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 4		
Date Issued:	September 2016	**Review Date:**	September 2019
Approved by:	Robert Moscrop	Professional Lead	
Record Reference:	TRIM Folder 1.1.3.776. (2016/381958)		
Revision commentary:	Routine fit for purpose update. No significant changes from Rev 3. To bring into compatibility with 2014 SAP, and revised references. A more extensive update is in preparation. In the meantime the current version is fit for purpose.		

TABLE OF CONTENTS

Published 09/16

1. INTRODUCTION

1.1 ONR has established its Safety Assessment Principles (SAPs) 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's inspectors in their technical assessment work in support of 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) explains the approach adopted by ONR in its assessment of licensees' safety submissions that relate to internal hazards that could have a detrimental effect on nuclear safety and are described in Office for Nuclear Regulation (ONR) Safety Assessment Principles (SAPs) [1] EHA 1 to EHA 19 (paragraphs 228 to 274).

2.2 The SAPs require that internal hazards on nuclear facilities be identified and their effects considered in safety assessments. Internal hazards are those hazards to plant, structures and personnel which originate within the site boundary but are external to the process in the case of nuclear chemical plant or primary circuit in the case of power reactors. That is, the licensee has control over the initiating event in some form. Internal hazards include internal flooding, fire, toxic gas release, collapses, dropped loads, impacts from vehicular transport and explosion/missiles. Detailed knowledge of the plant and site layout is required for an internal hazards assessment. Hazard identification involves a facility and site review together with event tree analysis. Multi-facility sites would require appropriate interface arrangements to deal with the potential knock-on/domino effects of internal hazards.

2.3 The SAPs require that the risk from hazards be minimised by attention to plant layout, by adopting 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.

2.4 The safety assessment should demonstrate that threats from internal hazards are either removed or tolerated and minimised. This may be done by showing that items important to safety (i.e. safety systems and safety related items) are designed to meet appropriate performance criteria, 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).

2.5 The hazards from all facilities and activities that the operator might reasonably need to undertake on the site need to be considered, including those associated with inspection, maintenance and testing.

2.6 The objective of the Western European Nuclear Regulators Association (WENRA) [2] is to develop a common approach to nuclear safety in Europe by comparing national approaches to the application of IAEA safety standards. The 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.

2.7 The WENRA reference levels were re-issues in 2014. This TAG will be updated to reflect these changes in due course and in the meantime, inspectors need to check that they are using the correct versions of those publications during their assessments.

2.8 International Atomic Energy Agency (IAEA) guidance relevant to internal hazards can be found within:

- NS-G-1.7, “Protection against Internal Fires and Explosions in the Design of Nuclear Power Plants” [3],
- NS-G-2.1, “Fire Safety in the Operation of Nuclear Power Plants” [4]
- NS-G-1.11, “Protection against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants” [5]
- SSR-2/1 Safety of Nuclear Power Plants: Design [6]
- SSR-2/2 Safety of Nuclear Power Plants: Commissioning and Operation [7]

2.9 This guidance should also be consulted by the assessor as these documents are judged to provide relevant good practice and also provide further explanation of a number of internal hazards covered as part of this TAG. The SAPs have recently been reviewed and revised. The review included benchmarking against the IAEA safety standards and the revised SAPs are consistent with the expectations of the IAEA.

2.10 This TAG contains guidance to advise and inform ONR inspectors in the exercise of their professional regulatory judgment. Comments on this guide, and suggestions for future revisions, should be recorded within the appropriate Electronic Document Record Management folder.

3. RELATIONSHIP TO LICENCE AND OTHER RELEVANT LEGISLATION

3.1 The majority of internal hazards could have an impact on the nuclear site licence conditions however, the following are seen as being most relevant to the specific threats posed by internal hazards on nuclear facilities:

