



ONR GUIDE			
Emergency Power Generation			
Document Type:	Nuclear Safety Technical Assessment Guide		
Unique Document ID and Revision No:	NS-TAST-GD-103 Revision 1		
Date Issued:	February 2019	Review Date:	October 2023
Approved by:	Gavin Smith	Mechanical Engineering Professional Lead	
Record Reference:	CM9 Folder 1.1.3.978. (2020/139085)		
Revision commentary:	Rev 0: New document		
	Rev 1: Updated review period		

TABLE OF CONTENTS

1. INTRODUCTION	2
2. PURPOSE AND SCOPE	2
3. RELATIONSHIP TO LICENCE AND OTHER RELEVANT LEGISLATION	3
4. RELATIONSHIP TO SAPS, WENRA REFERENCE LEVELS AND IAEA SAFETY STANDARDS ADDRESSED	4
5. ADVICE TO INSPECTORS	6
6. GLOSSARY AND ABBREVIATIONS (EXAMPLE LIST)	20
7. APPENDICES.....	21

1. INTRODUCTION

- 1.1 ONR has established its Safety Assessment Principles (SAPs) which apply to the assessment by ONR 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.
- 1.2 Technical assessment guides (TAGs) primarily provide guidance to ONR inspectors on the interpretation and application of the SAPs. They also contain guidance relevant to principles underlining the enforcement of licence condition compliance which supplements the technical inspection guides (TIGs). Thus the TAGs have relevance to all inspectors within ONR, regardless of function. The guides also provide information to licensees regarding ONR's expectations of the nature and content of relevant technical elements of licensees' submissions.

2. PURPOSE AND SCOPE

- 2.1 The purpose of this TAG is to provide guidance to assist ONR inspectors in the assessment of Emergency Power Generation systems (EPGS). An EPGS comprises of the prime mover, generator together with its auxiliaries up to the generator terminals, and the electrical equipment that enables installation of a generator(s), as necessary, to the plant and its structures, systems and components (SSCs).
- 2.2 Following a loss of normal power supply (eg Loss of Off-Site Power (LOOP)) event, an EPGS provides electrical power to the specific nuclear safety systems identified within the licensee's safety case; typically providing essential cooling and containment.
- 2.3 The guidance in this TAG is also applicable to mobile generators. The adequacy of the transport, connection and re-fuelling provisions should also be considered.
- 2.4 The principal focus of this TAG is mechanical engineering, further guidance is available in Appendix 1 and as follows:

Electrical systems

- 2.5 EPGSs are a means of increasing the availability of the electrical essential services necessary to support specified safety functions of the nuclear installation throughout its lifecycle. Inspectors are therefore advised to consider the guidance within the Essential Services TAG [3] in carrying out the assessment of EPGSs.

Control and instrumentation systems

- 2.6 The control and instrumentation (C&I) systems, including elements such as the starting system, automatic voltage regulator, EPGS synchronising schemes and multi-set controllers, are key considerations when assessing the overall ability of the EPGS to meet the safety case claims.
- 2.7 If these systems contain software elements (as in the case of smart devices, for example), ONR's expectations are as set out in SAP ESS.27 and further developed in TAG 046 [3].
- 2.8 Other C&I issues that should be considered but are not included within the scope of the TAG are:
 - Potential for environment, human error or cyber security threat to prevent correct operation.

- Support and auxiliary systems commensurate with claims being made (eg power supplies and HVAC).
- Diagnostics to identify faults and appropriate measures to address faults (eg critical spares holding and availability of technical support).

3. RELATIONSHIP TO LICENCE AND OTHER RELEVANT LEGISLATION

3.1 This section identifies the relationship of EPGSs to the site licence conditions (LC) [1]. Under the Nuclear Installations Act 1965, a set of 36 standard licence conditions are attached to each nuclear site licence. These conditions cover the facility lifecycle from design, construction, and operation through to decommissioning and include management oversight and reviews. They require licensees or duty-holders to implement arrangements to ensure compliance. The LCs and ONR Safety Assessment Principles [2] considered applicable to this TAG are presented below.

- **Licence Condition 10: Training** - The licensee shall make and implement adequate arrangements for suitable training for all those on site who have responsibility for any operations which may affect safety.
- **Licence Condition 11: Emergency Arrangements** – The role of EPGSs, as a means of dealing with any accident of emergency arising on the site and its effects, should be considered.
- **Licence Condition 12: Duly authorised and other suitably qualified and experienced persons** - Only suitably qualified and experienced persons shall maintain and operate an EPGS.
- **Licence Condition 15: Periodic review** - The licensee shall make and implement adequate arrangements for the periodic and systematic review and reassessment of safety cases. The adequacy of the licensee's safety case, where it addresses EPGSs, should be reviewed. EPGSs should be reviewed against current operating conditions and legislative requirements. Suitable and sufficient analysis techniques should be used to ensure that there have been no significant changes or deterioration (eg corrosion, wear, ageing, fatigue and damage) that may invalidate the safety case. The effect of using new fuels and any possible future changes (eg biofuels) shall be taken into account.
- **Licence Condition 20: Modification to design of plant under construction** – Modifications should be assessed to ensure that they do not impact adversely on the design and capability of the EPGS or the nuclear safety case.
- **Licence Condition 21: Commissioning** - Appropriate commissioning tests should be carried out on EPGSs to ensure, for example, that design criteria, and where practicable, the safety functional requirements claimed within the safety case have been met.
- **Licence Condition 22: Modification or experiment on existing plant** – Modifications should be assessed to ensure that they do not impact adversely on the design and capability of the EPGS or the nuclear safety case.
- **Licence Condition 23: Operating Rules** – These should determine the EPGS availability requirements for safe operation of the nuclear facility. For example, if there are insufficient operable EPGSs to meet the requirements of the safety case, the facility may have to be shut down or placed in a lower risk condition.
- **Licence Condition 24: Operating instructions** – Appropriate instructions shall be provided for operation and maintenance of EPGSs. These should

include instructions for the periodic testing of EPGs that are typically undertaken to ensure the operating service lifetime of an emergency generator set is achieved. Instructions should ensure the EPG is returned to normal condition following the test. The actions to be taken in the event of extreme weather conditions and abnormal events (eg earthquakes) should be specified.

