Radioactive Waste Management

NDA Report no. DSSC/431/01

Geological Disposal

Safety Case Production and Management

December 2016

Radioactive Waste Management

NDA Report no. DSSC/431/01

Geological Disposal

Safety Case Production and Management

December 2016

Conditions of Publication

ISBN 978-1-84029-562-7.

Other Publications

If you would like to see other reports available from RWM, a complete listing can be viewed at our website https://rwm.nda.gov.uk, or please write to us at the address below.

Feedback

Readers are invited to provide feedback on this report and on the means of improving the range of reports published. Feedback should be addressed to:

RWM Feedback
Radioactive Waste Management Limited
Building 587
Curie Avenue
Harwell Campus
Didcot
OX11 0RH
UK

email: rwmfeedback@nda.gov.uk

Preface

Radioactive Waste Management Limited (RWM) has been established as the delivery organisation responsible for the implementation of a safe, sustainable and publicly acceptable programme for the geological disposal of the higher activity radioactive wastes in the UK. As a pioneer of nuclear technology, the UK has accumulated a legacy of higher activity wastes and material from electricity generation, defence activities and other industrial, medical and research activities. Most of this radioactive waste has already arisen and is being stored on an interim basis at nuclear sites across the UK. More will arise in the future from the continued operation and decommissioning of existing facilities and the operation and subsequent decommissioning of future nuclear power stations.

Geological disposal is the UK Government's policy for higher activity radioactive wastes. The principle of geological disposal is to isolate these wastes deep underground inside a suitable rock formation, to ensure that no harmful quantities of radioactivity will reach the surface environment. To achieve this, the wastes will be placed in an engineered underground facility – a geological disposal facility (GDF). The facility design will be based on a multi-barrier concept where natural and man-made barriers work together to isolate and contain the radioactive wastes.

To identify potentially suitable sites where a GDF could be located, the Government has developed a voluntarist approach, based on working with interested communities that are willing to participate in the siting process. The siting process is on-going and no site has yet been identified for a GDF.

Prior to site identification, RWM is undertaking preparatory studies which consider a number of generic geological host environments and a range of illustrative disposal concepts. As part of this work, RWM maintains a generic Disposal System Safety Case (DSSC). The generic DSSC is an integrated suite of documents which together give confidence that geological disposal can be implemented safely in the UK.

Executive Summary

Radioactive Waste Management Limited (RWM) has been charged with implementing the UK Government's policy for the long-term management of higher activity waste by planning, building and operating a geological disposal facility. The UK has accumulated a legacy of radioactive waste from electricity generation, defence activities and other industrial, medical, agricultural and research activities. Radioactive wastes continue to be produced from these activities and some of these wastes will remain hazardous for hundreds of thousands of years.

The generic Disposal System Safety Case (DSSC) considers the safety of radioactive waste transport, the safety of the construction and operation of the geological disposal facility (GDF) and the safety of the facility in the very long term, after it has been sealed and closed. The DSSC is in the early stages of development, because the site and design have not yet been chosen. As such, it is referred to as a 'generic' safety case and the strategy to demonstrate safety is also termed 'generic' because it must cover a range of possible disposal environments and facility designs. Nevertheless, this work builds on more than 30 years of experience studying geological disposal and undertaking safety assessments in the UK. It also draws on the extensive body of knowledge and experience in other countries gained through overseas radioactive waste management programmes.

The three primary elements of the geological disposal facility system covered by the generic DSSC are as follows:

- transport of the radioactive wastes to the disposal facility
- waste emplacement operations including backfilling
- post closure evolution of the GDF

The generic DSSC presents the available evidence that each of these aspects of the disposal system will be capable of implementation with levels of safety and environmental protection compliant with regulatory requirements and modern standards of good practice. It consists of an Overview describing the safety of a GDF and three main documents, one for each of the three components of the overall safety argument – the generic Transport Safety Case, the generic Operational Safety Case and the generic Environmental Safety Case.

The purpose of the Safety Case Production and Management report is to describe the management arrangements, requirements, expectations and constraints, safety principles and procedures and the methodologies used for the development of the generic DSSC. The aim is to provide confidence that the safety cases for the eventual transport, operation and post closure (long-term environmental safety) can be developed to support GDF activities and that this safety case is suitable and appropriate for an early illustrative stage in the development of the disposal system concept.