- Licence Condition 7: Incidents on the site - records should be kept of the occurrence of relevant hazards.
- 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, e.g. fire and flooding
- Licence Condition 11: Emergency arrangements – internal hazards are one of the range of possible motives for the instigation of the emergency arrangement procedures.
- Licence Condition 14: Safety documentation - this condition requires internal hazards to be considered for new plant.
- Licence Condition 15: Periodic review - this condition requires internal hazards to be considered for older plant.
- Licence Condition 20: Modification to design of plant under construction - this condition requires that a modification to the design of plant under construction is assessed in the context of the internal hazards safety case, where appropriate.
- Licence Condition 22: Modification or experiment on an existing plant - this condition requires that a modification or experiment on an existing plant is assessed in the context of the internal hazards safety case, where appropriate.
- Licence Condition 23: Operating Rules – this 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.
- Licence Condition 28: Examination, Maintenance, Inspection and Testing (EMIT) – this 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:

- Pressure Systems Safety Regulations (PSSR) 2000, SI 2000 No. 128.
- Dangerous Substances and Explosive Atmospheres Regulations (DSEAR) 2002.
- Fire Safety (Regulatory Reform) Order (E&W), 2005.
- Fire (Scotland) Act, 2005.

3.3 In addition to the above, there are numerous standards and guidance documents relating to the design, commissioning, operation and maintenance of safety systems associated with internal hazards.

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

SAPs [1]

4.1 The specific internal hazard SAPs are: EHA 1, EHA 3, EHA.4, EHA 5, EHA 6, EHA.7, EHA 10 and EHA 13 to EHA 19, which cover the wide range of internal hazards identified above.

4.2 There are a number of supporting and related SAPs. These include:

- EKP 1 – EKP 5 on Key Engineering Principles.
- ECS1 – ECS 5 on Safety Classification and Standards.
- EDR 1 – EDR 4 on Design for Reliability.
- FA1 – FA3 on Fault Analysis.
- ELO.1 – ELO.4 on Layout.
- ESS 1 - ESS 27 on Safety Systems.

4.3 A licensee's safety principles must define the deterministic and probabilistic criteria against which the licensee will consider the acceptability of safety arguments for internal hazards and whether his safety goals have been met. ONR inspectors will consider the safety arguments against the ONR SAPs and would expect the arguments to meet or exceed the advice to Inspectors in the Principles, but only ‘So Far As Is Reasonably Practicable’, subject to a demonstration of tolerable risk.

4.4 Items important to safety should be qualified to withstand the effects of relevant internal hazards or be protected against the hazards. Internal hazards may include fire, explosion, flooding, missiles, release of flammable materials, toxic or asphyxiating gases, and impacts from dropped loads or from vehicular transport. As there will be limitations on the accuracy with which the initiation and the effects of hazards can be predicted and because random failures of equipment can occur, the licensee's safety principles should recognise that diverse and segregated systems and components may be required to establish the level of reliability needed to meet their safety goals.

4.5 In order that items important to safety will have the level of reliability required to meet the safety goals, the licensee must consider the possibility of single random failures, common cause failures, simultaneous and consequential events and unavailability of SSCs due to maintenance activities. Common causes include both SSC failures and effects of internal hazards such as fire. The appropriate level of reliability of essential

safety functions may be achieved by incorporating redundancy within single trains and/or segregation and diversity between trains.

4.6 The relationship between the frequency and consequences of hazards and the reliability of items important to safety should be defined by the licensee. These should include guidelines for translating high level goals into practical engineering requirements. The provision of well-engineered passive safety measures is to be preferred but in practice, for some internal hazards, active systems and procedural controls will need to be relied upon. Ideally a "Safety Class Analysis" should be undertaken whereby the number and types of safety measures required are determined using criteria that have a dependency on the frequency and consequence of the internal hazard.

4.7 Redundancy, diversity and segregation should be incorporated as appropriate within the design of items (i.e. structures, systems and components) important to safety.

1.1. Procedures for minimising the risk and consequences from internal hazards should be documented and justified. Good safety management practices should be adopted in reviewing and monitoring application of such procedures, considering lessons learnt and implementing appropriate improvements.

4.8 Moreover it is expected that a safety case will demonstrate that safety system support features, and facilities such as access roads, water supplies, fire mains and site communications important to the safe operation of the nuclear plant should be designed and routed so that, in the event of any incident, sufficient capability to perform their emergency functions will remain.

Internal Hazards SAPS

4.9 The following are extracts from the 2014 SAPs relevant to the field of internal hazards. In order to ensure clarity in the transfer across from the SAPs the relevant paragraph numbers have been retained.

