are assumed lost by the explosion unless suitably qualified for the overpressure and impulse levels arising from the explosion (and against the impact / damage from any debris generated).
- Qualification of equipment against blast effects is generally very onerous and therefore redundancy of SSCs segregated by robust physical barriers is generally preferable unless is not reasonably practicable to do so.
- Specific assumptions during maintenance operations, outages etc. should be developed to take into account the worst permitted configuration including openings through barriers, doors, hatches etc.

5.57 In line with the points above, inspectors should expect licensees' safety cases to identify and characterise bounding explosion load scenarios from the relevant plant operational states. Appropriate explosion consequence analysis should then be developed for each source in turn. Depending on the type of explosive atmosphere, this may involve the following:

- Gas / vapour substances:
  - Quantification of the released inventory based on the substance properties (temperature, pressure, vessel / pipework size and isolation arrangements), and determination of the flammable cloud size based on dispersion analysis. For contained gaseous mixtures, the flammable cloud size in the containment should be determined.
  - The layout and routing of plant systems and supplies, room geometry, confinement, congestion, ventilation in the area of release are all relevant parameters which should be taken into account.
  - Explosion modelling (using appropriate techniques to characterise the explosion overpressure) should determine the hazard range, impulse and overpressure levels.
  - It is generally expected that the load from a vapour cloud explosion on a barrier would be considered as a dynamic load uniformly distributed across the barrier.
  - SSC / barrier response criteria should be set conservatively according to relevant codes and standards e.g. codes for the design of reinforced concrete structures of nuclear safety significance (e.g. ACI codes [23]).
- For Physical Explosions/ blast: the fluid type, properties, all foreseeable operating conditions including pressure and temperature, vessel/pipework size, isolation arrangements, location / geometry and blast modelling results.
- For HEAF the analysis may include:
  - Identification of source characteristics such as voltage, fault current, arc time, arc energy etc. These should be defined in line with relevant codes

and standards e.g. IEEE 1584-2002 [24] and then used to characterise the potential load.

- The dynamic response of the barrier should be evaluated against suitable performance criteria.

- For oil mist clouds explosions the analysis may include [25]:
  - Identification of pressurised substances and their properties e.g. viscosity, density, flash point temperature, system capacity, flow rate / leak size, pressure and design temperature to characterise the potential for the release to give rise to a stable mists.
  - Determination of droplet size, distribution, and percentage of leak converted to mist and volume of mist.
  - Evaluation of the average explosion overpressure from ignition of the flammable mist volume e.g. assuming stoichiometric conditions and using appropriate modelling techniques and design codes (e.g. BS EN 1992-1-1, ACI 349, UFC 3-340-02 [21, 23, 26]).
  - Less conservative approaches may also be considered, but licensees / requesting parties should be expected to document the evidence base for any such approach.

5.58 Inspectors should expect deterministic and probabilistic data used in the analysis to be supported by appropriate references. Explosion model limitations, errors and assumptions should be made explicit and the uncertainty should be identified.

Explosion Safety Measures

5.59 Based upon the explosion analysis and plant availability / responses predicted, licensees should demonstrate that nuclear safety is ensured in all operating states.

5.60 Generally, licensees should follow a series of steps in defining safety measures based on the result of the explosion analysis. Specifically, this may involve the following:

- Determination of the hazard ranges, SSC responses and, consequently, SSC withstand capacity as applicable.
- Based on the design provision and plant / system's nuclear safety significance, confirmation of whether redundancy is required (EDR.2, ESS.18), and specifying segregation, physical separation or isolation requirements accordingly.
- Testing the assumptions and limitations of the explosion characterisation for cliff- edge effects.
- Determine whether combined/ consequential effects such as missile, fire, flood, drop loads etc. could arise.
- Specify the capacity and capability of any gas detection and alarm systems.

5.61 The specific measures provided to deliver nuclear safety will vary according to the plant, however, inspectors should expect the design provision to demonstrate that redundant safety systems remain available e.g. segregated by suitably designed barriers so far as is reasonably practicable, or the plant is qualified to withstand the explosion and consequential hazards (and/or safely shutdown under the conditions of the explosive hazard). The number, type and level of substantiation of the above safety measures should be aligned with the categorisation of safety functions and classification of SSCs, according to their role in delivering defence-in-depth.

5.62 The DSEAR Approved Code of Practice [2] provides guidance that the concentration of dangerous substances should be maintained, during normal operation, below 25% of their LEL by means of appropriate ventilation subject to reasonable practicability. Other standards e.g. BS EN 50272-1:2010 [27] take into consideration the presence of personnel and stipulates stringent design considerations in battery installations. Licensees should identify and apply relevant standards according to the plant type and the nuclear safety consequences associated with failure.

5.63 In developing their judgement on whether explosion risks have been reduced so far as is reasonably practicable, inspectors may seek to check for the following features of good design and operational practice against explosion hazards, where applicable.

- Any processes involving or producing flammable gases use the minimum quantities practicable and take place in well ventilated areas and segregated by suitable barriers from items important to safety (EHA.13). Sufficient procedures and controls are in place to ensure that the level of explosive substances, both fixed and transient, within a compartment do not exceed the design basis with a suitable margin.
- The design and location of SSCs delivering safety functions is optimised against explosions: storage facilities, pipelines carrying flammable / combustible materials and blast sources in general, are segregated from areas containing safety related plant and equipment by qualified physical barriers so far as is reasonably practicable (ELO.4).
- Consideration is given to the need to provide structures forming part of, or supporting barriers, with explosion resistance protection according to their safety function.
- Storage facilities are provided with suitable flammable gas/ vapour / mist detection and alarm systems. The gas detection and alarm system are commensurate with the explosion hazard scenarios stipulated in the safety case and are appropriately categorised and classified (EHA.16).
- Ignition sources (e.g. hot surfaces, flames and hot gases, mechanically generated sparks, electrical apparatus, exothermic reactions (chemical), spontaneous ignition, static charge) should be eliminated so far as is reasonably practicable. The control of ignition sources should be managed to minimise the likelihood of ignition of explosive substances adjacent to or near to items important to safety. Only suitable electrical / mechanical equipment should be used in areas where explosive substances or flammable vapours exist. Such areas should be categorised accordingly using appropriate methodologies e.g. BS EN 60079-10 [28]). Adequate risk assessments are required in areas where there are dangerous and explosive substances present during normal operation under the requirements of DSEAR.
- Electrical panels meet relevant codes and standards [29]. Electric circuits are protected from overload and shorting, including earthing high voltage enclosures. Consideration has been given to arc ducts to safely vent arc flash pressure and hot gases from high voltage panels.
- Consideration has been given to blast resistance of control rooms and buildings, and/ or the alternative locations which may be used to monitor and control the plant in the event of damage to these areas.
- Similar expectations to those outlined in the Fire section apply to penetrations, doors, ventilation dampers in divisional or compartment barriers if these play a role in limiting the effects of explosions.

Flooding / spray

5.64 Flooding and spray hazards arise from failure of pipework or tanks containing any process fluids. Typically flooding sources involve fluids as a liquid phase, however rain-out or condensation of vapours e.g. from steam releases are also credible sources.

5.65 Flooding safety cases should not only consider water e.g. from general cooling water services, fire suppression systems, boiler feedwater and condenser cooling water supplies, roof leaks or failure of internal rainwater downpipes, but also coolants, oils or any other chemicals kept in storage, process vessels, etc.

5.66 This TAG covers flooding as an internal hazard, i.e. when its occurrence is within the control of the licensee. It covers flooding inside and outside buildings, but the flooding sources will normally be within the site boundary and therefore within the control of the licensee.

5.67 Flooding from external hazards as defined in the SAPs, e.g. high rainfall / storm events, riverine or coastal flooding or elevated groundwater levels are considered external hazards and are addressed in NS-TAST-GD-013 – External Hazards [30].

5.68 Flooding and spray releases can result in damage to SSCs by wetting or hydrostatic loading. Flooding can result in criticality hazards to arise in, for example, fuel fabrication facilities due to increased moderation. Inspectors should expect safety cases to demonstrate how the design of the facility prevents water / fluids from adversely affecting SSCs (EHA. 15).

Hazard Sources

5.69 Generally, and as a starting point, dutyholders would have identified and recorded all internal flooding sources according to the fluid type, pipework layout, inventories and isolation arrangements credited in line with EHA.14. This should include locations with towns water supplies or any other potentially very large flood inventories (including those where isolation would result in unacceptable nuclear safety consequences in the event of an accident).

5.70 Design characteristics of systems involved such as pipework diameter, pump or fluid head, upstream restrictions to flow etc. should be well understood, as they will determine the dynamics of the flooding event and the worst-case unmitigated consequences.

5.71 Inspectors should expect the design basis events to include foreseeable failures such as full bore pipework ruptures which should be postulated in the worst operational state and/or with least control (mode of operation with the highest energy). The consequences of such events (releases from a double ended guillotine break) should be analysed accordingly.

5.72 In addition to the general points, inspectors should also consider the following points when undertaking their assessments:

- The hazard analysis should include flooding and spray hazards originating from both random and common cause failures, including component failures and human error.
- The state, physical and chemical properties of the fluids should be taken into account in the analysis as they may lead to distinct SSC damage e.g. rapid erosion due to particulate impacts, chemically-induced corrosion etc.
- Sprays or condensing steam may pose a risk of pooling at higher elevations such as within cable trays, open penetrations or vent ducts and therefore should also be considered in safety cases.

- The intended or accidental operation of fire protection systems should be considered as internal flooding sources. Water or other extinguishing media from fire suppression systems has the potential to pass into safety related rooms e.g. through cable trays and risers and result in spurious operation or failure of items important to safety.
- The design of the plant should include adequate provision for identifying and collecting fluid discharges from any failed systems on site.
- The interfaces between internal and external hazards should be adequately managed. For example, there are consequential internal flooding hazards associated with responses to external hazards effects e.g. thawing conditions following clearance and storage of snowfall can result in internal flooding.
- The interfaces between internal hazards, mechanical engineering and structural integrity should be adequately managed. The safety case may assume that certain failures that could lead to a flood cannot occur because the plant (pipework vessels, etc.) is of highest integrity. Any such claims would need to be considered by structural integrity assessors, and the impact of hazard loadings on those plant items also needs to be considered.
- Interfaces with other specialisms include process engineering on the design aspects and criticality hazards due to water.

Hazard Analysis

5.73 For all potential flood scenarios identified to pose a hazard to nuclear plant, inspectors should expect safety cases to identify the maximum flood level for the room / area which contains the source and all areas where the flooding inventory could spread by gravity or other means e.g. pumped drainage systems. There should be a clear link between the maximum flood level and the design capacity of compartment barriers against the hydrostatic loading.

5.74 The flood level as a function of time as well as other dynamic effects such as wave formation (e.g. as a result of a dropped load into a pool, bund overtopping or failure of doors) or cascading effects (stairwells / flow through penetrations) may impact SSC and should be considered by dutyholders as appropriate.