The generic DSSC includes all the evidence relating to the overall safety and environmental implications of a GDF. In due course, individual, specifically tailored regulatory submissions for the GDF will be generated. This current safety case has been produced prior to any knowledge of the locations or geological environment of potential GDF sites and therefore remains generic until such time as potential sites have been identified.

This report describes RWM's understanding of the principal requirements for safety cases relevant to a licensed nuclear site, for safety reports that justify the safety of radioactive waste transport packages and safety cases to justify the long-term environmental safety of the GDF post closure. It describes the legislation that is applicable to safety cases and the regulatory expectations and guidance for the content and scope of safety cases. It also

describes how RWM has developed, and is intending to develop further, the safety principles that underpin the criteria that the design will have to meet and gives guidance on the methodologies used to produce the safety cases that justify the safety of the design through the safety case manuals. In addition, the report describes how RWM will manage the design and safety case processes as a competent organisation through managing the supply chain, meeting the requirements of being a design authority and an intelligent customer for the GDF. This will be a necessary demonstration as part of RWM's future application to be licensed as a site licence company under the Nuclear Installations Act 1965.

In order to develop the GDF, it will be necessary to develop a staged series of safety cases to demonstrate to the regulators that the project can proceed safely through the siting process, surface investigation, underground investigation, construction, commissioning, operational (waste emplacement), decommissioning and closure phases. This report describes how the various safety documents have been managed, and how RWM expects to manage this documentation as the project progresses and safety cases are produced to support the future construction and operation of the GDF.

List of Contents

1 Introduction

1.1 The generic Disposal System Safety Case

RWM has been established as the delivery organisation responsible for the implementation of a safe, sustainable and publicly acceptable programme for geological disposal of the UK's higher activity waste. Information on the UK Government and devolved administrations'[1] approach to implementing geological disposal, and RWM's role in the process, is included in an overview of the generic Disposal System Safety Case (the Overview) [1].

The geological disposal facility (GDF) will be a highly-engineered facility, located deep underground, where the waste will be isolated within a multi-barrier system of engineered and natural barriers designed to prevent the release of harmful quantities of radioactivity and non-radioactive contaminants to the surface environment. To identify potentially suitable sites where the GDF could be located, the Government is developing a voluntarism approach based on working with interested communities that are willing to participate in the siting process [2]. Development of the siting process is ongoing and no site has yet been identified for the GDF.

In order to progress the programme for geological disposal while potential disposal sites are being sought, RWM has developed illustrative disposal concepts for three types of host rock. These host rocks are typical of those being considered in other countries, and have been chosen because they represent the range that may need to be addressed when developing a GDF in the UK. The host rocks considered are:

- higher strength rock, for example, granite
- lower strength sedimentary rock, for example, clay
- evaporite rock, for example, halite

The inventory for disposal in the GDF is defined in the Government White Paper on implementing geological disposal [2]. The inventory includes the higher activity wastes and nuclear materials that could, potentially, be declared as wastes in the future. For the purposes of developing disposal concepts, these wastes have been grouped as follows:

- High heat generating wastes (HHGW): that is, spent fuel from existing and future power stations and High Level Waste (HLW) from spent fuel reprocessing. High fissile activity wastes, that is, plutonium (Pu) and highly enriched uranium (HEU), are also included in this group. These have similar disposal requirements, even though they don't generate significant amounts of heat.
- Low heat generating wastes (LHGW): that is, Intermediate Level Waste (ILW) arising from the operation and decommissioning of reactors and other nuclear facilities, together with a small amount of Low Level Waste (LLW) unsuitable for near surface disposal, and stocks of depleted, natural and low-enriched uranium (DNLEU).

RWM has developed six illustrative disposal concepts, comprising separate concepts for HHGW and LHGW for each of the three host rock types. Designs and safety assessments for the GDF are based on these illustrative disposal concepts.

---

[1] UK Government in this context means the Department for Energy and Climate Change (DECC). The devolved administrations are the Welsh Assembly Government and the Department of the Environment Northern Ireland. Scottish Government policy is that the long term management of higher activity waste should be in near-surface facilities and that these should be located as near as possible to the site where the waste is produced.