Engineering principles: external and internal hazards	Identification and characterisation	EHA.1
External and internal hazards that could affect the safety of the facility should be identified and treated as events that can give rise to possible initiating faults.		

231 Hazards should be identified in terms of their severity and frequency of occurrence and characterised as having either a discrete frequency of occurrence (discrete hazards), or a continuous frequency-severity relation (non-discrete hazards). All hazards should be treated as initiating events in the fault analysis.

232. Discrete hazards are those that are realised at a single frequency (or set of discrete frequencies) with associated hazard severity/magnitude(s). Most internal hazards such as steam release are discrete hazards.

233. Non-discrete hazards are those that can occur across a continuous range of frequencies and are defined in terms of a hazard curve (a plot of hazard severity against the frequency of this severity being exceeded). Seismic hazard is an example of a non-discrete hazard.

234. The identification process should include reasonably foreseeable combinations of independently occurring hazards, causally-related hazards and consequential events resulting from a common initiating event (see Principle FA.2). This identification should include consequential events and, as appropriate, combinations of consequential events from a common initiating event.

Engineering principles: external and internal hazards	Design basis events	EHA.3

For each internal or external hazard which cannot be excluded on the basis of either low frequency or insignificant consequence (see Principle EHA.19), a design basis event should be derived.

Engineering principles: external and internal hazards	Design basis event operating states	EHA.5
Hazard design basis faults should be assumed to occur simultaneously with the most adverse normal facility operating condition.		

243. The analysis should apply an appropriate combination of engineering, deterministic and probabilistic methods in order to:

- *understand the behaviour of the facility in response to the hazard; and*
- *confirm high confidence in the adequacy of the design basis definition and the associated fault tolerance of the facility.*

244. The analysis should include hazard analysis to:

(a) identify the potential impact of the hazard on the facility's structures, systems and components, and in particular its safety systems;

(b) determine the need for segregation, diversity and redundancy of plant and equipment and the location of barriers to limit this impact; and

(c) determine the safety functions (eg the withstand capability) to be provided by such barriers.

245. The analysis should take into account that:

(a) certain internal or external hazards may not be independent of one other and may occur simultaneously or in combinations that are reasonable to expect;

(b) the initiating hazard, or its effects may persist as the fault sequence progresses (see paragraph 631 a)).

(c) an internal or external hazard may occur simultaneously with a facility fault, or when plant is out for maintenance;

(d) there is significant potential for internal or external hazards to act as initiators of common cause failures, including loss of off-site power and other services;

e) the most severe internal and external hazards have the potential to threaten more than one level of defence in depth (see Principle EKP.3) at once;

(f) internal hazards (eg fire) can arise as a consequence of faults internal or external to the site; and

(g) the severity of the consequences of internal and external hazards will often be affected by aspects such as facility layout, interactions between structures, systems and components, and building size and shape.

Engineering principles: external and internal hazards	Analysis	EHA.6

The effects of internal and external hazards that could affect the safety of the facility should be analysed. The analysis should take into account hazard combinations, simultaneous effects, common cause failures, defence in depth and consequential effects.

Engineering principles: external and internal hazards	Electromagnetic interference	EHA.10
The facility design should include preventative and/or protective measures against the effects of electromagnetic interference.		

256. An assessment should be made to determine whether any source of electromagnetic interference either on-site or off-site could cause malfunction in, or damage to, the facility's systems and components, particularly instrumentation.

Engineering principles: external and internal hazards	Use, storage and generation of hazardous materials	EHA.13
The on-site use, storage or generation of hazardous materials should be minimised, controlled and located, taking due account of potential faults.		

268. Principle EKP.1 is relevant here and should lead to designs that seek to (for example) eliminate the hazard or use less hazardous substitutes.

269. The analysis should take due account of fires, missiles, toxic gases etc, either resulting from a fault or as part of an initiating event. The potential faults considered should include the inadvertent release of the hazardous material.

270. The potential for generation of hazardous materials (including toxic, corrosive and flammable materials) through normal processes or in fault conditions should be analysed.