5.75 Any reliance on drainage systems should also be documented, including their capacity, layout, connections with systems and compartments, ultimate receptors e.g. sumps, as they play a role in primary and/or secondary flooding and can play a role in the spread of contamination or lead to consequential hazards e.g. running pool fires.

5.76 Flooding analysis will usually consider that flooding can spread through any available opening, such as penetrations in walls, floor gratings, stairwells, vents, drains and gaps under doors.

5.77 Plant layouts and 3-D plant models are often valuable in displaying flood paths and key barriers to flood progression.

5.78 Safety cases should identify flood doors and non-flood doors in their role in facilitating or preventing progression of flooding events, and should be classified accordingly in line with their nuclear safety significance. If drains are claimed to remove flooding inventories from specific areas, the capacity, layout and features delivering isolation of the drain system from other nuclear safety significant plant should be confirmed. Inspectors should also consider whether failure to drain (e.g. where drains are blocked by debris) or pumping is not available e.g. upon consequential loss of power would give rise to cliff-edge effects, and that these have been considered in the safety case.

5.79 Inspectors should satisfy themselves that all reasonably practicable means are provided to address the consequences of unisolatable releases e.g. failure to shut off very large / 'inexhaustible' inventories or those where continued injection is required to maintain a minimum level to prevent severe radiological consequences.

5.80 ONR expectations on deterministic analysis, treatment of cliff-edge effects, time-at-risk and worst operational state outlined in the general sections apply to internal flooding and spray hazards.

Safety Measures

5.81 Inspectors should seek assurances that relevant SSCs remain available to ensure nuclear safety under flooding hazard conditions. In line with the general considerations, this is preferably achieved by segregation i.e. provision of redundant SSCs in separated flood compartments, substantiated against the highest hydrostatic load so far as is reasonably practicable, or by placing SSCs at heights above the maximum credible flood levels.

5.82 Alternative approaches such as qualification of SSCs to remain operational under hazard conditions (e.g. under flooding, steam or spray release) or combination of segregated SSCs and qualification of equipment may be appropriate where full segregation is not reasonably practicable.

5.83 Inspectors should also take into account the following considerations when judging the adequacy of internal flooding safety cases.

- Drainage, provision of drip trays and installation of equipment above floor level may be employed to minimise the effect on items important to safety including electrical control and protection equipment. Inspectors should seek to understand the level of reliance placed on leak tightness and drainage availability which may degrade during the lifetime of the plant.
- Where equipment is wetted through exposure to humidity, spray or submergence, inspectors should liaise with the relevant disciplines including Electrical, Control & Instrumentation specialists with regards to the suitability of equipment qualification provided.
- Where there is potential for flood water to exert hydrostatic loads on SSCs including flood barriers, doors and penetrations, inspectors should assure themselves that the safety case adequately addresses the consequences of localised failures and there are no cliff-edge effects for which the consequences of failure would be significantly more severe than those provided for in the design basis. Inspectors should liaise with civil engineering or mechanical engineering assessors as appropriate relating to loads on structures or equipment.
- Where operator actions play a role in preventing or mitigating the consequences of flood scenarios, e.g. by isolating the flood source / paths, then the feasibility of performing the required actions under the hazard conditions is a matter for consideration by Human Factors and/ or Radiological Protection specialists in conjunction with Internal Hazards. Inspectors should ensure that the safety case assumptions and calculations (available response times, flood levels) are compatible with the release scenarios and proposed actions (e.g. deploying defences, closure of flood doors etc.). This should also consider how the flood will be notified to operators with a sufficiently reliable system that is subjected to EIM&T.

5.84 To form an overall judgement on the adequacy of the safety case, inspectors should satisfy themselves that defence-in-depth (EKP.3) against internal flooding effects is

achieved by an adequate balance of measures according to the hierarchy of measures in the SAPs (para. 155). Accordingly, preference should be given to inherently safe design options and engineered measures versus operator intervention, and the overall ALARP demonstration should be underpinned by suitable optioneering, arguments and evidence.

Hot gas and steam release

Hazard sources

5.85 In the context of the existing fleet of Advanced Gas Reactors (AGRs), hot gas releases are generally associated with releases of carbon dioxide, the primary coolant of the reactor pressure vessel, which is held at a pressure of approximately 40 bar. Although this is currently the most well-known source of hot gas release in an UK nuclear power reactor context, consideration should be given to other potential sources which may be present in nuclear facilities.

5.86 Loss of gas from the reactor pressure vessel leads to a reduction of the cooling efficiency and a significant loss of gas can result in fuel failure and potentially very significant radiological consequences. These are the direct consequences of the fault and are generally considered by Fault Studies inspectors. Additionally, other effects from the release can arise through direct impingement or as a result of the global heating effects and should be considered by internal hazards specialists.

5.87 Steam release is associated with failure of steam pipework or vessels, and includes failures of water filled systems operating at temperatures in excess of 100°C.There are similarities with the hot gas release hazard, but it is sufficiently different to be considered as a separate hazard e.g. environmental moisture effects.

5.88 The assessed frequency of significant failures in the steam or water-filled pipework systems may relate to structural integrity arguments, so it is advisable for internal hazards inspectors to discuss these aspects with structural integrity or mechanical engineering specialists.

5.89 Vessel or pipework failure may result from internal failure mechanisms, such as crack propagation or penetration failures, but there may be other (non-structural) causes. In particular some steam releases may be caused by human failure / mal-operation, or by external challenges, such as impacts from dropped or traversing loads. The basic assumption is that failures are possible, unless the components of the system are claimed as High Integrity (with associated implications for design, procurement, quality assurance (QA), commissioning and in-service inspections).

5.90 Safety cases should identify all hot gas and steam release sources, including the fluid, key design features and normal operating conditions, isolation arrangements e.g. response time in case of failure (EHA. 1 and EHA.14).

Hazard characterisation

5.91 The assessment of consequences of hot gas and steam releases should be supported by assumptions consistent with the level of uncertainty associated with the hazard. Leak detection before gross failure (leak-before- break) is not generally accepted as a primary safety claim. ONR's expectation is that assessment of the consequences will have considered a full circumferential guillotine break and a double ended release of material from both ends of the pipework.

5.92 Following identification of hot gas/ steam release sources, the analysis should identify the release paths including all relevant features e.g. barriers, penetrations including any unsealed penetrations and engineered pressure relief provision.

5.93 In the assessment of overpressure levels and temperature distributions across the hot gas / steam release compartment / route, it should be considered that full room volumes are not available to accommodate the released material and reduction factors are applied according to the level of congestion by plant and equipment. Whilst the reduction factors are subject to plant-specific considerations, this should be suitably conservative so that they capture the worst case plant configuration and room utilisation in all credible plant operating states.

5.94 Consequences from steam release can include both pressure and temperature effects, and include moisture/humidity effects. When judging the adequacy of the safety case, inspectors should consider the following:

- The pressure effects are generally short term but generally depend of the steam inventories released and, in turn, system isolation times e.g. via excess flow isolation valves. Any restrictions to release duration, break sizes and thus inventory released will need to be supported by design evidence e.g. performance requirements.
- The event consequences include local disruptive effects – these include pipe whip, effects of jets on structure and plant items, local pressure effects in constrained spaces or close to the point of release. This should be considered as combined events and the cumulative effects on SSCs evaluated.
- Pressure effects may include global effects from room pressurisation, leading to structural challenge on walls, floors, ceilings, doors, windows, cladding, etc. This may occur at a significant distance from the release point e.g. through the engineered release route. The integrity of the route including weakest points e.g. thinnest barrier, penetrations should be demonstrated and supported by design evidence.
- Temperature effects can be both near field and far field, and may change as the release continues.
- Local temperatures are strongly influenced by the conditions of the fluid released. For example, items or building elements suffering jet impingement may rapidly warm up to the temperature of the escaping fluid. There can also be significant combined effects e.g. high pressure jets of hot gas may chemically react with concrete e.g. carbonation and also physically erode the surface in the jet's cone of influence.
- Temperatures in the far-field will be affected by heat losses through engineered routes e.g. ventilation systems, so detailed modelling may be necessary.
- Plant away from any local effects, may still be exposed to local moisture/humidity conditions, elevated temperatures and overpressure which they may need to withstand.

5.95 If the safety case requires modelling of the effects of the steam release, inspectors should look for robust modelling and adequate conservatisms. Simplified modelling approaches may give useful scoping results, but there is the possibility that too much weight is given to the predictions, especially as these may not model all the physics of the release. In particular:

- Modelling may be undertaken with a granularity that will not fully represent local effects.
- Modelling may include assumptions on mixing that does not fully allow for flow separation, wall attachment of flows, etc.

- Modelling may make assumptions about the heating, ventilation and air conditioning (HVAC) system performance and availability.
- Modelling may assume a break size and isolation time, which will need to be supported by evidence and performance requirements.

Safety measures

5.96 Efforts should be made to minimise the number and energy of the steam and hot gas release sources, and to place them in areas furthest away and preferably segregated from nuclear safety significant plant (by suitably qualified barriers and penetrations) so far as is reasonably practicable. In conjunction with this, there may be features to direct the gas via an engineered route away from release points out to open air via vents, louvres, or quick release dampers. In some cases it has been necessary to qualify essential SSCs against the effects of the hot gas. The hot gas release strategy requires suitable design and qualification of the vent route boundary including barriers and penetrations e.g. doors and blowout panels, etc.

5.97 Typical protection and control measures against hot gas and or steam releases may include:

- Design of barriers and structures against the maximum credible overpressure along the vent route, local strengthening of structures – or deliberately opening up vent routes e.g. via doors or panels to prevent local pressure build up / high differential pressure across structures (EPS3 and EPS. 5).
- Pressure relief provision – such as automatically opening louvres or blowout panels. If these are used, modelling may need to be carried out to determine the pressure “overshoot” above the set points to ensure that sensitive structures will not fail and suitable margins should be built in the design and specification of the pressure relief provision.
- Temperature and humidity effects may be controlled by additional vent provisions. For example, HVAC may be expected to clear the air of high temperature or high humidity. Alternatively passive ventilation may be utilised – possibly with a combination of high level and low level openings to promote natural draft.

5.98 It is generally preferable to ensure that the potential for equipment to be affected through the vent route is factored in the design by provision of suitably segregated, redundant equipment elsewhere in the facilities. However, where this is not reasonably practicable, it may be the case that equipment cubicles, electric panels and plant may be expected to withstand high temperature and humidity conditions. Suitable design and performance requirements supported by qualification in the conditions of the steam / hot gas release hazard will then be necessary along with an attendant inspection and maintenance regime.

5.99 It should be noted that safety cases could refer to design standards which are intended against different challenges. For example, a cubicle or electrical enclosure may be marked IP55, because it has been designed against the requirements of IEC 60529 [31] for its ingress protection against solid objects, dust, and water spray. This IP rating does not automatically guarantee its performance in resisting steam or moisture ingress; however, the features of the cubicle or enclosure which provide dust and moisture protection may also be effective against the steam hazard. Inspectors may choose to sample the licensee’s evidence base for any claimed withstand capability.