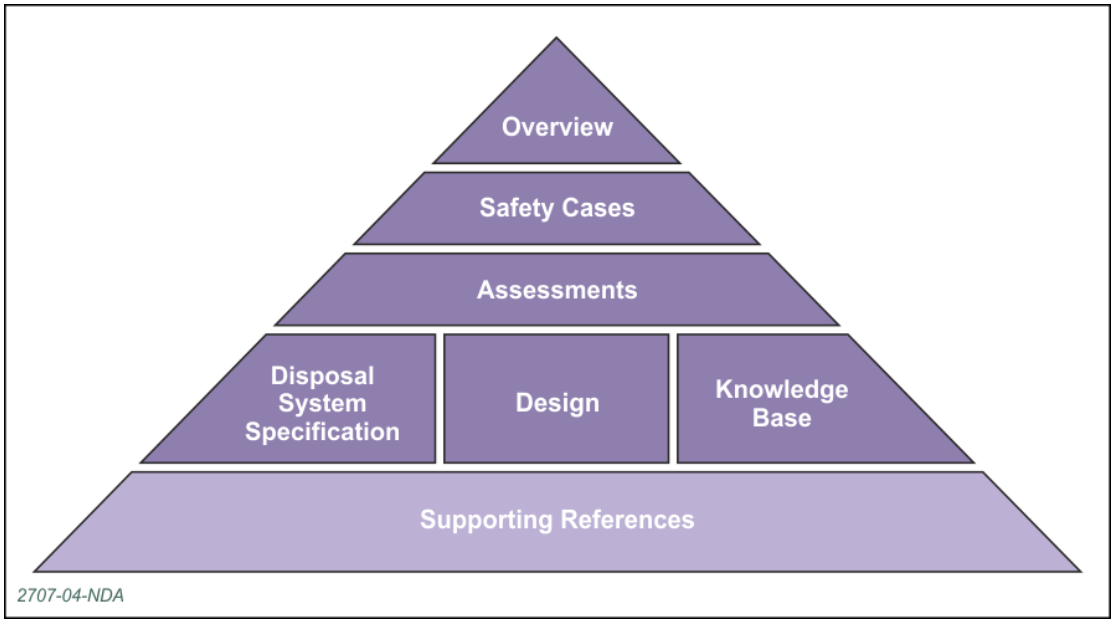
High level information on the inventory for disposal, the illustrative disposal concepts and other aspects of the disposal system is collated in a technical background document (the Technical Background) [3] that supports this generic Disposal System Safety Case.

The generic Disposal System Safety Case (DSSC) plays a key role in the iterative development of a geological disposal system. This iterative development process starts with the identification of the requirements for the disposal system, from which a disposal system specification is developed. Designs, based on the illustrative disposal concepts, are developed to meet these requirements, which are then assessed for safety and environmental impacts. An ongoing programme of research and development informs these activities. Conclusions from the safety and environmental assessments identify where further research is needed, and these advances in understanding feed back into the disposal system specification and facility designs.

The generic DSSC provides a demonstration that geological disposal can be implemented safely. The generic DSSC also forms a benchmark against which RWM provides advice to waste producers on the packaging of wastes for disposal.

Document types that make up the generic DSSC are shown in Figure 1. The Overview provides a point of entry to the suite of DSSC documents and presents an overview of the safety arguments that support geological disposal. The safety cases present the safety arguments for the transportation of radioactive wastes to the GDF, for the operation of the facility, and for long-term safety following facility closure. The assessments support the safety cases and also address non-radiological, health and socio-economic considerations. The disposal system specification, design and knowledge base provide the basis for these assessments. Underpinning these documents is an extensive set of supporting references. A full list of the documents that make up the generic DSSC, together with details of the flow of information between them, is given in the Overview.

Figure 1 Structure of the generic DSSC



1.2 Introduction to the Safety Case Production and Management report

The generic DSSC was previously published in 2010. There are now a number of drivers for updating the safety case as an entire suite of documents, most notably the availability of an updated inventory for disposal.

This document is the Safety Case Production and Management report. This document updates and replaces the 2010 Safety Case Production and Management report published as part of the 2010 generic DSSC suite.