Engineering principles: external and internal hazards	Fire, explosion, missiles, toxic gases etc – sources of harm	EHA.14
Sources that could give rise to fire, explosion, missiles, toxic gas release, collapsing or falling loads, pipe failure effects, or internal and external flooding should be identified, specified quantitatively and their potential as a source of harm to the nuclear facility assessed.		

271. The safety case should include:

(a) projects and planned future developments on and off the site;

(b) the adequacy of protection from the effects of faults and accidents either within or external to the facility; and

(c) sources of harm such as means of transport, pipelines, power supplies and water supplies, located either inside or outside the site.

Engineering principles: external and internal hazards	Hazards due to water	EHA.15
The design of the facility should prevent water from adversely affecting structures, systems and components.		

272. The design of the facility should include adequate provision for the collection and discharge of water reaching the site from any design basis external event or internal flooding hazard. Where this is not reasonably practicable, the structures, systems and components should be adequately protected against the effects of water. (See also Principle EHA.12.)

Engineering principles: external and internal hazards	Fire detection and fighting	EHA.16

Fire detection and fire-fighting systems of a capacity and capability commensurate with the worst-case design basis scenarios should be provided.

273. A fire hazard analysis should be carried out to:

(a) analyse the potential for fire initiation and growth and the possible consequences for the facility's structures, systems and components;

(b) determine the need for segregation of plant and equipment and the locations and required fire resistance of boundaries needed to limit the spread of fires; and

(c) determine the capacity and capability of the detection and fire-fighting systems.

274. The systems should be designed and located so that any damage they may sustain, or their spurious operation, does not affect the safety of the facility (see Principle EHA.15).

Engineering principles: external and internal hazards	Appropriate materials in case of fires	EHA.17
Non-combustible or fire-retardant and heat-resistant materials should be used throughout the facility.		

5. ADVICE TO INSPECTORS

General

5.1 The overall objective of the principles is to minimise the effects of internal hazards, particularly to ensure that internal hazards do not adversely affect the reliability of safety systems designed to perform essential safety functions and that the potential common cause effects of internal hazards have been adequately addressed. Items important to safety (i.e. safety systems and safety related systems) should be either qualified to withstand the effects of internal hazards or protected against the hazards, i.e. appropriate use of equipment qualification, redundancy, diversity, separation or segregation.

5.2 In achieving this objective, the principles require that a comprehensive and systematic approach is used to identify the internal hazards and that the hazards are then appropriately combined with consequential and/or simultaneous hazards and/or faults and, where necessary, take into account plant out for maintenance. A "defence in depth" approach should be applied to internal hazards, that is, for each internal hazard that cannot be eliminated the following approach is used:

- Prevent the hazard
- Limit the severity of the hazard should it occur
- Limit the consequence of the hazard should it occur and be severe

5.3 The safety case should demonstrate how the "defence in depth" philosophy has been applied to each internal hazard and identify the appropriate control measures.

5.4 With regard to the hazards analysis and the requirement for an appropriate combination of consequential and/or simultaneous hazards and/or faults, see EHA.5 & 6, the following interpretation should be applied:

5.5 ((Hazard + consequences[i]) + (independent fault[ii]) + (minimum plant availability)) applied with the system parameters at their most adverse allowed limits[iii].

[i] The consequences of a hazard should include consequential hazards and consequential faults

as appropriate.
[ii] The reference to “fault” also included hazards and the possibility of single failure.
[iii] Not all elements of the combination should be applied deterministically (i.e. hazard + fault + maintenance) and lead to the requirement for 4 x 100% trains, but consideration of the frequency of the hazard and the reliability of plant equipment need to be included. That is (hazard including consequences + minimum plant availability) applied with adverse system parameters to be applied deterministically and the inclusion of an independent fault (fault or hazard) be related to the initial hazard frequency.

Fire

5.6 One of the basic safety requirements found in both the SAPs and IAEA Safety Standards Series No. SSR-2/1 (Ref. 6) is to engineer "defence in depth". “Defence in depth” within the SAPs is addressed within EKP. 3 and its associated commentary.