- **Licence Condition 25: Operational Records** – The licensee shall ensure that adequate records are made of the operation, inspection and maintenance of EPGs that may affect safety.
- **Licence Condition 26: Control and supervision of operations** – The licensee should ensure that EPG operations that may affect safety are carried out under the control and supervision of suitably qualified and experienced persons appointed for that purpose by the licensee.
- **Licence Condition 27: Safety mechanisms, devices and circuits** – An EPG is a SMDC. The licensee shall ensure that plant is not operated, inspected, maintained or tested unless suitable and sufficient EPGs are properly connected and in good working order.
- **Licence Condition 28: Examination, inspection, maintenance and testing** – The licensee shall make and implement adequate arrangements for the regular and systematic examination, inspection, maintenance and testing of all aspects of an EPG, including emergency generators and their electrical installation which may affect safety at a site or facility.

3.2 The following Statutory Instruments are considered directly applicable to EPGs:

- Health and Safety at Work Act (HSWA) 1974
- Supply of Machinery (Safety) Regulations 2008
- The Provision and Use of Work Equipment Regulations 1998
- Management of Health and Safety at Work Regulations 1999
- The Electromagnetic Compatibility Regulations 2016
- The Low Voltage Electrical Equipment (Safety) Regulations 1989
- The Electricity at Work Regulations 1989

The following Statutory Instruments may also be applicable (eg compressed air systems for emergency generator starting)

- Pressure Systems Safety Regulations 2000
- Pressure Equipment (Safety) Regulations 2016
- Control of Substances Hazardous to Health 2002

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

Safety Assessment Principles

4.1 Whilst the SAPs [2] do not specifically mention EPGs, ONR inspectors should take the following into consideration in their assessment:

- ECS.1 to ECS.5 (Safety categorisation and safety classification)
- EQU.1 (Equipment qualification)
- EDR.1 to EDR.4 (Design for reliability)
- ERL.1 to ERL.4 (Reliability claims)
- ECM.1 (Commissioning)
- EMT.1 to EMT.8 (Maintenance, inspection and testing)
- EAD.1 to EAD.5 (Ageing and degradation)

- ELO.1, 2 and 4 (Layout)
- EHA.1 to EHA.17 (External and internal hazards)
- ESS.1 to ESS.27 (Safety systems)
- ESR.1 to ESR.7 and ESR.9 to 10 (Control and instrumentation of safety-related systems)
- EES.1 – EES.9 (Essential services)
- EHF.1 to EHF.10 (Human factors)

WENRA Safety Reference Levels

4.2 WENRA Reactor Safety Reference Levels [4] consider the safety requirements for existing reactors. The following areas are relevant to EPGs:

- Issue E: Design Basis Envelope for Existing Reactors
- Issue F: Design Extension of Existing Reactors
- Issue I: Ageing Management
- Issue K: Maintenance, In-Service Inspection and Functional Testing
- Issue LM: Emergency Operating Procedures and Severe Accident Management
- Issue R: On Site Emergency Preparedness
- Issue T: Natural Hazards

4.3 WENRA statement on safety objectives for new power plants defines the safety objectives for new power plants [4], so that:

- New nuclear power plants to be licensed across Europe in the future will present less risk than the existing ones, especially through the improvements of the design.
- Regulators press for safety improvements in the same direction and ensure that these new plants will have high and comparable safety levels.
- Applicants take into account this common position when formulating their regulatory position.

IAEA Safety Standards

- 4.4 IAEA Safety Standard SSR-2/1 [5], Revision 1 for the Safety of Nuclear Power Plants Design, Requirement 68 requires the emergency power supply at the nuclear power plant shall be capable of supplying the necessary power in anticipated operational occurrences and accident conditions, in the event of the loss of off-site power.
- 4.5 IAEA Specific Safety Guide SSG-34 [5] Design of Electrical Power Systems, for Nuclear Power Plants, contains recommendations and guidance on the provision of standby and alternate AC [alternating current] sources.
- 4.6 IAEA Specific Safety Guide SSG-34 [5] Design of Electrical Power Systems, for Nuclear Power Plants (NPP). ONR considers this to be a source of relevant good practice when assessing EPGs. Although written from a NPP perspective, ONR considers the guidance is applicable to Non-NPP situations.

- 4.7 IAEA Safety Guide NS-G-2.12 Ageing Management for Nuclear Power Plants, provides guidance on managing ageing for nuclear power plant. See NS-TAST-GD-098 (Asset Management) for further guidance on this topic.

5. ADVICE TO INSPECTORS

Overview

- 5.1 This guide sets out what ONR considers relevant good practice (RGP) taken from national and international guidance. In support of this TAG, ONR commissioned a report [8] to identify national and international relevant good practice for diesel generators.
- 5.2 This TAG can be used for assessment of activities and safety submissions such as:
- construction and installation of new plant (LC19)
 - modification or experiment on existing plant (LC22)
 - periodic review (LC15)
- 5.3 It also informs the inspection of licensees' arrangements for examination, inspection, maintenance and testing (LC28) of EPGs.
- 5.4 A multi-discipline approach should be taken for the assessment of EPGs, this will typically require interaction between the following specialisms:
- Mechanical engineering
 - Electrical, Control and Instrumentation engineering
 - Fault studies
 - Internal hazards
 - External hazards
 - Human factors

Emergency power generation system (EPGS) description

- 5.5 An EPGS is a prime mover, usually a diesel engine or gas turbine, coupled to an electrical generator that provides electrical power to plant essential for nuclear safety when the normal/preferred power supply is interrupted. They are important safety components as they provide a source of back-up power to activate and maintain nuclear safety systems (eg reactor cooling systems).
- 5.6 Each EPGS will include both primary and auxiliary structures, systems and components (SSC). Primary SSCs are those that are essential for delivering emergency power. Ancillary SSCs provide infrastructure, support and services for the EPGS. Examples are as follows:

Primary SSC	Ancillary SSC
<ul style="list-style-type: none"> • Diesel engine or gas turbine • Electrical generator • Generator exciter • Filtered combustion air intake • Cooling system (see below) • Lubrication system • Fuel tank and delivery system • Starter system (eg compressed air and batteries) • Electrical protection system for the EPGS • Control and instrumentation system • Distribution and connection of power to plant 	<ul style="list-style-type: none"> • Building structure and enclosure • Foundations • Exhaust extract system • Heating and ventilation system • Filling and draining equipment • Maintenance equipment (eg lifting and handling)

Table 1 – Primary and ancillary SSCs

5.7 The safety case should demonstrate that the EPGS has adequate energy (eg electricity and compressed air) stored for engine starting and restarting.

Safety case requirements

5.8 The safety function requirements attributed to an EPGS should be stated within the safety case. For example, an EPGS should provide adequate backup power to enable specified safety functions to be maintained by essential services systems for a suitable and sufficient period until either the function is no longer required or the preferred (normal) power supply has been restored.