5.100 Protection and control measures will need to be subject to in service EIM&T and should be formally documented equipment schedules, which should cover all relevant parts of the systems. There have been occasions, for example, when relief louvres

have not been maintained adequately. Similarly, cubicle withstand protection may be disturbed by work in which the cubicle is opened – it is expected that licensees manage the restoration of these protection features in the process of returning the cubicle to normal service.

Pipe Whip and Jet Impact

5.101 Pipe whip and jet impact are local dynamic hazards associated with the failure of pressurised equipment.

5.102 Pipe whip occurs when high pressure pipework fails in a catastrophic manner e.g. a double ended guillotine break, and the resulting energy release causes the pipe to develop a plastic hinge around a fixed point, bend and whip. The resulting movement of the pipework can impact neighbouring SSCs in the trajectory, other pipework, vessels, barriers, etc.

5.103 Jet impingement occurs when the fluid released from the failure of the pressurised components (pipework, vessel etc.) impacts upon nearby equipment or structures.

5.104 Both pipe whip and jet impacts on safety significant structures, systems and components (SSCs) including nuclear safety significant barriers can cause them to fail and impair delivery of the FSFs.

Hazard sources

5.105 Inspectors should expect safety cases to postulate pipe whip events resulting from double ended guillotine breaks of pipework when the systems are operating at high energy.

5.106 In line with the General considerations previously stated, Leak detection before gross failure (leak-before- break) is not generally accepted as a primary safety claim by ONR. ONR's expectation is that assessment of consequences will assume a full pipe fracture. Whilst there are systems which may be operating in high energy mode during short periods of time, inspectors should expect to see that pipe whip is postulated in the most onerous initial operating state. The short duration of the mode of operation should not be used to exclude it from analysis, or to consider consequences of failure at low energies exclusively.

5.107 It is generally considered that pipes operating below the high energy threshold would not whip, however, consideration should be given to cliff-edge effects especially for systems operating close to the above pressure/ temperature levels (EHA.7). The assumption for no pipe whip below 2.0MPa is not rigorous. ONR assessors should be open to the potential for some level of whip with flexible pipe work or some low schedule pipework on lower pressure systems. These impacts should not be damaging to walls or structures, but should be considered for the potential effects fragile plant components such as delicate instruments. Simple assessment or screening methods may be acceptable for these low energy impacts.

5.108 Pipe breaks for systems at low energy is covered in the general considerations section, and the flooding and spray hazards sub-sections as appropriate; jet impact at lower energies can still lead to significant effects on plant and are considered in this section, together with high energy pipe failures. Expectations on postulated pipe break locations are discussed in the General section and apply to all the above hazards.

Hazard analysis / characterisation

5.109 The effects of releases from high energy pipes are commonly modelled utilising computer models to predict the local and global effects. The predicted effects of such a release are sensitive to the granularity of model used and therefore it is important to understand the basis of the model, any underlying data used, the history of its development, and evidence of appropriate verification and validation.

5.110 Pipe whip and jet impact can be characterised using codes, standards and guidance such as that available in the R3 Impact Assessment procedure [32], ANSI/ANS58.2-1988 [33] or rules defined in NUREG 0800 [34]. These are considered as an acceptable starting position for hazard characterisations, however, safety cases should take into account their limitations and status of development at the time the analysis is undertaken.

5.111 It is generally considered that the worst case unmitigated consequences e.g. assuming the most onerous plant state and hinge location, no restraints, longest length or unrestrained pipe or sweeping angle should be assumed as a starting point to show the resilience of the design.

5.112 It is generally expected that the analysis will be based on pipework layouts and room dimensions, geometry and SSC layouts. Whilst simplification and assumptions may be made for ease of analysis (e.g. assuming longest length of unrestrained pipe equal to room dimensions etc.) these may be appropriate for an initial screening and are likely to result to very pessimistic results and significant challenges to SSCs.

5.113 The pipe whip and jet impact (local and global) effects should be evaluated using appropriate codes, standards and guidance e.g. R3 Impact Assessment procedure, and inform the design of the targets to demonstrate resilience according to their nuclear safety significance e.g. perforation, penetration or scabbing of barriers does not occur or the plant remains adequately protected and would not result in radiological consequences. Coordination with relevant ONR specialists, primarily Civil Engineering, Structural Integrity and Fault Studies in this area is essential.

Safety Measures

5.114 For pipe whip and jet impact effects, consequences can be limited by designing structures systems and components to withstand the effects of pipe failures e.g. barriers, and providing segregated redundant SSCs which remain unaffected by the postulated failure. Similarly, there are established ways of reducing the likelihood of pipe failure, for example, raising the construction class and associated provisions for structural integrity.

5.115 With respect to pipe whip, the extent of whipping can be reduced or eliminated by appropriate restraint design, which should be substantiated against the forces exerted.

5.116 Similarly, barriers such as reinforced concrete barriers and shields may prevent impact to nuclear safety significant SSC and should be substantiated against the dynamic and global loads exerted by the pipe whip and the jet.

5.117 The closure of isolation valves may be used where possible to limit the duration of the high energy fluid release and associated jet impact, and this should be supported by adequate design substantiation and performance requirements.

5.118 The number, type and level of substantiation of the above safety measures should be aligned with the categorisation of safety functions and classification of SSCs, according to their role in delivering defence-in-depth.

Internal Missiles

5.119 Pressurised components (e.g. pipe work, valves and pressure vessels etc.) and rotating machinery (e.g. turbine-generators, diesel generators, pumps, fans, blowers, compressors etc.) can fail disruptively ejecting highly energetic fragments which can damage SSCs important to safety and hence compromise the delivery of safety functions. Similarly, chemical or physical explosions can give rise to missiles which have the potential to exert a similar level of damage.

Hazard sources

5.120 Safety cases should identify the sources of possible missiles including pressurised vessels, pipework and components, rotating machinery and systems which can contain explosive mixtures under normal or fault operating conditions (EHA.1 and EHA.14). They should also identify the frequency, trajectory of the generated missiles, and consequences of impact on targets important to safety.

5.121 Inspectors should expect, particularly for new nuclear plant, that the number and energy of missile sources have been minimised, and their location chosen to ensure that the impact on nuclear safety significant plant is eliminated or reduced so far as is reasonably practicable.

5.122 The frequency of the initiating event (based on failure frequency of the relevant equipment should be developed) and justified. Inspectors should expect safety cases to provide an assessment of consequences for missile impacts within the Design Basis.

5.123 Probabilistic arguments alone should not be used to exclude assessment of missile sources or impacts/ strike on SSCs or nuclear safety significant plant.

Hazard analysis

5.124 When assessing internal missile safety cases, inspectors should expect that:

- Due consideration has been given to the type of missile i.e. whether it results from failure of rotating or high pressure equipment, and estimates of the kinetic energy of the missiles are developed accordingly.
- Key parameters and assumptions made in the evaluation of the missile energy include the size and geometry of the fragments ejected, and any credited loss of energy through interaction with equipment (e.g. rotating machinery casing, SSCs). It is necessary that any values used are supported by adequate design evidence. The hazard analysis should take into account the considerable level of uncertainty associated with failure modes and the characteristics of the missiles by making bounding assumptions on energy losses e.g. it is assumed that there is no loss of energy during the rupture of the vessel, the energy is released instantaneously, the largest credible fragment is released or there is no energy loss through interaction of missiles with the casing (rotating machinery).
- The trajectory of missiles is subject to high levels of uncertainty as a result of the uncertainty inherent to the missile fragment formation, the complex interactions between the fragment and equipment. Bounding arguments should therefore be expected e.g. consider that damage from internal missiles may occur in any direction from the source.
- It should be noted that, in the development of bounding arguments, the energy of the missile fragment is not the sole factor to be considered. A holistic view should be taken to include the location, vulnerability and nuclear safety significance of the SSCs potentially affected, and other internal hazard sources which may be located in the vicinity.
- Models used to estimate the energy, trajectory and consequences of missile impacts should be adequately verified, validated and applied within the limits of

application. A compilation of characterisation models and methods for internal missile hazards is available, for example, in the R3 Impact Assessment procedure [32] but others may also be appropriate.

5.125 The response of missile targets e.g. barriers, other SSCs should be evaluated and consideration should be given to the high levels of uncertainty inherent to missile sources-target interactions. Margins of safety should be built-in with suitable analysis assumptions e.g. it may be appropriate to consider that the fragments behave as a hard missile (a negligibly small proportion of the energy of the missile is dissipated in trajectory and the full kinetic energy of the fragment is transferred to the target).

Safety Measures

5.126 The results of a hazard analysis in conjunction with the designers' acceptance criteria should be used to verify the adequacy of protection provided by spatial segregation, protective barriers, and redundancy in safety related items and safety systems. Consideration should be given to the need for ensuring that control rooms and buildings are missile and/or blast resistant, and that there are suitable alternative arrangements in the event of damage to these areas.

5.127 Hazards should be avoided or minimised e.g. by use of low energy equipment but, where they are not avoidable; items important to safety should be protected by spatial or physical barriers, suitably substantiated against the postulated missile impacts. Rotating equipment casings should be suitably designed and manufactured to eliminate or reduce the potential for missile ejection so far as is reasonably practicable.

5.128 In the development of safety cases, consideration should be given to a need for redundancy and segregation in the design and layout of items important to safety to mitigate against any potential threat from missiles.

5.129 In line with the general expectation, the number, type and level of substantiation of the safety measures should be aligned with the categorisation of safety functions and classification of SSCs, according to their role in delivering defence-in-depth.

Turbine Missiles

5.130 Existing nuclear power stations generally convert energy from nuclear fission into steam which is then converted into electric power via steam turbines.

5.131 Steam turbines are large heavy rotating machines and they can fail disruptively following either a ductile or brittle failure or from an event external to the turbine. Similar turbine disintegration events can arise from other gas turbines e.g. such as those used at a number of reactor sites for auxiliary power or those proposed for Advanced Nuclear Technologies (e.g. supercritical carbon dioxide-driven turbines, helium-driven turbines).

5.132 Turbine disintegration events have the potential to eject large fragments from their casing travelling at high velocity and thus cause significant damage to safety related buildings and plant.

5.133 The significance of turbine disintegration events as an internal hazard is recognised in relevant good practice including IAEA guidance [13, 35].

5.134 Inspectors should therefore expect safety cases to include turbine disintegration events within the design basis and demonstrate that the events will not disable safety related plant and equipment or that there is an adequate combination of engineered safeguards and management controls to reduce the risk so far as is reasonably practicable (EHA.1, EHA.3, EHA.6, EHA.5, and EHA.14).

Hazard Sources

5.135 Turbine disintegration can occur via a brittle failure, which may be initiated by stress corrosion cracking in combination with low fracture toughness, or issues with weld quality, and low fracture toughness which may also occur at low speed. Another potential initiator for turbine disintegration is via an overspeed ductile failure.