5.7 With regard to fire, "defence in depth" may be achieved by:

- Preventing fires from starting,
- Limiting the severity of fires that start, and by
- Limiting the consequences of fires that start and are severe

5.8 The measures required to achieve these objectives encompass good engineering design and subsequent residual hazard identification and assessment. Clearly:

- Combustibles should be minimised, fires quickly detected and extinguished. Items important to safety should be protected from fire effects and adequately segregated using fire barriers. The fire barriers should be rated to withstand total combustion of the fire load in the compartment (i.e. total burnout); this is referred to as the “fire containment approach”. Where this is not practical due to conflicts with other plant design requirements, separation of the items important to safety could be achieved using an appropriate combination of limited combustibles, distance, local passive fire barriers, shields, cable wrap and fire suppression systems etc; this is referred to as the “fire influence approach”. The fire containment approach is the preferred approach [4].
- Residual hazards due to omission of adequate measures (e.g. fire barriers, detection and suppression etc) or where possible failure of the measures may result in significant consequences, should be identified and documented using a systematic methodology aimed at ensuring completeness.
- Where appropriate the hazards arising from fires, where either single or multiple measures are designed to prevent their escalation, should be quantified and assessed to verify the adequacy of the measures for preventing fire spread and maintaining the integrity of the safety systems. As part of the verification, the measures should be allocated an appropriate safety category (A-C) and safety classification (1-3) to clearly identify their role in ensuring nuclear safety. Refer to SAP Engineering Principles ECS.1 & ECS.2 respectively.

5.9 IAEA guidance documents consider the need for fire protection in the design and operation of nuclear power plants ([3]&[4]). A number of the recommendations within those documents have been incorporated within this TAG, however, these documents, including all of their recommendations, should be considered as part of the assessment as they contain further detailed information.

5.10 The achievement of adequate fire safety has three essential elements, the first of which may be summarised as:

All reasonably practicable means commensurate with good engineering practice should be adopted in the design and layout of the plant, and through the use of fire detection and suppression equipment of appropriate capacity and capability, to reduce the likelihood of fires and mitigate against the consequences of fires.

To meet this objective it is necessary that:

- Non-combustible construction materials, electrical cabling and working fluids should be used wherever it is reasonable to do so.
- Ignition sources should be eliminated so far as is reasonably practicable. 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 categorised accordingly. Adequate risk assessments are required in areas where there are dangerous and explosive substances present under the requirements of DSEAR Regulations and other relevant regulations.
- 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.
- The quantity of combustible materials in storage should be minimised. Storage facilities should be segregated from areas containing safety related plant and equipment by spatial or physical barriers. Storage facilities should be provided with suitable fire detection and suppression facilities.
- Bunds, drip trays and flange shields etc, should be provided to control and contain any leakage of combustible or flammable liquids as well as any potential fire initiators.
- Multiple trains of systems and components required to perform essential functions should be suitably segregated either by the fire containment approach (i.e. fire barriers) or the fire influence approach (i.e. combination of distance and fire detection and suppression systems etc).
- All penetrations in fire barriers should be minimised and specified to at least the same level of fire resistance as the 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/and the acceptability of, the transmission of “cold” smoke. The ventilation system integrity should be maintained despite possible filter fires or any other fire or explosion hazards.
- Consideration should be given to the need to provide structural steelwork with passive fire protection depending on its safety function.
- The importance of safety features and fire protection systems should be assessed, assigned appropriate safety categories and safety classifications and included as appropriate in maintenance schedules and operating instructions. In particular safety management procedures should be established for maintaining the integrity and reliability of fire barriers and any penetrations such as doors, cable and pipe conduit seals, heating, ventilation and air conditioning ducts and dampers.

5.11 The second element is:

The adequacy of the engineered safeguards should be assessed. Residual fire hazards, in particular hazards to items important to safety that may arise due to the failure of barriers and escalating fires should be identified using an appropriate systematic methodology, the results documented and consideration given to any

requirement for a hazard analysis. Any hazards caused by the use of firefighting equipment or its spurious operation should also be identified.