5.9 It is expected that the safety case should:

- Establish the safety functional requirements (i.e. claims) for the EPGS.
- Determine the safety classification of the EPGS (based on the relevant safety classification of the SSC(s) they support).
- Demonstrate that the EPGS is meeting the relevant claims and safety classification (through a combination of design considerations, commissioning, testing and EIM&T).

5.10 For the purposes of this guide, the term 'mission time' is the time an EPGS is required to provide back-up power as defined by the safety case.

5.11 When determining the safety function requirements, it is essential to determine:

- The electrical generation capacity required
- The time over which the generation is required
- What start-up time is acceptable (i.e. delay) before the generation is effective
- The appropriate safety function category. SAP ECS.1 (Safety categorisation).
- The appropriate safety classification of the SSCs that make up the EPGS in its role as an essential support system. SAP ECS.2 (Safety classification of structures, systems and components)
- Internal and external hazards (SAP EHA.1 to 19)
- The interfaces and supporting systems needed to ensure successful delivery of the electrical generation to the specified safety-related electrical loads.

- 5.12 It is expected that the safety case will present arguments based on ONR's SAP EKP.3 (Defence in depth), which reflects international good practice regarding the need for independent safety barriers. It should be noted that some of the safety measures at each defence in depth level may be diverse systems and, hence, do not place any claims on the EPGs. If such measures offer an adequate means of protection, this might provide adequate diversity eliminating the potential for common cause failures associated with diesel generator (DG) and gas turbine generator (GTG) systems.
- 5.13 Adequate defence-in-depth provision relies on:
- There being sufficiently robust measures at each level.
 - Common cause failures should not adversely affect levels of redundancy and diversity. SAP EDR.3 (Common cause failure).
- 5.14 A fault studies specialist may be required to assess the licensee's overall safety case and claims on the EPGs. A key point of clarification being whether the support from an EPGs is for postulated design basis fault scenarios (Levels 1, 2 & 3 of the defence in depth model) or for beyond design basis scenarios (Levels 4 & 5 of the defence in depth). This will impact on the safety classification of the EPGs and hence ONR's assessment in determining the detail and rigour expected from the licensee's substantiation.
- 5.15 The operating and EIM&T strategy for EPGs should prioritise the safety case requirement to deliver reliable emergency power generation. It is therefore not expected that an EPGs would be operated for commercial gain (eg to earn revenue or reduce operating costs). This would deplete available fuel stocks and reduce the duration that essential loads could be supplied during a LOOP event. Extended non-safety related operation of an EPGs might also increase wear and tear and thereby reduce reliability. Where the duty holder's safety case requires a test regime which involves extended operation (eg to demonstrate satisfactory performance or to ensure fuel is refreshed) a reasonable side benefit might be commercial gain. Inspectors should note that such practices would also have to be agreed with the Environment Agency (EA) and the Scottish Environment Protection Agency (SEPA).

Note:

An EPGs may be combustion plant and require a permit from the Environment Agency. If the total thermal input exceeds 20 MWth [thermal megawatts], the combustion plant is also a 'regulated activity' as defined in the Greenhouse Gas Emissions Trading Scheme Regulations (2012) and will require a permit under those regulations.

- 5.16 Inspectors should ensure that the licensee has considered how the available generation capability would be used during an extended loss of power. For example, it may be necessary to provide emergency power for a longer period than the maximum mission time assumed in the design basis scenario. Over time, the emergency power demand for some essential services may reduce (eg decay heat removal). This may offer the opportunity to preserve fuel stocks. A risk-based approach should be considered as a means of prioritising fuel usage. This is illustrated in Figure 1 below.

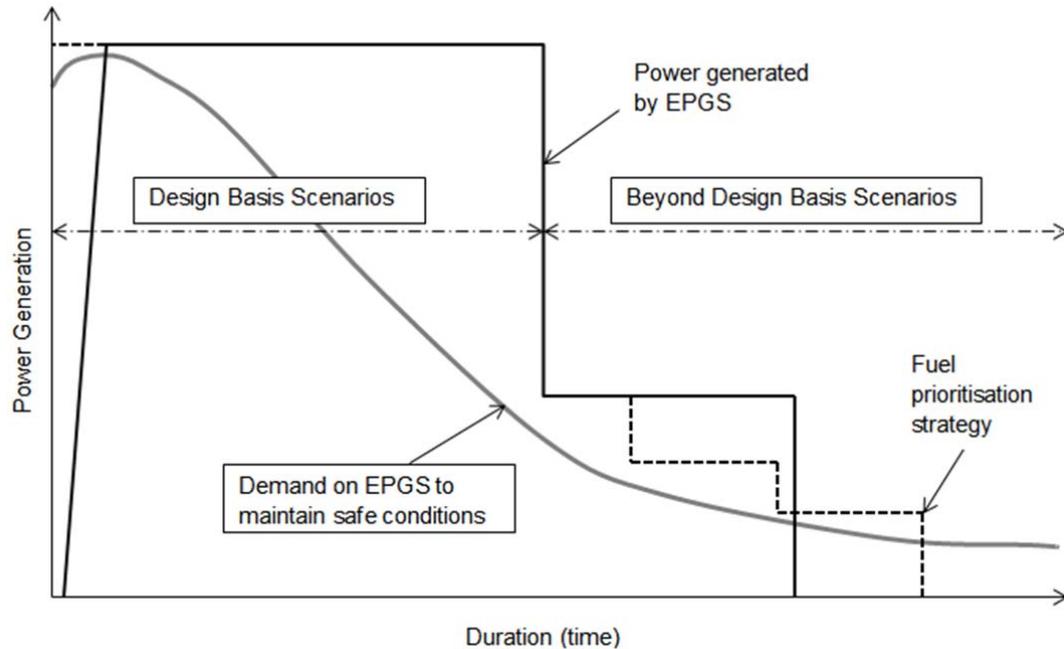


Figure 1 – Extended Power Loss Scenario

- 5.17 It is expected, in line with ONR SAP SC.6, that the safety case identifies the important aspects of operation and management required for maintaining safety and how these will be implemented. This includes:
- The operating limits and conditions (operating rules) required to ensure that the facility is operated safely at all times (LC23)
 - The procedures and instructions that need to be followed (LC24)
 - The necessary safety mechanisms, devices and circuits (SMDCs) installed and functioning (LC27)
 - The examination, inspection, maintenance and testing regimes justified in or assumed by the safety case (LC 28)
 - Control, supervision, qualification and training and other safety management requirements (LC10 and LC12)
 - Inputs to emergency arrangements (LC11)
- 5.18 ONR inspectors should review how licensees monitor and adequately demonstrate the satisfactory performance of their EPGs in comparison with the claims made within nuclear safety case, including any relevant reliability claims.
- 5.19 The safety case claims on EPGs should not be undermined by dependencies on their supporting services. For example, EPGs should not only store sufficient energy for engine starting and restarting but have a suitable means to replenish the lost energy.
- 5.20 Licensees should be able to demonstrate from a suitable test programme that there is sufficient fuel and services capacity (eg batteries and compressed air) to meet the safety case demand.