5.136 The number and velocity of turbine missile fragments ejected is subject to considerable uncertainty and will depend on the design and fabrication of the specific turbine under consideration. Inspectors should expect failure to be conservatively postulated e.g. disk ruptures to result in several fragments which would impact adjacent disks resulting in a number of missiles ejected from the turbine cases. Both high and low trajectory missiles should be postulated.

5.137 Internal Hazards inspectors should seek advice from structural integrity and mechanical engineers on the postulated failure modes and the likely missiles that would be generated according with the turbine designs.

5.138 A turbine disintegration can also be initiated following damage to steam turbines caused by other events including but not limited to:

- dropped loads;
- vehicle collision;
- structural collapse;
- earthquakes.

5.139 These initiating events should be understood by the licensee / requesting party and the turbine set designed in such a way that it is either robust against the initiator or show that a case can be made that following a turbine disintegration, the plant can be safely shut down and maintained in a safe condition.

Hazard analysis

5.140 Based on the failure rate of steam turbines (around 10^{-4} per year), inspectors should expect safety cases to postulate and analyse turbine disintegration events within the plant's design basis.

5.141 In the analysis of turbine disintegration consequences, particular attention should be given to the area where missile fragments are considered to concentrate i.e. location of buildings on either side of the turbine axis, but evidence is available which shows the ejection of missiles further afield and therefore these should also be studied proportionately for cliff-edge effects (EHA.7).

5.142 IAEA guidance (IAEA NS-G-1.11) [10] provides plant layout expectations to address areas at particular risk of turbine missile impacts. Specifically, it indicates that the layout of the main turbine generator should be such that potential critical targets (such as the control room) lie within the area least susceptible to direct strikes from the turbine; that is, within a cone with its axis along the axis of the turbine shaft. This arrangement takes account of the fact that large fragments, if ejected, will tend to be expelled within 25° of the plane of rotation. It is considered that the above arrangement does not eliminate the possibility of the fragments hitting a critical target, but significantly reduces the probability of a direct strike.

5.143 General expectations on turbine disintegration analysis and plant design against the consequences of turbine disintegration events as per above can be found in the US NRC RG1.115 [35].This US NRC regulatory guide expects missile protection for relevant SSCs to ensure the integrity of the reactor coolant pressure boundary. It also expects that the plant can be shut down (and maintained in a safe shutdown condition)

or that the plant is capable of preventing accidents resulting in potential offsite exposures, as applicable.

5.144 When assessing the turbine disintegration safety case, inspectors should check that the above considerations have been reflected in the proposed layout, subject to reasonable practicability. It should be apparent that the design provides a sufficient set of safety related equipment for containment, cooling and criticality control that will survive a turbine disintegration event, preferably by layout considerations, and by provision of redundant systems as appropriate. Examples of facilities and SSCs which should be considered in the assessment include (but are not limited to) the following:

- Back up diesel buildings;
- Pump houses;
- Heat exchangers;
- Spent fuel storage;
- The effect on adjacent turbines / domino effect;
- Turbines on adjacent facilities;
- Spread of contamination via primary circuit steam (boiling water reactors).
- Any SSCs that would give rise to secondary internal hazards, for example, fire, flooding and gas release etc.

5.145 Safety cases may opt to include calculations or modelling which justify the number, size and likely location of missiles. These calculations/models should be appropriately developed, validated and verified for the proposed turbine and plant design.

5.146 A probabilistic argument alone e.g. to support unfavourable layouts and lack of design provision against turbine disintegration is not acceptable and risk should be demonstrated to be ALARP.

Safety Measures

5.147 Based on the above expectations, inspectors should expect safety measures against turbine disintegration events. These would preferably consist of favourable layout considerations to prevent missile strikes on key facilities and plant, and include protection and mitigative features to ensure that nuclear safety functions continue to be delivered following a turbine disintegration event. The following is a list of typical measures provided in safety cases:

- Good turbine design, fabrication and maintenance according to relevant codes and standards. Internal Hazards inspectors should seek views from mechanical engineering and structural integrity specialists as to the suitability of plans and approaches in these areas.
- Layout of plant in relation to turbines / positioning of key safety related equipment. Inspectors should expect plant and equipment important to safety to be located away from the turbine axis where practicable and/or spatial separation / distribution across the site of multiple safety systems to ensure survival of key safety related equipment, back-up power supplies etc.
- Regular inspections of the turbine set to identify, for example, signs of stress corrosion cracking or other hazard initiators. Internal hazards inspectors should check the suitability of the licensee's / requesting party's proposals in this area with structural integrity inspectors.
- Overspeed protection to prevent turbine overspeed events and reduce the potential for ductile failure. Internal hazards inspectors should discuss the suitability of the proposals in this area with electrical, control and instrumentation specialists.
- Civil structures expected to protect plant from missiles as a result of turbine disintegration should be suitably substantiated against relevant turbine missile

strikes. ONR Internal Hazards specialists should seek views from civil engineering specialists on the design substantiation available in the safety case for any proposed or existing civil structures acting as barriers to protect relevant safety related equipment.

Dropped loads

5.148 The internal hazard of dropped loads includes any item that is dropped, swung or otherwise falls or is lowered out of control. Dropped loads may be the result of mechanical failure of nuclear related lifting equipment, structural failures caused by external hazards (such as high winds, seismic event), local hazards (such as impact from a heavy load following an uncontrolled swing) or human error (such as incorrect slinging or attachment).

5.149 The potential consequences of dropped loads in nuclear plant include damage to containment of nuclear matter, redistribution of nuclear material into hazardous configurations (leading to a criticality event), loss of bulk shielding leading to shine paths/ increased radiation dose, or damage to SSCs important to safety. As loss of control of loads can result in impacts to SSCs, they should therefore be considered as a potential initiator of fault sequences with nuclear safety consequences.

5.150 The use of cranes and other lifting equipment is covered within NS-TAST-GD-056, Rev 3 - Nuclear Lifting Operations [36]. However, the threats associated with dropped loads as an internal hazard and the potential consequential hazards e.g. fire, explosion and flooding are considered within this guidance.

Hazard sources

5.151 In the context of nuclear plant, typical lifting equipment includes the following:

- Cranes (which can be mobile, telescopic, tower, truck mounted [also known as boom or picker truck], loader, overhead, Turbine Hall, reactor pile cap, polar, dockside or pool-side, luff, construction, mobile, runway beams and long travel girders);
- Drum or flask handling machines;
- Maintenance hoists and chain blocks;
- Fuel handing machines
- Fork lift trucks;

5.152 Other hazard sources include any item of plant, equipment or building fabric which are located at an elevated level compared with SSCs and which may become dislodged, for example: in older facilities equipment above gloveboxes could fail and fall due to corroded fixings and brackets; or items stored on a mezzanine floor which could be pushed through railings or a tool dropped due to human error.

Hazard analysis

5.153 The approach expected for the analysis of dropped loads involves the assessment of the consequences of dropped loads on nuclear material and safety significant SSCs which results in the determination of the limits and conditions of operation of, for example, the lifting equipment, detailed load paths, and systems and administrative controls that need to be in place.

5.154 The response of nuclear plant and structures to a dropped load can be estimated using a wide range of tools e.g. the R3 Impact Assessment procedure [32] or Finite Element Analysis (FEA). These are considered as an acceptable starting position for hazard characterisations, however, safety cases should take into account their limitations and

status of development at the time the analysis is undertaken. Additionally, the chosen model and impact criteria should be supported by suitable evidence or analysis.

5.155 The energy of the impact from a dropped load is directly proportional to its mass and the height of the drop. The severity of the impact on SSCs depends on the energy of the impact, the geometry and shape of the dropped item and the characteristics of the target.

5.156 The energy of the impact from swung loads and drop loads can be estimated via relatively simple calculations. However, inspectors should check that adequately conservative assumptions have been made e.g. the mass of the load dropped includes that of any attachments and lifting devices where applicable, and that the specific vulnerabilities of SSCs have been taken into account.

5.157 It should be assumed that any load which may be lifted or carried may be inadvertently dropped and therefore the frequency of dropped loads with the potential to damage SSCs important to safety and the extent of possible damage should be estimated and its significance assessed.

5.158 All lifts, whether of nuclear or non-nuclear materials within, or in the proximity of, nuclear installations should be assessed to determine whether they pose risks with nuclear consequences. Consideration should be given to whether vulnerable material or SSCs lie within the:

- Drop radius, i.e. immediately underneath the movement path of the load.
- Swing radius, i.e. within the area over which the load might swing if given a suitable impetus.
- Throw radius, i.e. within the area into which the load could be thrown should it be given sufficient energy to break its tether.

Safety Measures

5.159 As per NS-TAST-GD-056, Rev 3 - Nuclear Lifting Operations [36], there are no SAPs that specifically mention lifting operations or lifting equipment. ENM.2 considers the arrangements for the safe management of nuclear matter and such arrangements may include the provision of handing and lifting systems.

5.160 Adherence to the LOLER [4] and PUWER ACOPs [37] is a fundamental starting point from which to seek compliance with the law. The assessor should confirm that required aspects of the regulations are met. Details are not reiterated here but cover the general topics of (not inclusive):

- Strength and stability;
- Lifting equipment for lifting persons (may be relevant to nuclear when nuclear items are hand-carried or moved by trolleys etc. via elevators or escalators)
- Positioning and installation;
- Marking of lifting equipment;
- Organisation of lifting operations;
- Examination and inspection;
- Reports, defects and retention of information;
- Training and competence;
- High and very low temperatures;
- Controls.

5.161 Where practicable, nuclear safety significant slabs or walls (or those whose consequential failures would be similarly challenging) should be substantiated to the highest energy drops or additional protection or operating restrictions should be provided.

5.162 In reaching an overall judgement on the adequacy of a dropped load safety case, ONR internal hazards inspectors may seek assurances from the following specialisms (this list is not intended to be exhaustive):

- Mechanical Engineering specialists (regarding the design and operation of the lifting equipment);
- Civil Engineering specialists, who can confirm, for example, the adequacy of walls or structures onto or into which the cranes are supported;
- Control and Instrumentation (C&I) and Human Factors specialists, for the design of control systems, load detection systems, selection and use of equipment and correct operational procedures and human-machine interfaces. Many lifting operations have high levels of operator input and control.
- Civil Engineering Specialists, regarding the adequacy of SSC responses and structural withstand of nuclear plant e.g. reinforced concrete slabs.
- Conventional Safety specialists in relation to the application of LOLER and PUWER to specific lifting equipment and operations.