In meeting this objective it is necessary that:

- The location of combustible inventories in the vicinity of items important to safety should be identified and documented. Similarly any ignition sources should be documented.
- Sufficient procedures and controls should be 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. Likewise, the control of ignition sources should be managed to minimise the likelihood of ignition of combustibles adjacent or near to items important to safety.
- Systematic methods and procedures should be detailed and employed for identifying the consequences of escalating fires. Assurance should be provided on the completeness of the hazard identification methodology.
- The results of the fire hazard identification procedures should be documented to provide a basis for any hazard analysis that may be required.
- 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.
- The consequences of flooding from the operation or failure of water or gas based fire suppression systems should be assessed 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 items important to safety.
- Possible consequences of fire water run-off 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.

5.12 The third element is:

The potential for fire initiation and growth and the possible consequences on items important to safety should be determined to confirm the adequacy of fire resistant boundaries and the capacity and the capability of the fire detection and firefighting systems designed to limit the spread of fires.

Compliance with this objective requires:

- Hazard analyses are carried out, as appropriate, to confirm the adequacy of the fire barriers, the adequacy of passive protection applied to structural steelwork, to confirm that equipment is adequately qualified against fire, and to justify deterministic rules for using distance and fire detection and suppression systems etc, to provide an alternative means of equipment segregation.
- All deterministic and probabilistic data used in the analysis are justified. Licensees should place the greater emphasis on deterministic means of demonstrating safety, however, it is recognised that some recourse may be made to probabilistic arguments when assessing the effectiveness of fire protection measures. In such an event, estimates of failure probabilities and consequences should be shown to be commensurate with the age of the plant and equipment.

- Computational methods are validated and verified for the type of building construction and spatial features of the area requiring an analysis.

Explosion/missiles

5.13 Nuclear Sites contain 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) that can fail disruptively and materials that can react explosively. Therefore safety cases must demonstrate that the following requirement is met.

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 explosions and missiles. The hazards should be prevented or minimised but where they are not avoidable items important to safety should be protected by spatial or physical barriers. The potential for explosions/missiles to damage firefighting systems should be recognised when deciding on their design and location.

Some specific matters to be addressed in the design and safety of the plant with respect to missile/explosion hazards are:

- Sources of possible explosions/missiles should be identified, the possible magnitude of explosions, blast waves and the likely size, frequency and trajectory of missiles estimated, and their effects on items important to safety assessed.
- The results of a hazard analysis in conjunction with the licensee's 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.
- Possible causes of explosions to be considered include the ignition of flammable gas, vapour or oil-mist clouds, exothermic reactions, pyrophoric materials, failure of pressure parts, and explosions associated with switchgear, high energy transformers, electrical batteries, terminal boxes and power cables.
- Hydrogen must be treated with particular care as hydrogen explosions can be very violent. Flammable and potentially explosive gases such as propane and butane are burned to supply heat for carbon dioxide and nitrogen vaporisation. In addition to the effects of blast overpressure, the hazard analysis should consider the heat and toxicity of hot or burning gases, fire, and the generation of missiles.
- Missiles may be generated when a pipe or vessel totally disintegrates. Missiles may also be generated by failure of rotating plant. Devices should be fitted to prevent overspeed and to warn the operator of excessive vibration from rotating plant.
- Where substances such as high pressure gases have been released due to disruptive containment failure, it will be necessary to consider the effect of pressure and rarefaction wave propagation on components within the system. The discharging gas may have the potential to affect items important to safety out with the affected system. For example, in addition to missiles there may be significant reaction loads, pipewhip, and jet loads.
- Any movement of explosive materials or gases by vehicular transport or pipeline on the site should be considered.
- Consideration should be given to the need for ensuring that control rooms and buildings are blast resistant, or to the alternative arrangements in the event of damage to these areas.

Toxic and corrosive materials and gases

5.14 Toxic and corrosive materials and gases have the potential to disable both personnel and items important to safety. Therefore the safety case should provide a demonstration that the following requirement is met:

The safety case should identify the range of materials that if released could either disable/impair or cause the asphyxiation of personnel, or may disable items important to safety. The safety case should also demonstrate the adequacy of the engineered safeguards.