System management and accountabilities

- 5.21 Reliability claims within safety cases should address the risk and evaluate the consequences of EPGS 'failure to start' and 'failure to continue running' to operate for a defined time.
- 5.22 It is therefore expected that licensees will gather and analyse failure and asset condition data for the purpose of providing confidence, identifying shortfalls and, hence, suitable improvement. The licensee should therefore have clearly defined safety case derived criteria against which such technical assessments can be made. This will include a clear definition of the actions that need to be taken to secure safety of the plant or facility.
- 5.23 For new EPGS plant, safety case requirements should be determined early. As a means of identifying safety improvements and increasing plant availability, the original equipment manufacturer (OEM) and maintenance and operational staff should be actively involved in the design process.

Learning from the Fukushima accident

- 5.24 In March 2011, an undersea seismic event generated a tsunami that overwhelmed the seawalls and inundated the Fukushima Daiichi Nuclear Power Plant (NPP). The tsunami engulfed all the structures and equipment located at the seafront. Insufficient protection against flooding resulted in the loss of five of the six emergency diesel generators.
- 5.25 Inspectors should expect licensees to demonstrate that they have applied learning from the Fukushima Daiichi Nuclear Power Plant accident [7] to the provision of new EPGS facilities and incorporated suitable and sufficient redundancy, diversity, segregation and layout of the equipment. NS-TAST-GD-036 Redundancy, segregation and layout of mechanical plant [3] and should therefore be considered in the assessment of new EPGS facilities.
- 5.26 Learning from the Fukushima accident should be taken into account in the Periodic Review (LC15) of existing facilities. It is expected that licensees will take account of new technologies and worldwide operating experience to identify reasonable improvements to the resilience of its EPGSSs.

Redundancy

- 5.27 The safety case should determine the number of EPGs within an EPGS required to meet the deterministic and probabilistic safety requirements. This should include sufficient redundant provision to allow the safety function to be met when one or more EPGs are unavailable, eg equipment failure or planned examination, inspection, maintenance and testing (EIM&T) activities.
- 5.28 Support system equipment (eg cooling and lubrication pumps) for each redundant EPGS should be supplied with power from the division it serves, rather than from a common source. This is to preserve the redundancy and independence of the divisions.
- 5.29 At all times there should be sufficient EPGSSs available to deliver the emergency power requirement. These should be defined by the safety case (LC23 – Operating Rules and LC24 – Operating Instructions) to limit the effect of plant unavailability on the system contribution to the risk.
- 5.30 The impact of the anticipated maintenance, test and repair work on the reliability of EPGSSs should be considered. If the resultant reliability or availability to perform a

safety function is such that the EPGS no longer meets the claims defined in the safety case, the nuclear plant it serves should be placed in a safe state and the relevant EPG temporarily out of service should be substituted or restored within a specified time.

Segregation

- 5.31 The risk of common cause failures from hazards may be reduced by system segregation. This is the separation of components by distance or physical barriers. The safety case should demonstrate that EPGs and key components (eg fuel tanks and fuel feed lines) are adequately segregated.
- 5.32 Evidence should be provided to demonstrate that functionality will be adequately maintained when the EPGS is subjected to a range of relevant internal hazards, (eg projectiles, fire and internal flooding) and external hazards (eg aircraft crash, flooding and seismic activity). SAP EHA.6 (Analysis).

Layout

- 5.33 EPGs should be assessed to ensure that they remain operable and accessible in the event of design basis faults, accidents or hazards occurring. This is particularly important where SSCs important for safety or parts thereof are co-located with other plant which may not be safety related. SAP ELO.1 (Access).
- 5.34 A manufacturer's preferred layout of an EPGS may be driven by non-nuclear safety requirements which may not be suitable for nuclear use. Consideration should be given to alternative layouts that ensure that EPGs can perform their safety function following any postulated initiating event.
- 5.35 The EPGS layout should ensure that local access is provided for manual intervention, wherever necessary. These aspects of an EPGS design, construction and installation need to be assessed in relation to the claims made by the licensee's safety case regarding access provision during operating and fault conditions. An example of this would be the refilling of EPGS fuel tanks following a seismic event.

Diversity

- 5.36 Engineering diversity is considered to be the provision of dissimilar means of achieving the same safety function, eg the use of features which differ in the physical means of achieving a specific function or use of different equipment made by different manufacturers. The safety case should clearly demonstrate that diversity has been achieved so far as is reasonably practicable. SAP EDR.2 (Redundancy, diversity and segregation).
- 5.37 Key elements of an EPGS such as DGs and GTGs may be based on commercial off the shelf (COTS) items of equipment that are procured from a small number of specialised manufacturers. Opportunities for engineering diversity should be investigated but in practice options may be limited. It may therefore not be appropriate to modify EPGS designs and manufacturing techniques that have evolved over many years through operational feedback that has progressively improved reliability and durability. Likewise, changes to the manufacturers' established supply chains may have a negative effect on EPGS reliability.
- 5.38 Diversity might be claimed, in part, by procuring emergency generators from different manufacturers or a different type offered by one manufacturer, but with a different configuration and running parameters. Inspectors should note that even units from different suppliers, or those manufactured in a different factory, may use common components (eg castings, bearings, fuel injectors and engine controllers). It may therefore not be practicable to achieve true diversity for this equipment.

- 5.39 Diversity might be claimed by the provision of both DG and GTG systems. However, the two systems may share common components and sub-systems eg air compressors for starter systems and generator sets.
- 5.40 One aspect of diversity is the selection of cooling systems. A diesel engine can be water or air-cooled, whereas gas turbines are air-cooled. However, each system type is vulnerable to individual component failure, such as pumps and fans. Consideration of diversity should also apply at component level to avoid failure modes that could affect all emergency generators. This is consistent with the expectation that licensees should demonstrate the cooling system reliability and fault tolerance does not affect the ability of the emergency generator to adequately deliver its nuclear safety function.