5.163 The following are indicators of adequate safety cases:

- The safety case considers all sources of dropped loads, whether as a result of lifting operations specifically, or intended or unintended drop of plant from height.
- The safety case shows that optioneering has been undertaken to identify whether the lifting activity is actually necessary, and to identify the preferred method and equipment for undertaking the lift;
- The safety case shows that lifting over/near safety significant SSC's is avoided, and the height of the lift minimised so far as is reasonably practicable.
- The safety case shows that items / packages containing nuclear matter are designed to retain their integrity following the worst case impact.
- The safety case clearly defines acceptable routes for loads being carried by lifting equipment and the applicable limits and controls.
- The safety case considers the various potential effects of dropped loads on SSCs (including civil structures in nuclear plant) and should include: penetration, spalling, cone cracking and perforation.
- An impact from a dropped load can cause multiple system failures and consequential hazards, for example, may include the release of a combustible gas or liquid, coupled with loss of the engineered fire protection system.
- A quantitative assessment of the lift is provided. This should consider: the equipment used; items being lifted; the local environment; the potential for crane overlift, energy of impact of drops, potential for energy transfer (e.g. catapulting of load); effect of rotational inertia; and required Factors of Safety for components of the lifting system.
- Failure of lifting equipment is postulated including gross failure of the lifting equipment structure, failure of the mechanism itself, (e.g. cable or gearing or brake), overloads caused by dynamic magnification of normally safe working loads or as a consequence of fatigue crack propagation, corrosion or component wear etc.
- The lift analysis should consider the effect of the load swinging and snagging (or being otherwise restrained). Swinging may be intentional (to move a load horizontally as well as vertically) or unintentional due to accidental impact or factors such as high wind velocity. Either way a swung load has a wider impact footprint and can move unpredictably. Snagging can cause the load to drop or swing unpredictably and can damage: the load, the item causing the snag,

slings, the lifting equipment structure, the lifting equipment drive chain (e.g. motors, gearing and brakes) and other fixed and moveable equipment (e.g. from collisions). Hazards created by load hang-ups and hook-ups are considered.

- The integrity of overload protection systems and both mechanical and civil support structures should be assessed, as should any failure modes and effects of equipment introduced to protect against other faults.
- The standards of design, construction, operation and maintenance of supporting and lifting equipment should be commensurate with the radiological consequences of their failure. This is notwithstanding regulatory requirements, such as those arising from Lifting Operations and Lifting Equipment Regulations 1998.
- Where necessary, appropriate engineered and managerial mitigating systems should be identified (depending on the estimated frequency of the dropped load event) or additional protection or operating restrictions should be provided.
- The above considerations are brought together to form an ALARP justification.

5.164 Given the multiple fault sequences typically associated with lifting operations it is expected that a high degree of redundancy and diversity will be employed in the protective systems where significant consequences are identified. The number, type and level of substantiation of the safety measures should be aligned with the categorisation of safety functions and classification of SSCs, according to their role in delivering defence-in-depth.

Toxic and/or corrosive solid, liquid or gaseous releases

Hazard sources

5.165 Nuclear facilities generally make use of substantial quantities of hazardous materials and gases. Such materials consist of bulk and bottled storage of chemotoxic substances, asphyxiants, corrosive materials, oxidising agents, flammable solvents e.g. nitrogen, hydrogen, propane, chlorine, carbon dioxide, hydrazine, ammonia etc. Inspectors should be aware of those nuclear licensed sites which fall under COMAH by virtue of their hazardous substances inventories, and seek advice from Conventional Safety Specialists

5.166 The safety case should identify the range of hazardous materials that, if released, could disable plant items important to safety or affect personnel carrying out actions important to safety. The hazard identification process should be rigorous and well documented and provide details on the quantity, nature and storage arrangements associated with toxic and corrosive materials and gases stored and generated on-site. The hazard identification should also take account of storage location and the routes followed by distribution pipework, delivery vehicles, as the location of potential releases will be important to understanding the potential consequence.

5.167 The safety case should consider the consequential effects arising from both internal and external hazards. Examples of potential secondary internal hazards generated as a consequence of either external or internal hazards include:

- Release of toxic and corrosive materials and gases as a result of failures in engineered safety systems or as a result of other internal hazards such as fire, explosion and dropped loads.
- Seismically-induced release of toxic or corrosive materials and gases from failures of pipework or storage tanks.
- Pipe-whip impacts and jetting effects from pipework failure.
- Missile generation from failures in pressurised or rotating plant.

- Releases of chemicals which could accidentally mix and form secondary products which could affect both safety of plant and personnel.
  N.B. the effect of these secondary internal hazards are discussed in more detail in this guide under the specific internal hazard

Hazard analysis

5.168 The hazard analysis should consider the impact of release of hazardous materials and gases on the ability of the operator to take necessary action to control the incident or to safely shutdown a plant and maintain it in a safe shutdown state.

5.169 A release of hazardous materials may cause toxic or asphyxiation effects on personnel or cause a sudden, uncontrolled evacuation, so the location of permanently occupied areas such as control rooms and offices in relation to the storage of hazardous materials should be selected carefully.

5.170 The potential for hazardous gas to be drawn into the ventilation systems and transported to control rooms or other locations where operators may be expected to carry out actions to safely control the plant should also be considered.

5.171 The hazard analysis should consider the impact of release of hazardous materials and gases on the performance of plant items important to safety. For example a release of hazardous material may cause shorting on electrical contacts which could disable equipment controlling safety related plant, or cause starvation of air breathing equipment such as safety related diesel generators. Consideration should also be given to the toxic and corrosive effect of releases which could weaken plant materials and threaten the performance of safety related plant.

5.172 There is potential for hazardous materials and gases to spread from site of release to other areas of plant. The hazard analysis should therefore consider the dispersal of hazardous material and gases from site of release to other areas of plant. The spread of release depends on a number of factors e.g. location of breach, density, release phase, temperature and buoyancy effects, the effects of ground contours, buildings etc. The hazard analysis should consider the potential to spread via drains, ducts, ventilation systems. The prediction of the impact of hazardous material and gas release is complex and safety cases may rely on modelling techniques. Caution should also be exercised when deciding whether the model is representative and sufficiently robust with adequate conservatisms to take account of all the uncertainties associated with the model assumptions. The model used should be adequately validated and verified.

Safety Measures

5.173 Where the on-site use, storage or generation of hazardous materials cannot be avoided, their amounts should be minimised, controlled and located so that any accident to, or release of, the materials will not jeopardise the establishing of safe conditions on the facility (EHA.13). This includes the potential impacts on plant items important to safety or the ability of personnel to carry out actions important to safety.

5.174 In line with the SAPs, one of the basic safety requirements is to adopt a defence-in-depth approach (EKP.3). This should provide a series of levels of defence to prevent the release of hazardous substances in the first instance, or if prevention fails should ensure detection, limit the potential consequences and prevent escalation. This can be achieved by:

- adopting good engineering design, including conservative design and material choices for the storage of hazardous substances;
- installation of relief vents to reduce potential of gross failure of storage tanks;

- installation of bunds for the storage of hazardous liquids;
- installation of pipe restraints to minimise pipe-work failures;
- leak detection installed on storage tanks;
- use of regular walkdowns and inspections to identify any degradation and ageing of plant;
- considering the need for redundancy and diversity, separation and segregation (e.g. segregating walls) to mitigate against release of hazardous materials;
- good design and layout of plant and items important to safety (such as cabling and electrical control cabinets) to minimise potential damage due to release of any hazardous materials.

5.175 ONR assessors should also consider the following when undertaking their assessments:

- In line with the expectations outlined generally, the safety case should demonstrate that items important to safety (including operator actions of nuclear safety significance) are either qualified to withstand the effects of hazardous material releases or are protected against such hazards through adequate redundancy, diversity, separation or segregation. The safety cases should outline features of the design which prevent, control and mitigate releases, and these may include robust design and structural integrity of storage vessels and transfer systems, automatic isolation arrangements, as well as ventilation systems, bunds etc. to mitigate any release. The number, type and level of substantiation of the safety measures should be aligned with the categorisation of safety functions and classification of SSCs, according to their role in delivering defence-in-depth.
- The safety case should provide assurance that the asset condition of plant containing toxic and corrosive materials and gases is adequately managed to minimise the potential for ageing and degradation processes which can increase potential for release, by compromising containment integrity.
- The need to consult with other technical specialists should be considered. For example, consultation with structural integrity assessors may be necessary to ensure claims made on metal components such as pipework and storage vessels in the internal hazards aspects of the safety case are appropriate and valid. Also, the need to consult with chemistry and/or chemical engineering specialists should be considered, given chemistry can impact on the rate of production, distribution, magnitude and removal mechanisms for hazardous materials and gases. Where COMAH applies, conventional safety specialist advice should be sought.
- Generally, internal hazards and conventional safety specialists should work closely on any matters relating to toxic and/or corrosive solid, liquid or gaseous releases. This is because of the expected degree of overlap. For example, IH inspectors will have an interest if there are claims on operator performance to sustain nuclear safety under hazard conditions, or if consequential failures of nuclear-safety significant plant may be triggered by the release or operator actions. However, these releases pose conventional health and safety hazards as personnel is within the hazard ranges, regardless of whether there are nuclear safety claims placed upon them or not

Vehicular Transport Impacts

5.176 Loss of control during the transport of materials and equipment in nuclear plant has the potential to trigger events with nuclear safety consequences. It is therefore necessary that safety cases give due attention to vehicular transport and that the safety implications are adequately understood, controlled and key SSCs are protected so that the risks are reduced so far as is reasonably practicable

5.177 This TAG section covers impacts from vehicles, which may occur inside or outside buildings but the impact originating the event occurs within the site boundary and is therefore within the control of the existing or prospective licensee. The potential exists for deliberate actions or malicious intent causing a traffic incident, but this is a security event and is therefore outside the scope of this TAG.

Hazard Sources

5.178 In the case of vehicular impacts, any means of transport for equipment, fuel, goods or nuclear matter are a potential hazard source and should therefore be considered in line with EHA.13. Similarly, fire fighting vehicles and generally, any vehicles used in emergency response should be considered.

5.179 The hazards from traffic incidents largely arise from potential impacts on plant or buildings containing safety significant plant, which may trigger combined consequential hazards, such as fire or release of gases or toxic materials from a traffic incident and these should also be considered as appropriate.

5.180 Many nuclear sites include rail infrastructure, especially associated with fuel flasks/casks or major waste consignments. At facilities where submarines operate there is increased potential for impacts associated with submarine and ship movements. Loss of control of railcars and impacts on plant, and submarines-ship collisions and between submarines and shore facilities are all potential hazards which should be considered.

Hazard Analysis

5.181 The layout of plant (and specifically of plant containing radioactive materials or with a safety function) is a key consideration in the identification of potential impact hazards (EHA. 13).Transport routes, vehicle characteristics (maximum speed, mass, load) are other key considerations needed to gauge the potential consequences of impact with nuclear plant.

5.182 Inspectors should expect the identification of vehicle impact scenarios on an unmitigated basis e.g. in the absence of speed restrictions and other administrative measures should not form the sole basis for excluding vehicle impact scenarios from assessment.

5.183 The analysis of unmitigated impacts of road vehicles on to nuclear plant can often be simplified by consideration of a number of bounding cases. Due to the uncertainty associated with of the level of damage which may be caused by collisions and for the purpose of screening, qualitative approaches may be appropriate. This may involve conservatively assuming that any SSCs impacted will fail to deliver their safety functions e.g. pipework impacted will be breached, buildings impacted may collapse.