The following require consideration when assessing the effects of toxic or corrosive materials and gases:

- On nuclear facilities there are a number of asphyxiants, acids, alkalis and solvents whose release may jeopardise nuclear safety. In the case of a number of these chemicals, a large release may disable operators or cause a sudden, uncontrolled evacuation, so the location of permanently occupied areas such as control rooms and offices in relation to hazardous chemical storage should be chosen carefully.
- The hazard analysis should consider the probability of major releases and the subsequent effects of gas clouds on personnel and plant equipment. Care should be taken to ensure that the release of toxic substances could not prevent any necessary operator action to control the incident or to safely shutdown a plant and maintain it in a safe shutdown state.
- Items important to safety, including cabling and electrical control cabinets should be designed and located so as to minimise, consistent with other safety requirements, damage due to the release of gas, water, steam, smoke or any other noxious substance.
- The possibility of toxic gases entering ventilation systems and thereby affecting operators in the control room should be minimised. Adequate arrangements should be made to mitigate the effects of releases of toxic substances.

Dropped loads

5.15 Nuclear installations contain a variety of cranes and nuclear related lifting equipment - pile cap and polar cranes, flask handling machines, Turbine Hall cranes, maintenance hoists etc. The failure of this equipment potentially risks damaging nuclear material containment or damage to items important to safety. The use of cranes and other lifting equipment is covered in detail within. However, the threats associated with dropped loads and the potential domino effects e.g. fire, explosion and flooding are considered within this guidance. To control the risks the following objective should be met:

A safety case should demonstrate that dropped loads either have no potential to disable items important to safety or that there is an adequate combination of engineered safeguards and management controls to adequately limit the risk.

The following matters should be borne in mind by the assessor:

- The standards of design, construction, operation and maintenance of cranes and lifting equipment should be commensurate with the radiological consequences of their failure.
- Failure of lifting equipment can result from overloads caused by dynamic magnification of normally safe working loads or may be a consequence of fatigue crack propagation, corrosion or component wear etc. The integrity of overload protection systems and both mechanical and civil support structures should be assessed.
- 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 items important to safety and the extent of possible damage should be estimated and its significance assessed. Where necessary appropriate mitigating systems should be identified (depending on the estimated frequency of the dropped load event) or additional protection or operating restrictions should be provided.

Structural Collapses

5.16 It is to be expected that structures present at a nuclear site will be conservatively designed against severe hazards to an appropriate level commensurate with their consequence of failure. Therefore it is to be expected that the risk of a structural collapse will be low. Nevertheless it is appropriate that there is no disproportionate failure consequence as a result of an error or omission during operations or maintenance.

A safety case should demonstrate that structural collapses are either not nuclear safety related or that responses to possible operator errors could not lead to a disproportionate failure consequence.

The following matters should be borne in mind by the assessor:

- It is preferable to justify structures as hazard resistant rather than to provide barriers as a defence against structural collapses.
- Failure modes should be ductile rather than brittle.
- Under possible overload situations failure modes should be controlled with minimal potential for damage and release of energy, not disproportionate. (For instance should a load lifted by a crane snag it is preferable that the failure mode should be controlled and near to the point of the snag, rather than a full crane topple or a collapse of a structure supporting the crane.)
- Single failure mode criteria should be applied.

Impacts from Vehicular Transport

5.17 At nuclear installations material and equipment is moved using a variety of forms of transport. If the transport is not adequately controlled there is a potential for impacts that could have implications for nuclear safety. At facilities where submarines operate there is increased potential for impacts associated with submarine and ship movements. Impacts between submarines and ships and between submarines and shore facilities are potential hazards. The safety case needs to justify that movements with safety implications are controlled and sufficient defences are provided so that the risk of an impact leading to a nuclear consequence is acceptably low. To control the risks the following objectives should be met:

A safety case 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 limit the risk.

The following matters should be borne in mind by the assessor:

- The speed and travel paths of vehicles need to be controlled and monitored using appropriate procedures commensurate with the consequences of an operator error.
- Consideration needs to be given to having more onerous operating restrictions if there is potential for two vehicles to be moving in the same area at the same time.
- When appropriate vehicles need to be provided with automatic systems to prevent operation outside the design basis envelope.

- When a possibility exists that an impact might reasonable occur with a nuclear consequence appropriately designed energy absorbing barriers should be provided. The design specification should allow for vehicles operating outside of their normal procedures.