Dependent failures

- 5.41 ONR inspectors should be satisfied that the risk from dependent failures of EPGs has been reduced to a level which is acceptable within the limits set by the documented safety case. This should include both deterministic and probabilistic considerations where appropriate.
- 5.42 Multiple failures can occur due to common weaknesses or dependencies shared by components. Inspectors should be aware that this also applies to dissimilar emergency generators that are designed and manufactured by different subdivisions within a larger parent company. Design (or 'systematic') failures also become more prevalent as complexity increases.
- 5.43 Such failures can result in the failure of all redundant components in a single protection system or failure of components in more than one system. Dependent failures can considerably reduce the reliability of the protection systems relative to that expected from consideration of random failure mechanisms acting alone. See NS-TAST-GD-036 (Diversity, redundancy, segregation and layout of mechanical plant) for further guidance.
- 5.44 ONR inspectors should review the measures taken by the licensee to limit the effect of dependent failures on EPGs.
- 5.45 Where multiple emergency generation sets are used, the safety case should state the level of redundancy to accommodate failures, and diversity and independence between sets to reduce the likelihood of common cause failures (CCF). SAP EDR.2 (Redundancy, diversity and segregation) and EDR.3 (Common cause failure).

Start Up

- 5.46 The starting of an EPG is critical to delivery of the required safety function. The EPG selected should be capable of generating sufficient electrical power within the time period specified by the safety case. Licensees should demonstrate that the EPG starting system reliability is commensurate with the overall reliability being claimed.
- 5.47 Common to all turbines, GTGs will only work when the fuel is ignited and the blades are spinning at sufficient speed to compress the incoming air to the required pressure. Another means is therefore required to spin the compressor up to speed. This must be factored into the starting time and needs to be considered in the selection of the EPG.
- 5.48 EPG starter systems should have sufficient services (eg battery capacity and compressed air volume) and fuel for several start-up attempts and to allow for a period of continued operation beyond the normal start-up timescale. This should be factored into the capacity of the starter system.

- 5.49 The guidance on DGs within this TAG is applicable to diesel engines should they be used for starting GTGs.

Spurious operation

- 5.50 EPGs may be subject to spurious operation faults in addition to operational failures. Measures need to be employed by the licensee to ensure that wherever possible EPGs are not adversely affected by the spurious operation or failure of other systems, especially through any potential for hidden dependency. SAP ESS.17 (Faults originating from safety systems).

External hazards

- 5.51 External hazards challenge the ability of EPGs to deliver their nuclear safety function. The nuclear safety case may require the EPGs to operate during and following an external hazard event. Inspectors should consider the guidance in External Hazards TAG [3].

Design basis events

- 5.52 The EPGs design should take account of power de-rating during high ambient temperatures.
- 5.53 Combustion air intakes may require frost protection for low ambient temperatures. Control and instrumentation may also be affected, eg fuel level gauges on external storage tanks.

Loss of normal power source

- 5.54 Design basis loss of off-site power events could range from a short power dip of a few milliseconds to a national grid blackout which may last for several days. On site electrical infrastructure failures and mal-operation in addition to grid phase unbalance faults, grid high and low voltage and grid high and low supply frequency are all faults that may result in EPGs being used as an alternative source of power.

Aircraft crash

- 5.55 The nuclear safety case should define the EPGs facility withstand requirements for design basis aircraft crash, including fire and explosion hazards. Where there is no withstand requirement, the safety case should establish the requirements for segregation and redundancy to ensure that the loss of one (or more, if applicable) EPGs can be acceptable.

Earthquake / seismic event

- 5.56 EPGs are likely to be required to operate following a seismic event, which may result in loss of incoming supply, sub-station trip or a reactor shutdown. EPGs should therefore be seismically assessed to ensure that they can operate as required by the safety case.
- 5.57 EPGs supporting structures should withstand the design basis earthquake and limit movement between the components of the emergency generator (eg drive couplings and fuel lines) so that its functionality is not affected.

Flooding

- 5.58 EPGs should be located above the level of the design basis flood. Where this is not practicable, permanent external barriers such as levees, sea walls and bulkheads should be provided.

- 5.59 For existing facilities, where the above provisions are not practicable, suitable and sufficient permanent or temporary protection systems may be considered. These may take the form of 'drop-in' entrance barriers, drains, sumps and pumps. The installation of electrical switchboards and equipment should be arranged to avoid the adverse effects of flooding. ONR inspectors should confirm the adequacy of the licensees' arrangements for ensuring that the temporary measures can be deployed in sufficient time to avoid flood water entering the EPG facility. There should be a minimum number of trained staff available on site to achieve the timescale stated in the safety case with evidence of satisfactory deployment trials being undertaken on a regular basis.
- 5.60 A programme of EIM&T should be in place to ensure that the temporary flood protection equipment is stored securely in a protected location, is in a satisfactory condition and in working order.
- 5.61 EPGs should be a suitable distance above outside ground level, wherever practical, this will also serve to protect them against rainwater ingress. External storm drains should be sized to cope with the design basis rainfalls.

Internal Hazards

- 5.62 EPGs facilities should be protected (eg by location or physical barriers) from other plant, equipment and materials that might generate a hazard (eg fire or projectiles).

Fire

- 5.63 Suitable and sufficient fire protection shall be provided within the facility. Specialist advice should be sought from an Internal Hazards or Fire Inspector, as this may exceed normal fire detection and protection measures. Fuel and lubrication leaks should be minimised by adequate EIM&T. Good housekeeping provisions should be in place to ensure that leaks are detected and dealt with to prevent them accumulating in unacceptable quantities.

Lifting equipment

- 5.64 It is expected that permanently installed cranes and hoists will be required to support maintenance activities. Lifting equipment should be positioned and/or restrained such that it cannot impact on 'in service' EPGs.

Commissioning

- 5.65 Setting to work and commissioning trials of EPGs should demonstrate adequate confidence that the emergency generators and their ancillary equipment can meet the declared safety function including the load to be met for the mission time specified in the safety case. SAP ECM.1 (Commissioning).
- 5.66 In addition to individually testing the sub-systems and elements. The test plan should include a full system test. One advantage of such a test is to exercise common equipment (eg fuel supply, oil supply, cooling systems, control cabinets and battery systems) to reveal any weaknesses in their ability to meet all demands placed on them for a sustained period.

Examination, inspection, maintenance and testing (EIM&T)

- 5.67 One of the essential precursors in the formation of a suitable and sufficient EIM&T regime is the safety classification of the particular structures, systems and components (SSC) on the basis of their safety significance, as determined by the fault analysis of the facility. It is important that all EPG SSCs are designed, manufactured, installed,

commissioned, operated and maintained to a level of quality commensurate with their safety classification. ONR SAPs ECS.1 to ECS.5 (Safety classification and standards).