5.184 Where the withstand capacity of structures is claimed in safety cases, internal hazards inspectors should seek assurances from structural integrity and civil engineering specialists that the design of the structures is sufficiently robust to accommodate loads from vehicle impact on the weakest members, and that they are adequately substantiated.

5.185 Fault studies and PSA also represent key interfacing disciplines in the consideration of fault sequences and consequences, taking cognisance of SAPs FA.3, FA.6, FA.7 and FA.8. Sensitivity analysis should be used to identify plant and system vulnerabilities. This should consider the most onerous operating mode. For example, vehicle impact risk may be greater during maintenance shutdown activities with the use of transporters or fork lift trucks.

5.186 Licensees and requesting parties may base their safety case on low frequencies of damaging traffic incidents within nuclear installations. These claims are often justified by claims on the low site speed limits, and driver behaviour although there have been incidents involving vehicles exceeding site speed limits (e.g. emergency services/site fire team under blue lights).

5.187 Safety cases should demonstrate that vehicular impacts either have no potential to disable safety related plant and equipment or that there is an adequate combination of engineered safeguards and management controls to reduce the risk to ALARP.

Safety Measures

5.188 In forming a judgement as to the adequacy of safety cases for vehicular transport, inspectors should consider the degree to which licensees and requesting parties have considered the following:

- The speed and travel paths of vehicles, which should be controlled and monitored according to procedures commensurate with the consequences of loss of control and impact.
- The consideration given to two or more vehicles moving in the same area at the same time.
- The overall provision of engineered measures, including any automatic systems to control vehicle speeds (to values below the design capacity of structures or SSCs should they be impacted) and zonal restrictions (which prevent operation outside a specified location).
- The provision of appropriately designed energy absorbing barriers suitable for the vehicle types in operation. These should particularly feature as far as is reasonably practicable in areas where there is potential for collision or impact with plant performing a safety function or containing radioactive substances.
- The design specification should cover vehicles operating outside of their normal procedures i.e. encompass the worst case unmitigated consequences.
- Inspectors should be aware that many barrier systems for road traffic perform better for glancing impacts, than for direct impacts.
- Some barriers to road vehicles may be argued to give absolute protection against low speed collisions, but this may assume compliant behaviours or normal traffic. Nevertheless, even these may not be guaranteed for moving vehicles of high mass or vehicles of different types.

5.189 In addition, the following represent typical engineered and administrative controls which are available to licensees and designers to provide additional protection to SSCs with nuclear safety significance:

- Re-routing loads to avoid travelling close to sensitive plant and buildings is a simply and obviously effective measure which may be practicable in less congested sites.
- Appropriate protection at reversing bays, especially for delivery of hazardous material. This may also include posts or bollards to protect walls at entry points of buildings e.g. entry points for flask/ radioactive waste transporters.
- To prevent consequential fire damage following vehicle impacts on wall/ barriers, drains may be covered within vehicle bays, and culverts may run any spilled fuel away from key walls and structures.
- If space allows, any traffic barriers should be situated at a distance away from walls and structures for defence-in-depth, and allow additional space to stop vehicles and loads.
- Use of banks personnel for heavy crane loads, and potentially to guard entry points to buildings from impact by heavy vehicles e.g. those transporting nuclear materials.

5.190 The number, type and level of substantiation of the above safety measures should be aligned with the categorisation of safety functions and classification of SSCs, according to their role in delivering defence-in-depth.

Electromagnetic Interference

5.191 Electromagnetic interference (EMI), also called radio-frequency interference (RFI) when in the radio frequency spectrum, is a disturbance generated by an external source that has the potential to affect electrical or electronic devices. It is caused either by electromagnetic induction or by electromagnetic radiation. The disturbance may interrupt, obstruct degrade or limit the performance of electrical and C&I circuits performing nuclear safety significant functions and therefore impact nuclear safety.

5.192 EMI can also be an external hazard e.g. as a result of space weather events, and these would generally be assessed by External Hazards specialists, with the internal hazard definition (site boundary, within the control of the dutyholder) being the differentiating factor. A collaborative approach is nevertheless needed as EMI hazards may be man-made and external to the licensed site, for example, in multi-facility sites.

5.193 It is noted that EMI hazards will be principally considered by electrical, and C&I inspectors where they relate to the functionality of electronic equipment. However, the consequences of EMI can be considered as internal hazards and may impact on claims made in the safety case. It is important to note that where EMI hazards are addressed in a licensee's or requesting party's safety case, internal hazards inspectors should liaise closely with the C&I inspector to ensure that all aspects of the hazards are assessed.

5.194 International guidance for the design and construction of equipment [38, 39] addressees the prevention of the sources of EMI and the ability of equipment to withstand EMI.

Identification of EMI hazards

5.195 Significant sources of electromagnetic interference within the control of existing and prospective licensees include (but are not limited to):

- battery chargers;
- generators;
- the operation of switchgear, circuit breakers, variable speed motor drives or HVAC systems;
- electric fields caused by radio transmitters;
- maintenance or construction activities, for examples portable arc welding equipment, portable radio communications or telephony;
- ground-penetrating radar used for ground surveys.

5.196 Identification of potential EMI hazards should account for potential sources during maintenance or faults, for example electrical faults from cables with insulation degradation or from transformer insulator breakdown faults.

Prevention of EMI

5.197 Guidance is available for minimising the effects of EMI on C&I components or systems in international guidance [38]. This guidance includes a number of techniques such as:

- Suppression of electromagnetic interference at the source;
- Separation and isolation of C&I signal cables from power cables;

- Shielding of equipment and cables from external sources of magnetic and electromagnetic radiation;
- Filtering of electromagnetic noise before it can couple to sensitive electronic circuits;
- Neutralization or isolation of electronic equipment from ground potential differences;
- Effective grounding of electrical and C&I equipment, raceways, cabinets, components and cable shields.

5.198 If testing is to be carried out to demonstrate the efficacy of the protection against EMI provided by the design, the equipment under test needs to be in a state that if it were to mal-operate this does not result in a threat to nuclear safety.

5.199 Portable electronic devices (e.g. computers, devices with wireless transmitters such as mobile phones, radios, etc.) close to sensitive equipment should be controlled. This may use a number of measures, such as exclusion zones or other administrative controls. Exclusion zones may be reinforced by physical controls (for example EMI detection devices), by administrative controls (such as access arrangements, warning notices, work control systems) and by good safety culture (training, awareness, self-checking, questioning attitude). The choice of approaches to enforce exclusion zones will depend upon the required level of reliability.

Mitigation of EMI hazards

5.200 The consequences of individual component failures on the overall success or failure of the system or on the overall safety function and the impact on claims in the safety case should be understood.

5.201 As with other internal hazards good design principles such as redundancy and diversity, separation and segregation should be adopted as they can have a significant effect on reducing the vulnerability to and effect of the EMI hazard. In many cases, care in design over choice of the location of systems or subsystems can have a major effect on the potential overall consequences to system functionality and hence to the nuclear safety risks. EMI hazards, however, are not necessarily localised, as EMI can travel along poorly shielded cables from one location to another.

5.202 Where a potential EMI hazard exists that could have significant implications to nuclear safety, mitigation measures considered by the licensee should include:

- Relocation of equipment to eliminate the hazards;
- Rerouting of cables;
- Installation of shielding.

5.203 Further guidance on EMI is given in the ONR Controls & Instrumentation EMI TAG [40].

Combination of Hazards

5.204 Single Internal and External Hazards, whilst usually studied individually, rarely occur in isolation. A single event, e.g. high energy pipe break results in a number of hazards e.g. pipe whip, jet impact, flooding, steam release which occur simultaneously or in quick succession. Similarly, an internal flooding event may trigger a fire or explosion, or a seismic event may be followed by fires or almost any other internal hazard. These are generally referred to as hazard combinations.

5.205 In terms of types of hazard combinations, the following classification is generally considered appropriate:

- Independent Hazards; when more than one internal and/or external hazard applies simultaneously. This can be the case, for example, of nominally frequent events such as internal fire and flooding when there is no causation link between them.
- Consequential Hazards; an internal or external hazard directly poses one or more additional hazards to plant and structures (e.g. fire activating a water-based fire supressing system leading to water spray and flooding effects).
- Correlated Hazards; a common cause results in multiple hazard(s) which occur simultaneously. An example of this would be pressure part failure giving rise to pipe whip impact and flooding.

Identification of hazard combinations

5.206 Whilst the focus of safety cases is usually the identification of individual hazards and the selection of measures to address each hazard challenge, the added benefits from adopting inherently safe design options cannot be emphasized highly enough from a combined hazards perspective.

5.207 Consideration of key combined hazard challenges from early in the design process ensures that there is scope for change as layouts have not been fully fixed and design options foreclosed. However, formal identification of hazard combinations often takes place later in the design process, and relies heavily on systematic and comprehensive identification of individual hazards.

5.208 Given the high number of internal and external hazards, and possible permutations, it is necessary that safety cases apply screening criteria and follow pragmatic approaches.

5.209 National and company standards [41, 42] and past project experience [43] provide some guidance on key internal hazard combinations and screening options, but there is generally limited international consensus or dedicated guidance that can be applied when carrying out the process.

5.210 ONR recognizes the need for systematic identification, but also the need for screening so that the list of scenarios developed represents a credible and reasonable set of plant challenges. The screening should aim to capture consequences that differ or are more challenging than those of individual hazards. Some key considerations for inspectors are as follows:

- A good starting point to the identification of hazard combinations which often acts as an indicator of the adequacy of the case is a hazard combination matrix, developed from a consolidated list of all internal and external hazards. The list can be followed by a “what-if” exercise to challenge whether hazards can occur in combination in the context of plant conditions following the initial

hazard or within the mission time for the management of the plant in the event. This requires judicious selection of the plant within the scope of the screening study (for which layout plans and information on the location of key SSCs and protection features often proves invaluable).

- It is important that safety cases record any assumptions made to dismiss hazard combinations or their effects (e.g. limiting hazard effects because of an assumed barrier withstand capability) and that these are checked periodically as the design evolves (e.g. following changes to layout, location of SSCs, or key equipment qualification decisions).
- It is also important to ensure that the above approach does not entirely focus on cause-effect relationships between the hazards, but also includes combinations of independent hazards which may provide additional challenges to the plant design.
- It is generally expected that a hazard combination sequence will be developed, particularly for concurrent and consequential hazards. This is effectively a form of early screening.
- Whilst some concurrent and consequential hazards may arise directly and unequivocally following the initiating event, dutyholders will essentially be making decisions as to whether the damage to plant will be sufficiently severe to trigger further hazards. Needless to say, the credibility of such decisions and the hazard sequences will be heavily influenced by the level of design development and the availability of consequence analysis at the time the decisions are made.
- Conservative decision making carried out too early in the design process can lead to the identification of numerous hazards and complex sequences which will pose unnecessarily onerous constraints to the location and specification of key SSCs. Conversely, discounting hazard combinations at an early stage of design, or not performing a preliminary analysis, can lead to unexpected challenges later in the design process when the impact of changes means that there is less flexibility for layout changes.
- The identification of combined hazard identification is not the exclusive ground of hazard analysis specialists. Inspectors should seek evidence of good cross-discipline interactions between fault studies, internal and external hazard specialists. These are generally required to consolidate insights from any preliminary hazard characterisation work and transient analyses available. Additionally, input from engineering disciplines (e.g. structural integrity, mechanical and civil engineering) should be expected to ensure that the assumed responses of SSCs are realistic and consistent with relevant operational experience. This also applies to judgements made on the credibility of specific failure consequences made in the sequence. It is expected that internal hazards inspectors will seek similar cross-discipline interactions to make their judgements.