Flooding / spray

5.18 Flooding and spray hazards can occur due to leakage from any pipework or tanks containing any fluid, including general cooling water services, fire suppression services, boiler feedwater and condenser cooling water supplies, oil and acid reservoirs, etc.

The potential hazard to items important to safety from flooding and spray due to leaking vessels and pipework should be identified. Items important to safety should be sited so as to minimise the risk and other appropriate engineered safeguards implemented. The impact of the environment and the chemical composition of the spray also need to be considered.

Examples of specific matters that should be addressed are:

- Hazard analysis should consider flooding and spray hazards originating from both random and common cause effects, including component failure and human error. In the event of a spray from an oil line or tank the risk of fire and explosion is increased and can result in ignition of the spray at temperatures far lower than their flash point.
- The design of the plant should include adequate provisions for identifying and for the collection and discharge of water arising from any failed systems on site.
- A systematic approach to the mitigation of the consequences of all assumed flooding events should be demonstrated. This should include detailed consideration of the plant layout, preferably including a specific walkdown. For each assumed flooding event mitigating features such as drainage, provision of drip trays and raising of equipment above floor level should be employed to minimise the effect on items important to safety including electrical control and protection equipment. Wherever possible it is particularly important to ensure adequate segregation of any alternative/redundant system to ensure that a single source of flooding cannot jeopardise both (or all) systems.
- The effects of flooding on nuclear significant floors and walls should be assessed to ensure any credible flood could not result in potential domino effects. Where there is potential for flood water to build up to any depth appropriate checks should be undertaken to confirm the integrity of structural components to the water loading.
- The effects of internal flooding as a result of the operation of fire protection systems should be assessed. Water from fire suppression systems within cable flats and risers has the potential to pass into safety related rooms and result in spurious operation or failure of items important to safety.

6. REFERENCES

1. Safety Assessment Principles for Nuclear Facilities. 2014 Edition Revision 0. November 2014. www.onr.org.uk/saps/

2. WENRA Safety Reference Levels for Existing Reactors, September 2014 http://www.wenra.org/

3. *Protection against Internal Fires and Explosions in the Design of Nuclear Power Plants.* International Atomic Energy Agency (IAEA), Safety Guide, NS-G-1.7. IAEA, 2004 www.iaea.org

4. *Fire Safety in the Operation of Nuclear Power Plants*. International Atomic Energy Agency (IAEA), Safety Guide, NS-G-2.1. IAEA, 2000 www.iaea.org.

5. *Protection against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants*. International Atomic Energy Agency (IAEA), Safety Guide, NS.G.1.11. IAEA, Vienna 2004. www.iaea.org.

6. Safety of Nuclear Power Plants: Design. International Atomic Energy Agency (IAEA). Specific Safety Requirement No. SSR-2/1. IAEA. Vienna. 2016 www.iaea.org

7. *Safety of Nuclear Power Plants: Commissioning and Operation.* International Atomic Energy Agency (IAEA). Specific Safety Requirement No. SSR-2/2. IAEA. Vienna. 2016 www.iaea.org

Note: ONR staff should access the above internal ONR references via the How2 Business Management System.

7. GLOSSARY AND ABBREVIATIONS

ALARP	As low as reasonably practicable
BSL	Basic Safety Level
BSL(LL)	Basic Safety Level (legal limit)
BSO	Basic Safety Objective
CBA	Cost Benefit Analysis
CCF	Common Cause Failure
DBA	Design Basis Analysis
DSEAR	Dangerous Substances and Explosive Atmospheres Regulations
EMIT	Examination, Maintenance, Inspection and Testing
HSE	Health and Safety Executive
HSWA74	The Health and Safety at Work etc Act 1974
IAEA	International Atomic Energy Agency
OBE	Operating Basis Earthquake
PSA	Probabilistic Safety Analysis
PSR	Periodic Safety Review
PSSR	Pressure Systems Safety Regulations
SAP	Safety Assessment Principle(s)
SFAIRP	So far as is reasonably practicable
SEPA	Scottish Environment Protection Agency
SSC	Structure, System and Component
TAG	Technical Assessment Guide(s)
WENRA	Western European Nuclear Regulators' Association