- 5.68 The safety management arrangements will often divide the EPGS into discrete sub-systems and the EIM&T on each sub-system undertaken to optimise the overall performance.
- 5.69 The licensee should be able to demonstrate confidence that the EPGSs can meet the declared reliability and safety function including the load to be met for the mission time specified in the safety case. SAP EMT.6 (Reliability claims).
- 5.70 EPGSs should be capable of delivering their design intent at all times. This requires an effective EIM&T programme. EPGS reliability should be demonstrated by appropriate testing and the availability of EPGSs for operation established by a suitable monitoring regime.
- 5.71 The adequacy of EPGS availability might be affected by EIM&T requirements. The inspector should establish that the licensee's operating rules and operating instructions specify suitable and sufficient levels of EPGS redundancy, diversity and segregation for safe reactor operation. The actions to be taken (eg safe plant/reactor shutdown) in response to partial or total loss of EPGS availability should be clearly stated.
- 5.72 Electrical generators are specialist equipment and it is therefore expected that licensees will have significant reliance on original equipment manufacturers (OEM) for EIM&T, technical support and advice. For example, routine EIM&T activities may be undertaken by the licensee's maintenance personnel but major overhauls and breakdowns are often carried out by OEM service organisations. ONR inspectors should seek evidence that all EIM&T is carried out by suitably qualified and experienced personnel (SQEP).
- 5.73 Electrical generators require regular preventative maintenance and testing. EPGS run testing provides assurance that the generator is in satisfactory working order and likely to start and run on demand. The run test, carried out in an appropriate manner, might also serve as a maintenance function, eg delivery of lubrication fluids to dry components. The run test should be carried out at prescribed intervals in accordance with plant maintenance schedule. It should be expected that this is undertaken in consultation with the OEM, eg to take benefit from their operating experience feedback. SAP EMT.7 (Functional testing).

Testing

- 5.74 There have been a number of reports [8], which present an analysis of failures of emergency DGs which can also apply to GTGs. The reports give a breakdown of failures within the sample. The top five categories are identified as:

Failure to start	Failure to run
<ul style="list-style-type: none"> • control and instrumentation system • starting sub-system • electrical generator • diesel engine • lubrication oil 	<ul style="list-style-type: none"> • engine • cooling system • fuel oil • generator • control and instrumentation system

Table 2 – EPGS failures

- 5.75 It was identified that approximately two-thirds of failures were found through testing which indicates the importance of suitable and sufficient programme of testing. The failure analysis reports describe the failures. One representative example is as follows:
- “Both emergency DGs failed to continue running 22 hours into 24 hour test due to a short on voltage suppression devices due to inadequate cooling in the excitation cabinet.”*
- 5.76 This implies a successful test would have been achieved by both generators running for 24 hours. This was a CCF because the generation excitation equipment shared an inadequately cooled cubicle. The failure may not have been discovered if the DGs were tested one at a time.
- 5.77 It is expected that regular testing of the EPGS is undertaken to demonstrate the availability reliability and capability in accordance with the safety case requirements. SAP EMT.7 (Functional testing).
- 5.78 Tests should be full system tests, so far as is reasonably practicable. By this, the tests should consider the complete system from engine to loads to reduce the risk that sub-systems of EPGS are overlooked. Such tests should be undertaken in islanded mode (i.e. disconnected from the normal grid supply) to demonstrate the required speed and voltage control of the EPGS as well as, where applicable, load shedding and sequencer systems.
- 5.79 Where full system tests are not practical, or where appropriate in between full system tests, testing of sub-systems should be undertaken. Such testing may be required to demonstrate the capability of those systems in response to specific events. Examples, of this could include demonstrating manual operation of the EPGS, or demonstrating the full power rating of the EPGS, which may only be possible in normal conditions through parallel operation with the offsite power supply or operation with a load bank. It is expected that licensees can demonstrate that such testing regimes encompass all required conditions of the safety case and do not exclude any required sub-systems. SAP EMT.6 (Reliability claims).
- 5.80 The licensee should demonstrate that it has adequately considered a range of factors and evaluated the impact of alternative options to arrive at a reasonably practicable testing regime.

- 5.81 Maintenance induced defects are a common failure mechanism and, where maintenance of similar equipment is undertaken in short succession, it can lead to common cause failure of redundant and diverse equipment. It is expected that testing should be undertaken following completion of maintenance activities to demonstrate that the equipment is capable of delivering its safety case requirements. The licensee's EIM&T programme should also ensure that the fuel is stored safely and securely and is maintained in a satisfactory condition for reliable operation.
- 5.82 To demonstrate the integrity of the fuel-oil system it should be periodically tested and undergo condition monitoring. This should be defined by the plant maintenance schedule and followed by a visual examination for evidence of component leakages, structural distress or corrosion. SAP EMT.5 (Procedures).

Spares

- 5.83 The management of spares holding is an important area that can impact on the safety case claims. The expectation is that the licensee should have determined its spares policy and holdings of critical spares based on factors including obsolescence, failure rates, required repair time, lead time for obtaining spares and support from equipment manufacturers. SAP EAD.5 (Obsolescence).

Equipment outages

- 5.84 At all times there should be sufficient EPGSs available to deliver the emergency power requirement. These should be defined by the safety case (eg Operating Rules and Instructions) to limit the effect of plant unavailability on the system contribution to the risk.
- 5.85 The impact of the anticipated maintenance, test and repair work on the reliability of EPGSs should be considered. If the resultant reliability or availability to perform a safety function is such that the EPGS no longer meets the criteria used for design and operation, the nuclear plant it serves should be placed in a safe state and the EPGS temporarily out of service should be substituted or restored within a specified time.

Fuel management

- 5.86 The nuclear safety case for the facility should state the mission time that the EPGSs will be required to provide electrical power to the specific nuclear safety systems following LOOP event(s). The minimum quantity of fuel stocks required to achieve this mission time should be stated in the relevant operating rules and operating instructions for the licensed site. The licensees' operational records should be reviewed to confirm that minimum stock levels are maintained. SAP FA.8 (Linking of initiating faults, fault sequences and safety measures).
- 5.87 Minimum fuel stocks should be stated in the safety case and be sufficient to allow for periodic maintenance/test running of the EPGSs. The licensee should have an effective system in place to ensure that the fuel tanks are replenished in a timely manner to maintain minimum stock levels.

Fuel specification and quality

- 5.88 Licensees should specify the fuel quality required by its EPGSs and have sufficient and suitable controls in place to ensure that the fuel received from its suppliers is to the correct standard.
- 5.89 Within the EU, diesel for road use allows up to 5% biodiesel content (B5), a proportion which is set to rise to 7% (B7). Eventually, biodiesel might be introduced for all

applications. It is therefore possible that biodiesel might inadvertently or otherwise enter EPG diesel systems.