5.211 With the above considerations in mind, it is still possible that long lists of hazard combinations and complex hazard sequences will be derived and presented in safety cases. Dutyholders should therefore develop and apply suitable approaches to reduce the lists to a meaningful set of credible and bounding challenges.

Screening of combined hazards

5.212 A resilient design should be able to demonstrate not only that the plant remains safe in the selected hazard sequences, but also that all other sequences are bounded appropriately by the set of combined hazard challenges. The screening of hazard combinations can be deterministic or probabilistic. Key considerations in are discussed below.

Deterministic screening

5.213 From a deterministic point of view, hazard sequences can be grouped based on the challenges to specific protection features e.g. each individual multi-hazard barrier. The physical withstand of the protection feature can then be chosen subject to further assessment against the highest combined challenge.

5.214 When following this bottom-up screening approach, it is essential to check that the combined load remains representative and bounding through the design process. This is particularly needed following subsequent input of geometry / SSC layout considerations and consequence assessment of individual hazards.

5.215 Whilst it is acceptable to remove any challenges that are no longer relevant, the set of combined hazard scenarios should be revisited to reconsider whether other sequences (previously considered bounded) have become the bounding/ representative case.

5.216 It may also be acceptable to group hazard sequences based on the combined challenge to each safety function. This top-down approach may prove useful in identifying challenging locations e.g. where the primary and secondary protection systems are in close proximity or, more critically, within the same compartment. A resilient design should preferably demonstrate that there are no such locations, or that there is suitable protection to demonstrate continued availability (under hazard conditions. This requires substantiation of the segregation features (multi-hazard barriers) or qualification of SSCs under the conditions of multiple hazards.

5.217 The two deterministic screening approaches above are not mutually exclusive and should be used to complement each other.

Frequency screening

5.218 Hazard combinations may be screened out because the frequency of occurrence is considered to be extremely low. This has generally been postulated when the frequency of a fault sequence is below 1 in 10 million years (10^{-7} per annum) (ONR SAPs) and is likely to be the case for the majority of independent external hazards.

5.219 Care should be taken in the use of frequency to screen out hazard combinations completely from assessment, as it could result in a complete lack of design provision. Whilst it may be acceptable to consider that two independent, low frequency hazards in the Design Basis have a very low probability of occurrence during each other's plant mission time, the combined consequential effects should be checked for cliff-edge effects not otherwise captured in the safety case.

Challenges in the screening of combined hazard sequences

5.220 In the process of screening of hazard combinations, it is essential to bear in mind that the duration of the hazards should also be taken into account when considering the possibility of other hazards during this period. Also, the duration of consequential effects on plant is equally, if not more, important. This duration should include consideration of the time it would take to introduce alternative equipment to take over the long-term provision of safety functions in accordance with the requirements of Paragraph 641 of ONR SAP FA.8.

5.221 In addition, paragraph 5.49 of IAEA document SSG-3 [44] states that "The success criteria should specify the mission times for the safety systems, that is, the time that the safety systems will need to operate so that the reactor reaches a safe, stable shutdown state and that will allow for long term measures to be put in place to maintain this state." Mission time should therefore be based on the consequences of the event and not just the duration of the hazards themselves.

5.222 Combinations of hazards can potentially affect plant in different ways. Some combinations can affect plant by affecting the diversity of systems. Other

combinations of hazards can affect a single system via the production of an additional load. The requirements for segregation, redundancy, separation and diversity should be considered.

5.223 Generally, robust segregation in safety divisions which applies consistently to the full set of internal hazards should prevent combined hazards from challenging the FSFs. It is, however, often the case that development of segregation requirements and subsequent barrier design decisions are made based on the outcome of individual hazard assessments. Care needs to be taken particularly when any of the following applies:

- There is reliance on qualitative arguments to substantiate the barrier against individual hazard loads;
- Hazard compartments or SSCs are credited to survive an event prior to consequence modelling and target response analysis being undertaken;
- Partial failure of segregation barriers is conceded and a residual withstand capacity is credited against secondary hazard propagations.
- Backup/redundant safety systems are housed in the same or adjacent hazard compartments to those where the hazard materialised.

5.224 Recent ONR experience in the assessment of Generic Design Assessment (GDA) safety cases has highlighted the effect that screening approaches may have on the bounding sets selected. Some key lessons learned are as follows:

- There is a need to revisit the set of combined hazard challenges following consequence analysis and consideration of plant geometry as detailed design becomes available. This is particularly important when the designer identifies that a previous bounding case has been designed out (so may no longer be regarded as credible), in which case care should be taken to also re sentence other scenarios which had grouped into this bounding case. In some cases scenarios not previously studied in detail may become dominant contributors to the risk.
- Significant levels of scrutiny and analysis should be expected in key areas e.g. where Class 1 and/or back up Class 2 systems are proposed to coexist without physical segregation (for example separated by fire shields rather than fire barriers). Also, the barriers between these areas (and others claimed to contain SSCs that provide the suitable diverse means) should be substantiated against the combined loads.
- Evidence should be provided to support the assumed availability of engineered measures and the effectiveness and practicability of human intervention measures expected to be performed under the conditions of the hazards. This may involve evidence on the withstand capability of equipment and preliminary human factors studies undertaken. Internal hazards inspectors should therefore liaise with the relevant engineering disciplines and human factors inspectors.
- For combinations of hazards, the individual hazard duration and severity should be underpinned by evidence. The functional performance characteristics and qualification of SSCs, where defined for an individual hazard should be extended to address the combined hazard scenarios;
- Where fail safe responses of SSCs are credited to prevent further hazards, this should be demonstrated as achievable under the hazard conditions (and not entirely based on plant responses in normal operation). An example could be design studies to confirm that a valve will close under fire conditions following loss of signal, if this is the behaviour required.
- Some of the evidence required above arises from individual and combined hazard characterisation / consequence modelling. A successful screening exercise requires inputs such as the location, design characteristics, operating envelope and response to individual hazard conditions of SSCs and

neighbouring plant. This may not be available at the stage of design where a safety case is required for regulatory scrutiny e.g. GDA.

Characterisation of hazard combinations

5.225 In the characterisation of hazard combinations, safety cases (and inspectors) should consider the following key points:

- The sequencing, duration and timing of the individual loads on specific SSCs or areas of plant can be critical in determining the joint effects, but may not be the prime focus of (or an output) from the individual hazard assessments.
- There is little available guidance, codes and standards to define the load combinations. Any assumptions on timing and duration should be based on robust consequence assessment, the layout of the plant in question, and the qualification and proven performance of the SSCs under the conditions of the hazard. For example, in pressure part failure consequences, the time to isolation should be based on valve performance characteristics and the time to peak compartment pressure, if used, should be based on analytical pressure relief calculations relevant to the compartments in question.
- The utilization of SSCs (e.g. reinforced concrete barriers) as a result of each individual hazard load and the residual withstand capacity of the SSCs should be determined analytically. This should, in turn, inform the analysis of the response of SSCs to the combined hazard sequence. It is expected that a pass/ fail criteria will be set. It is of course most appropriate to ensure that barrier withstand is proven for all potential barrier failure modes following consideration of all credible combined loads in the sequence. Engineering design codes and standards specify load combinations, load factors and acceptance criteria for use in the design of SSCs.
- Although it is often acceptable to conclude that specific hazards effects (e.g. jet impact) are bounded by other hazards (pipe whip) in the assessment of individual hazards, this does not mean that the hazards effects can be assumed not to combine when they occur in a combined hazard sequence, and indeed they most certainly do in the above example.
- As the hazard sequence is considered, it may be the case that partial or complete failure of SSCs or barriers (e.g. perforation or scabbing) are predicted when utilization is determined analytically. In these cases, ONR's expectation is that reasonably practicable measures to prevent the failures are implemented in line with UK regulatory requirements.
- Should partial failures e.g. scabbing of reinforced concrete barriers be accepted as the end point of the combined hazards sequence, it should be clear that all reasonably practicable measures have been implemented to avoid undesirable secondary effects, and that delivery of FSFs is still achieved.
- When discussing challenges in the screening of hazard combinations, it is essential that any assumed availability of claimed measures is supported by evidence.

5.226 As the hazard sequence is studied and it becomes apparent that the consequences of the combined loads are more severe than those of the individual hazards, the categorization and classification of SSCs (e.g. any means of isolation, barriers etc.) should be revisited to ensure that they represent the significance of the combined hazard effects. This is of course a multidisciplinary team effort, where input from structural integrity, mechanical and civil engineers (to mention but a few), is critical to ensure that the SSC design is appropriate to the level of challenge posed by the combined loads.

5.227 An integrated approach should be applied at an early stage of the design of SSCs to ensure that the potentially conflicting requirements of nuclear safety, security,

safeguards, fire and conventional safety are taken into account while ensuring that the measures adopted do not compromise one another. This approach may involve several iterations in order to develop the design and represents relevant good practice reflecting guidance and requirements in internationally recognized documents.

6. REFERENCES

1. ONR. Safety Assessment Principles for Nuclear Facilities. 2014 Edition Revision 0. November 2014. http://www.onr.org.uk/saps/saps2014.pdf (electronic reference last accessed 13 September 2018).

2. HSE. Dangerous Substances and Explosive Atmospheres, Approved Code of Practice and Guidance L138 (2nd edition), published 201 http://www.hse.gov.uk/pUbns/priced/l138.pdf (electronic reference last accessed 13 September 2018).

3. HSE. Safety of Pressure Systems, Pressure Systems Safety Regulations 2000 Approved Code of Practice L122 (2nd edition), published 2014 http://www.hse.gov.uk/pUbns/priced/l122.pdf (electronic reference last accessed 13 September 2018).

4. HSE. Safe Use of Lifting Equipment, Lifting Operations and Lifting Equipment Regulations 1998, Approved Code of Practice and Guidance, L113 (2nd edition), published 2014. Electronic reference available at http://www.hse.gov.uk/pubns/priced/l113.pdf (last accessed 13 September 2018).

5. HSE. Legal status of HSE guidance and ACOPs. Electronic reference available at http://www.hse.gov.uk/legislation/legal-status.htm (last accessed 28 August 2019).