- 5.90 Biodiesel in fuel oil could adversely impact diesel engine performance. ONR inspectors should secure assurances from licensees that they are aware of the potential problems associated with biodiesel and that they are taking appropriate action. Further information and guidance on the use of biodiesel is provided in Appendix 2 of this TAG.
- 5.91 Licensees should have a programme in place to ensure the initial and continuing quality of the fuel oil by regular sampling and, if appropriate, physical property testing.
- 5.92 The physical location of the fuel storage tanks, relative to the EPG is normally determined by the DG or GTG manufacturer. Consideration should be given to alternative fuel tank positions that offer greater resilience to fault conditions without affecting the primary safety function to provide back-up electrical power.
- 5.93 The tanks should be protected against external and internal corrosion. Tanks should be checked for water content and any accumulated condensate removed on a regular basis.
- 5.94 Periodically, the fuel stored in the supply tanks should be removed and any accumulated sediment removed. The tanks should be cleaned using a system that does not affect the fuel quality. For example, cleaning fluids should not introduce surfactants into the fuel system.
- 5.95 Cleaning may coincide with pressure testing and visual examination of the tanks for evidence of component leakages, structural distress or corrosion.
- 5.96 Fuel quality is affected by temperature. At low temperature, wax comes out of solution in diesel fuel and it becomes gel-like. If this happens, the diesel will not readily flow through valves and other devices. Temperatures should be controlled to ensure that the EPG fuel is maintained in a satisfactory condition at all times.

Asset management

- 5.97 SSCs within nuclear power plants experience both physical ageing (which results in degradation), and obsolescence (becoming out of date in comparison with current knowledge, standards and technology). The asset management TAG [3] includes guidance on ageing management and obsolescence.
- 5.98 The operating life of a nuclear facility may exceed the normal life expectancy of an EPGS or the time period that an OEM is willing to provide technical support and replacement parts. The licensee should have an appropriate strategy in place to manage ageing and obsolescence. This may involve wholesale replacement of one or more of the site's EPG systems. The ability to replace an EPGS without affecting delivery of the EPG nuclear safety function should be catered for. SAP EAD.5 (Obsolescence).
- 5.99 IAEA Safety Guide on Ageing Management for Nuclear Power Plants [5] provides recommendations for managing ageing of SSCs important to safety in nuclear power plants, including recommendations on key elements of effective ageing management.

REFERENCES

- 1 Licence condition handbook. Office for Nuclear Regulation. February 2017.. <http://www.onr.org.uk/documents/licence-condition-handbook.pdf>

- 2 Safety Assessment Principles for Nuclear Facilities. 2014 Edition Revision 0. November 2014. <http://www.onr.org.uk/saps/index.htm>
- 3 ONR Technical Assessment Guides:
 - External Hazards, NS-TAST-GD-013, Revision 6. ONR. December 2017.
 - Essential Services, NS-TAST-GD-019, Revision 3. ONR. July 2016
 - Redundancy Diversity Redundancy Segregation and Layout of Mechanical Plant, NS-TAST-GD-036, Revision 4. ONR. April 2017.
 - Computer Based Safety Systems, NS-TAST-GD-046, Revision 4. ONR. February 2017.
 - Asset Management, NS-TAST-GD-098, Revision 0. ONR. October 2016

http://www.onr.org.uk/operational/tech_asst_guides/index.htm
- 4 Western European Nuclear Regulators' Association. Reactor Harmonization Group. WENRA Reactor Reference Safety Levels. WENRA. September 2014. www.wenra.org.
- 5 IAEA Safety Standards
 - Design of Electrical Power Systems for Nuclear Power Plants. Specific Safety Guide. SSG-34
 - Safety of Nuclear Power Plants: Design. Specific Safety Requirements. SSR-2/1
 - Ageing Management for Nuclear Power Plants, Safety Guide. NS-G-2.12
- 6 Biodiesel in Fuel Oil for Diesel Engines. OPEX Advice Note 002/09. ONR. (CM9 Ref: 2009/200644)
- 7 Lessons Learned from the Nuclear Accident at the Fukushima Daiichi Nuclear Power Station. INPO 11-005 Addendum, Revision 0. Institute of Nuclear Power Operations (INPO). August 2012
<http://www.wano.info/Documents/Lessons%20Learned.pdf>
- 8 ONR207 – National and International Good Practices for Diesel Generators. Amec Foster Wheeler. April 2016 (CM9 Ref: 2016/144561)
- 9 IEC 61508 – Functional safety of electrical/electronic/programmable electronic safety-related systems
- 10 IEC 62671 – Nuclear power plants – Instrumentation and control important to safety – Selection and use of industrial digital devices of limited functionality

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

6. GLOSSARY AND ABBREVIATIONS (EXAMPLE LIST)

AC	Alternating current
ALARP	As low as reasonably practicable
C&I	Control and Instrumentation
CCF	Common Cause Failure
COTS	Commercial Off the Shelf [equipment]
DG	Diesel Generator
EA	Environment Agency Scottish Environment Protection Agency (SEPA)
EIM&T	Examination Inspection Maintenance and Testing
EPG	Emergency Power Generator
EPGS	Emergency Power Generation System
EU	European Union
GTG	Gas Turbine Generator
HSWA	The Health and Safety at Work Act 1974
HVAC	Heating Ventilation and Air Conditioning
IAEA	International Atomic Energy Agency
ICBM	Independent Confidence Building Measures
LC	Licence Condition
LOOP	Loss of Off-site Power
OEM	Original Equipment Manufacturer
ONR	Office for Nuclear Regulation
OPEX	Operating Experience
NNP	Nuclear Power Plant
SAPs	Safety Assessment Principles
SEPA	Scottish Environment Protection Agency
SSC(s)	Structures, Systems and Components
TAG	Technical Assessment Guide
TIG	Technical Inspection Guide
WENRA	Western European Nuclear Regulators' Association

7. APPENDICES

APPENDIX 1:

Guidance for undertaking mechanical engineering inspections of EPGs

- A1.1 EPGs are specialist COTS equipment. ONR inspectors should therefore not attempt to influence the established principles of the OEM design or how the EPG is intended to function. The focus for the mechanical engineering assessment of EPG systems is most likely to be the suitability of the EPG system layout and the adequacy of the EIM&T provisions to ensure reliable operation on demand.
- A1.2 International operating learning data identifies nine common reasons for EPG failure, seven of which are judged to be the result of inadequate EIM&T. The mechanical engineering related issues are as follows:

Issue	Design	Site Inspection
Low coolant level	EPG coolant systems should be provided with a means of inspecting the coolant levels to ensure that they are within the acceptable range specified by the OEM.	Evidence of regular inspection of the coolant levels should be recorded in the maintenance logs, together with any actions taken by the licensee to address low coolant levels.
Leaks (fuel, oil or coolant)	Diesel injection systems* operated at high pressure. A leak not attended to can result in a significant fuel loss affecting mission time and increase the risk of fire. Consideration should be given to providing a means of early detection of leaks. <i>* Warning: Inspectors should be aware that high pressure diesel systems present a serious conventional health risk. Fine high velocity sprays can pass through the skin into body tissue.</i>	Inspectors should check for evidence that the licensee is adequately managing leaks. This should be visible to the naked eye, eg staining of paintwork and condition of sumps and drip trays.
Air in the fuel system	Fuel systems should be provided with means of bleeding air from the fuel lines.	Air in the fuel system is most likely to occur following a maintenance and breakdown activity. Maintenance instructions and records should be examined to ensure that measures are in place and being implemented to ensure that air is removed from the system.
Ran out of fuel	Maintenance running of an EPG will reduce the amount of fuel remaining in the fuel tank. Tanks should be sized to provide sufficient fuel to achieve the mission time specified in the safety case.	Fuel tank levels should be inspected. Refuelling logs should confirm that fuel levels are maintained above the minimum specified level at all times. Instructions should identify at tank level refuelling requirements, to ensure sufficient reserves between reordering and refuelling, allowing for maintenance running.

Issue	Design	Site Inspection
High fuel level	An alarm should be provided to warn of overfilling. There should be a means of removing excess fuel.	Overfilling of the fuel tanks may be detrimental to the reliable operation of the EPG, eg blocking of air filters on liquid fuel tanks may generate a vacuum as fuel levels drop. Refuelling logs should be inspected to ensure that refuelling is adequately controlled to ensure that tanks are not overfilled.
Controls not in auto	On completion of maintenance operations, EPGS controls should be reset to their normal (auto) state so that they will respond to any demand. Controls should be clear and unambiguous and positioned where they can be readily seen.	Inspectors should ensure that this is identified in the maintenance instructions and recorded as completed in the relevant logs. Regular checks should also be carried out, to an appropriate timescale, to ensure that controls are always in the “auto” position during normal plant operation states.
Ancillary equipment	Inspectors should review the design of ancillary systems to ensure they cannot compromise the reliability of the principal EPG systems, for example: <ul style="list-style-type: none"> • heating, ventilation and air conditioning (HVAC) system should ensure that suitable environmental conditions are maintained throughout the extreme weather events identified by the safety case. • a means of detecting leaks and build-up of liquids in drainage systems should be provided • ancillary systems should be positioned and/or protected to ensure that they cannot present a threat to the principal EPG system. 	Inspectors should review the ancillary equipment to confirm that it is being maintained in a satisfactory condition and does not present a potential threat to the principal EPG system, for example: <ul style="list-style-type: none"> • a faulty heating system may result in “clouding” of diesel fuel when external temperatures are very cold • a significant quantity of diesel in a drainage system may present a fire risk • a poorly secured item of equipment may become a projectile during a seismic event.

Table 3 – Common mechanical failures

EIM&T

A1.3 The licensee's maintenance procedures should be inspected to ensure that relevant good practice is adhered to and equipment is maintained in accordance with the OEM's recommendations. Typical examples are as follows:

- Maintenance, periodic inspections and testing should be in accordance with the OEM's instructions subject to oversight from the licensee as intelligent customer.
- Adequate lubrication should be established before all planned starts (N.B. including maintenance running). For DGs, this would typically involve starting the engine at low speed and running for a set period to deliver lubrication to all DG components. Running speed and load should be increased and decreased gradually.
- Bearing inspections should be carried out at suitable intervals.
- Regular oil sampling and analysis, eg for metal content and degradation
- Regular replacement of oil and air filters and inspection of oil strainers. This provides an opportunity for analysis of the oil filter media and any deposits found.
- Verification of fuel to ensure continued acceptability for emergency use, including low temperature suitability, i.e. the abnormal low temperature conditions stated in the nuclear safety case.
- Effects of ageing, eg degradation of rubber components.
- Appropriate use of condition monitoring and trending to identify adverse or deteriorating performance across all EPGSSs.
- Evidence of learning from internal and external operating experience to improve maintenance regime and practices.
- Good housekeeping practices, eg exclusion of foreign materials and contaminants.

A1.4 Inspectors should be aware that severe ageing can result from factors such as starting too often, sustained low or high engine loading and rapid engine loading.

APPENDIX 2:

Guidance on the use of biodiesel

- A2.1 There are a number of issues related to the use of biodiesel [6]. Licensees should be aware of these issues and have appropriate measures in place to address them. For example, Emergency DG manufacturers do not recommend the use of biodiesel for nuclear power plant (NPP) standby application.
- A2.2 Biodiesel fuels contain less energy than petroleum derived diesel. This will affect the minimum fuel stock levels required by the safety case, operating rules and operating instructions. Additional storage capacity may be required.
- A2.3 Biodiesel can have a cleaning effect that loosens accumulated sediment in fuel oil storage tanks. This sediment can then plug filters and other devices in the DG system thereby reducing reliability.
- A2.4 Biodiesel fuel has an affinity to absorb moisture and promote bacteria growth.
- A2.5 Biodiesel is biodegradable, and the presence of water, heat, oxygen, and other impurities accelerate degradation. Biodiesel might compromise DG reliability if it has been stored for an extended period of time.
- A2.6 EDGs may be preheated for standby mode applications. With biodiesel heating the fuel increases the risk of clogging of parts, injectors and filters.
- A2.7 Biodiesel contains suspended particles of water from the manufacturing process. Over time, this water will fall out of suspension and form “dirty water” in the fuel oil storage tank, which eventually leads to the formation and growth of algae.
- A2.8 Biodiesel has different chemical characteristics from diesel and can interact with materials in a different way. It can corrode and tribologically attack metallic components and degrade elastomer parts. DG components may need to be replaced.
- A2.9 Brass, bronze, copper, lead, tin, and zinc in tanks and fittings can accelerate the oxidation process of biodiesel, creating solids, gels and salts.
- A2.10 Biodiesels have higher cloud points (the temperature at which solid particles start to form, or gel) than conventional diesel. Clouding may also combine with suspended particles of water to prevent engine starting in cold temperature conditions.
- A2.11 Biodiesel is a solvent and might damage paint (eg internal finishes of storage tanks).