6. Western European Nuclear Regulators' Association (WENRA), WENRA Safety Reference Levels for Existing Reactors, Update in Relation to Lessons Learned from TEPCO Fukushima Dai-Ichi Accident, 24th September 2014. Electronic reference available at http://www.wenra.org/media/filer_public/2014/09/19/wenra_safety_reference_level_for_existing_reactors_september_2014.pdf (last accessed 13 September 2018).

7. Western European Nuclear Regulators' Association (WENRA), Radioactive Waste Treatment and Conditioning Safety Reference Levels. 2018. Electronic reference available at http://www.wenra.org/media/filer_public/2018/04/17/report_radioactive_waste_treatment_and_conditioning_safety_reference_levels.pdf (last accessed 29 August 2019).

8. Western European Nuclear Regulators' Association (WENRA), Radioactive Waste Disposal Facilities Safety Reference Levels 2014. Electronic reference available at http://www.wenra.org/media/filer_public/2015/03/18/srl_disposal_final_version_2014_12_22.pdf (last accessed 29 August 2019).

9. International Atomic Energy Agency (IAEA), Protection against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants. Safety Guide, IAEA Safety Standards Series No. NS-G-1.11. 2004. Electronic reference available at https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1191_web.pdf (last accessed 2 April 2018).

10. International Atomic Energy Agency (IAEA), Protection against Internal Fires and Explosions in the Design of Nuclear Power Plants. Safety Guide, IAEA Safety Standards Series No. NS-G-1.7. 2004. Electronic reference available at https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1186_web.pdf (last accessed 13 September 2018)

11. International Atomic Energy Agency (IAEA), Fundamental Safety Principles, IAEA Safety Standards Series No. SF-1. 2006. Electronic reference available at https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1273_web.pdf (last accessed 28 August 2019).

12. International Atomic Energy Agency (IAEA), Fire Safety in the Operation of Nuclear Power Plants. International Atomic Energy Agency (IAEA), Safety Guide, NS-G-2.1. 2000. Electronic Reference available at https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1091_web.pdf (last accessed 2 April 2018).

13. International Atomic Energy Agency (IAEA), Safety of Nuclear Fuel Cycle Facilities, No SSR-4. 2017. Electronic Reference available at https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1791_web.pdf (last accessed 29 August 2019).

14. International Atomic Energy Agency (IAEA), Safety of Nuclear Power Plants: Design. Specific Safety Requirements, No SSR-2/1 (Rev. 1). 2016. Electronic Reference available at https://www-pub.iaea.org/MTCD/publications/PDF/Pub1715web-46541668.pdf (last accessed 2 April 2018).

15. International Atomic Energy Agency (IAEA), Safety of Nuclear Power Plants: Commissioning and Operation, Specific Safety Requirements, No SSR-2/2 (Rev. 1). 2016. Electronic Reference available at https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1716web-18398071.pdf (last accessed 2 April 2018).

16. International Atomic Energy Agency (IAEA), Deterministic Safety Analysis for Nuclear Power Plants, No SSG-2 (Rev.1). Electronic Reference available at https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1428_web.pdf (last accessed 30 August 2019).

17. International Atomic Energy Agency (IAEA), Storage of Spent Nuclear Fuel, Specific Safety Guide, No SSG-15. 2012. Electronic Reference available at https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1503_web.pdf (last accessed 27 August 2019).

18. Office for Nuclear Regulation (ONR), Technical assessment guides, NS-TAST-GD-042 Revision 4 Validation of Computer Codes and Calculation Methods. Electronic reference available at http://www.onr.org.uk/operational/tech_asst_guides/index.htm (last accessed 17 October 2019).

19. British Standard Institute (BSI), BS EN 1363-1:2012, Fire resistance tests. General requirements, 31 August 2012. Electronic reference available online at https://shop.bsigroup.com/ProductDetail/?pid=000000000030251439 (last accessed 1 March 2018).

20. Office for Nuclear Regulation (ONR), Technical assessment guides, NS-TAST-GD-022 (Rev 5) April 2017 Ventilation. Electronic reference available at http://www.onr.org.uk/operational/tech_asst_guides/index.htm (last accessed 27 August 2019).

21. British Standard Institute (BSI), BS EN 1992-1-1:2004+A1:2014 Eurocode 2: Design of concrete structures. General rules and rules for buildings, 23 December 2004. Electronic Reference available at https://shop.bsigroup.com/ProductDetail/?pid=000000000030286962 (last accessed 1 March 2018).

22. British Standard Institute (BSI), BS EN 1363-2:1999, Fire resistance tests. Alternative and additional procedures, 15 November 1999. Electronic reference available online at https://shop.bsigroup.com/ProductDetail?pid=000000000019969922 (last accessed 14 September 2018).

23. American Concrete Institute Standard: ACI 349 – Code requirements for nuclear safety-related concrete structures (ACI 349-13) and Commentary, 13th Edition, January 1, 2013.

24. IEEE, IEEE Standard 1584-2002 - IEEE Guide for Performing Arc Flash Hazard Calculations. Electronic Reference available at https://standards.ieee.org/findstds/standard/1584-2002.html (last accessed 1 March 2018).

25. R. Bettis, "Oil mist area classification-final report of a Joint Industry Project (JIP)," MH/15/75, 2015.

26. U.S. Army Corps of Engineers, United Facilities Criteria UFC 3-340-02 Structures to Resist the Effects of Accidental Explosions, December 2008, Change 2, 1 September 2014. Electronic Reference available at https://www.wbdg.org/FFC/DOD/UFC/ufc_3_340_02_2008_c2.pdf (last accessed 1 March 2018).

27. British Standard Institute (BSI), BS EN 50272-1:2010, Safety requirements for secondary batteries and battery installations. General safety information, 28 February 2011. Electronic Reference available at https://shop.bsigroup.com/ProductDetail/?pid=000000000030141654 (last accessed 1 March 2018).

28. British Standard Institute (BSI), BS EN 60079-10-1:2015, Explosive atmospheres. Classification of areas. Explosive gas atmospheres, 31 March 2016. Electronic Reference available at https://shop.bsigroup.com/ProductDetail/?pid=000000000030353978 (last accessed 1 March 2018).

29. British Standard Institute (BSI), BS EN 62271-1:2017, High-voltage switchgear and controlgear. Common specifications for alternating current switchgear and controlgear, 14 November 2017. Electronic Reference available at https://shop.bsigroup.com/ProductDetail?pid=000000000030265354 (last accessed 14 September 2018)

30. Office for Nuclear Regulation (ONR), Technical assessment guides, NS-TAST-GD-013 (Rev 6) External Hazards. Electronic reference available at http://www.onr.org.uk/operational/tech_asst_guides/index.htm (last accessed 2 April 2018).

31. International Electrotechnical Commission (IEC), IEC 60529, Degrees of protection provided by enclosures (IP code), 2.2 Edition, August 2013. Electronic Reference available at https://global.ihs.com/doc_detail.cfm?rid=Z06&mid=IEC&document_name=IEC%2060529&item_s_key=00035807&utm_source=bing&utm_medium=cpc&utm_campaign=IEC&utm_content=IEC_60529&utm_term=IEC%2060529#product-details-list (last accessed 2 April 2018).

32. Magnox Electric Ltd & British Energy Generation Ltd., "R3 Impact Assessment Procedure," 2008.

33. American Nuclear Society. ANSI/ANS-58.2-1988, Design Basis for Protection of Light Water Nuclear Power Plants Against the Effects of Postulated Pipe Rupture. 1988.

34. US NRC. NUREG 0800 Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition, 2016.

35. US NRC. Regulatory Guide RG-1.115. Protection against turbine missiles, revision 2. January 2012. Electronic Reference available at https://www.nrc.gov/docs/ML1016/ML101650675.pdf (last accessed 2 April 2018).

36. Office for Nuclear Regulation (ONR), Technical assessment guides, NS-TAST-GD-056, Rev 3 - Nuclear Lifting Operations. Electronic reference available at http://www.onr.org.uk/operational/tech_asst_guides/index.htm (last accessed 2 April 2018).

37. Safe use of work equipment, Provision and Use of Work Equipment Regulations 1998, Approved Code of Practice and guidance. L22 (Fourth edition), Published 2014. Electronic reference available at: http://www.hse.gov.uk/pUbns/priced/l22.pdf (last accessed 2 April 2018).

38. International Atomic Energy Agency (IAEA), Design of Instrumentation and Control Systems for Nuclear Power Plants, Specific Safety Guide No. SSG-39, IAEA, Vienna (2016). Electronic reference available at https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1694_web.pdf (last accessed 2 April 2018).

39. International Atomic Energy Agency (IAEA), Design of Electrical Power Systems for Nuclear Power Plants, Specific Safety Guide No. SSG-34, IAEA, Vienna (2016). Electronic Reference available at https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1673web-53477409.pdf (last accessed 2 April 2018).

40. Office for Nuclear Regulation (ONR), Technical assessment guides, NS-TAST-GD-015 (Rev 2) April 2018 Electromagnetic compatibility. Electronic reference available at http://www.onr.org.uk/operational/tech_asst_guides/index.htm (last accessed 2 April 2018).

41. Nuclear Safety Standards Commission (KTA), KTA standards 2101.1, 2103, 2201.1 and 2206.

42. Swedish Radiation Safety Authority (Strålsäkerhetsmyndigheten - SKI) 02:27 Guidance for External Events Analysis (2003).

43. ASAMPSA_E, List of external hazards to be considered in ASAMPSA_E, Technical Report ASAMPSA_E /WP21/D21.2/2017-41, University of Vienna, 2016.

44. International Atomic Energy Agency (IAEA), Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-3. Electronic Reference available at https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1430_web.pdf (last accessed 2 April 2018).

7. GLOSSARY AND ABBREVIATIONS

ACI	American Concrete Institute
ACOPs	Approved Codes of Practice
ALARP	As Low As Reasonably Practicable
ANSI	American National Standards Institute
BS	British Standard
C&I	Control and Instrumentation
CFD	Computational Fluid Dynamics
DSEAR	Dangerous Substances and Explosive Atmospheres Regulations
EMI	Electromagnetic Interference
EIM&T	Examination, Maintenance, Inspection and Testing
GDA	Generic Design Assessment
HEAF	High Energy Arching Faults
HSE	Health and Safety Executive
HVAC	Heating, Ventilation and Air Conditioning
IAEA	International Atomic Energy Agency
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
LEL	Lower Explosive Limit
LOLER	Lifting Operations and Lifting Equipment Regulations
LPG	Liquefied Petroleum Gas
ONR	Office for Nuclear Regulation
PSA	Probabilistic Safety Analysis
PUWER	Provision and Use of Work Equipment Regulations
QA	Quality Assurance
RC	Reinforced Concrete
RFI	Radio-Frequency Interference
RGP	Relevant Good Practice
RLs	Reference Levels
SAPs	Safety Assessment Principles
SSC	Structures, Systems and Components
TAG	Technical Assessment Guide
UEL	Upper Explosive Limit
US NRC	United States Nuclear Regulatory Commission
VCE	Vapour Cloud Explosions
WENRA	Western European Nuclear Regulators Association