The report is intended to demonstrate that:

- the generic DSSC is soundly constructed by an auditable process and thus gives a reliable indication of the safety of the GDF and of transport operations
- there is a clear understanding of what needs to be done to put in place the infrastructure necessary for the production of future safety cases that meet current standards

The Safety Case Production and Management report presents much of the information that is (or will be) documented in the RWM arrangements to meet legislative and regulatory obligations together with the manuals, including supporting procedures which make up the RWM Engineering Design Manual and the various safety case manuals. As many of these documents are now available within the RWM management system, the need for the Safety Case Production and Management report has been removed and, therefore, this is expected to be the final publication of this document.

1.3 Objective

The objective of the Safety Case Production and Management report is to provide an overview of the RWM approach and arrangements for the management and production of safety cases and explain how RWM has put these into practice in the production of the safety cases supporting the generic DSSC. The report therefore:

- explains the key elements of nuclear safety cases, with reference to supporting RWM safety case manuals
- describes the expectations for the management of safety and how RWM's management system meets these expectations both now and in the future
- describes how RWM will manage its safety case documentation
- explains the legislative requirements for safety cases and describes the regulatory guidance for safety cases and how this has been documented within the RWM management system
- describes RWM's safety principles and guidance and how these will be developed
- describes RWM's methodologies for producing the safety cases supporting the DSSC
- details the safety cases that are expected to be produced in the future to support the developing design, construction and operation of the GDF and how they will develop from the safety cases supporting the DSSC

1.4 Scope

The scope of this Safety Case Production and Management report is to describe the following and how they relate to the safety case production and management process:

- management arrangements
- safety case process
- regulatory constraints and expectations
- safety principles and criteria
- safety case and assessment methodologies

- documentation streams

The report covers transport of waste packages to the GDF, operation of the GDF, closure and post-closure for all types of waste being emplaced for each type of host rock considered.

1.5 Document structure

The remainder of this report is structured according to the following format:

- Section 2 provides an overview of the generic DSSC and the background to the 2016 update
- Section 3 discusses the regulatory context including the requirements for radioactive materials transport, construction safety, operational safety and post-closure environmental safety
- Section 4 sets out the key elements of safety case production and management including the legal and regulatory expectations, RWM's process and the approach for the management of the generic DSSC including the role as an intelligent customer
- Section 5 describes the safety case management process including RWM's future aims to become a nuclear site licence holder, the associated requirements for safety management including safety culture, RWM's safety management structure and the means by which configuration and change control are managed
- Section 6 describes the relevant safety principles, criteria and supporting methodologies including the role of the safety case manuals and interfaces with the Disposability Assessment process
- Section 7 sets out the future safety case documents for transport, operations and post-closure environmental safety
- Section 8 sets out the conclusions of this report

Common terms and acronyms used throughout the generic DSSC are defined in the glossary and acronym list in the Technical Background document.

2 Summary of the generic Disposal System Safety Case

The three primary elements of the GDF covered by the generic DSSC, which includes the safety cases that summarise the safety arguments for their respective aspects of the disposal system, are as follows:

- transport of the radioactive wastes to the GDF, as described in the generic Transport Safety Case (TSC)
- construction, commissioning, waste emplacement operations, backfilling and decommissioning (together defined as the operational phase), as described in the generic Operational Safety Case (OSC)
- post-closure evolution of the GDF, as described in the generic Environmental Safety Case (ESC)

The generic DSSC presents:

- the available evidence that each of these aspects of the disposal system can be implemented with levels of safety and environmental protection compliant with regulatory requirements and current standards of good practice
- the demonstration that it will be possible to develop a GDF that is safe both in the operational and post-closure period
- the demonstration that the transport of packages from the waste-producing sites to the GDF can be carried out safely

The development of the generic DSSC carries with it a number of assumptions including:

- knowledge of the wastes and their associated records to support disposal are adequate
- knowledge of the geological environment of the identified site can be determined with sufficient confidence to support post closure models
- adequate and appropriate post-closure radionuclide release and behaviour models are available/can be developed

The 2016 generic DSSC reflects a periodic update relative to the original 2010 version. The main drivers for the 2016 update of the DSSC were:

- a revised derived inventory based upon the 2013 UK radioactive waste inventory [4] including new waste package types such as the inclusion of robust shielded containers and 500 litre and 1 cubic metre concrete drums and the exclusion of the Scottish waste
- the development of the RWM design and safety processes including the production and issue of safety case manuals

The update is supported and informed by:

- the Engineering Design Manual (EDM) [5] and associated procedures
- the safety case manuals (integrated with the EDM) comprising:
  - the Transport Safety Manual (TSM) [6] for the TSC
  - the Nuclear Operational Safety Manual (NOSM) [7] for the OSC
  - the Environmental Safety Manual (ESM) [8] for the ESC
- revised policies and procedures governing the collection, use and management of models and data for the assessments

The 2010 version of the generic DSSC was prepared based on understanding and extant procedures formalised in RWM toolkits available at the time; since then, the safety case manuals have been developed and approved for use by RWM. These manuals specify the methodologies, approaches and specifications for safety case documents and their associated assessments which are based on current standards and regulatory expectations. As a result, the 2016 generic DSSC reflects the requirements detailed in the safety case manuals which necessitated some significant changes relative to the 2010 generic DSSC.

In addition, RWM aims to use the staged submission process in order to:

- build confidence in the safety cases with regulators and stakeholders
- maintain generic safety cases for illustrative designs whilst developing site-specific cases in parallel; this permits the generic safety cases to support disposability assessments until there is confidence in a given site being taken forward, whilst site-specific safety cases will inform the iterative development of the design of a potential site
- allow for the possibility of additional, alternative sites being put forward and for RWM to continue to undertake disposability assessments that encompass a broad range of potential disposal facility designs
- ensure continued maintenance of the generic safety cases as a living suite of documents under change control arrangements
- facilitate iterative development of the site-specific safety case based on the iterative development of a geological disposal system

Once a preferred site is identified, disposal concepts will be developed for that site, on which preliminary and preferred designs will be developed. The site-specific safety cases will iteratively assess the transport, operational and environmental safety of those designs as they evolve.

3 Regulatory Context

The regulation of activities associated with the GDF will be subject to a range of legislation addressing the transport, operation and post-closure environmental aspects. This section sets out the UK regulatory requirements in relation to transport, operation and post-closure environmental safety.

The requirement to produce safety cases for nuclear facilities and the disposal of radioactive waste arises directly or indirectly from several UK legislation sources. These are:

- the Health and Safety at Work Act (HSAWA) 1974
- the Nuclear Installations Act (NIA) 1965 (as amended)
- the Management of Health and Safety at Work Regulations (MHSWR) 1999 (SI 1999/1877)
- the Ionising Radiations Regulations (IRR) 1999 (SI 1999/3232)
- the Energy Act 2013 (SI 2013/190)
- the Carriage of Dangerous Goods and Use of Transportable Pressure Equipment Regulations (CDG) 2009 (SI 2009/1348), as amended
- the Environmental Permitting Regulations (EPR) 2010 (SI 2010/675)

3.1 Radioactive materials transport

The transport of radioactive waste from the waste producing sites to the GDF, which includes intermodal transfer (transhipment), is subject to UK legislation implementing the requirements set out by the International Atomic Energy Agency (IAEA) Transport Regulations [9] which provides the international regulatory framework for all transport activities involving radioactive materials, including waste. The IAEA Transport Regulations establish standards of safety which provide an acceptable level of control of the radiation, criticality and thermal hazards to persons, property and the environment associated with the transport of radioactive material. The safety protection is achieved by requiring:

- containment of the radioactive contents
- control of external dose equivalent rates
- prevention of criticality
- prevention of damage caused by heat

These requirements are satisfied firstly by applying a graded approach to the application of contents limits for transport packages and conveyances and to performance standards applied to transport package designs depending upon the hazard of the radioactive contents. Secondly, they are satisfied by imposing conditions on the design and operation of transport packages and on the maintenance of transport packages, including consideration of the nature of the radioactive contents. Finally, they are satisfied by requiring administrative controls, including, where appropriate, approval by competent authorities.

The IAEA Transport Regulations are prescriptive and meet international requirements that enable transport of packages across international borders. The transportation of radioactive materials in the UK has to meet the requirements of the CDG 2009. These regulations implement provisions of European legislation on the carriage of dangerous goods and, in particular, the requirements contained in:

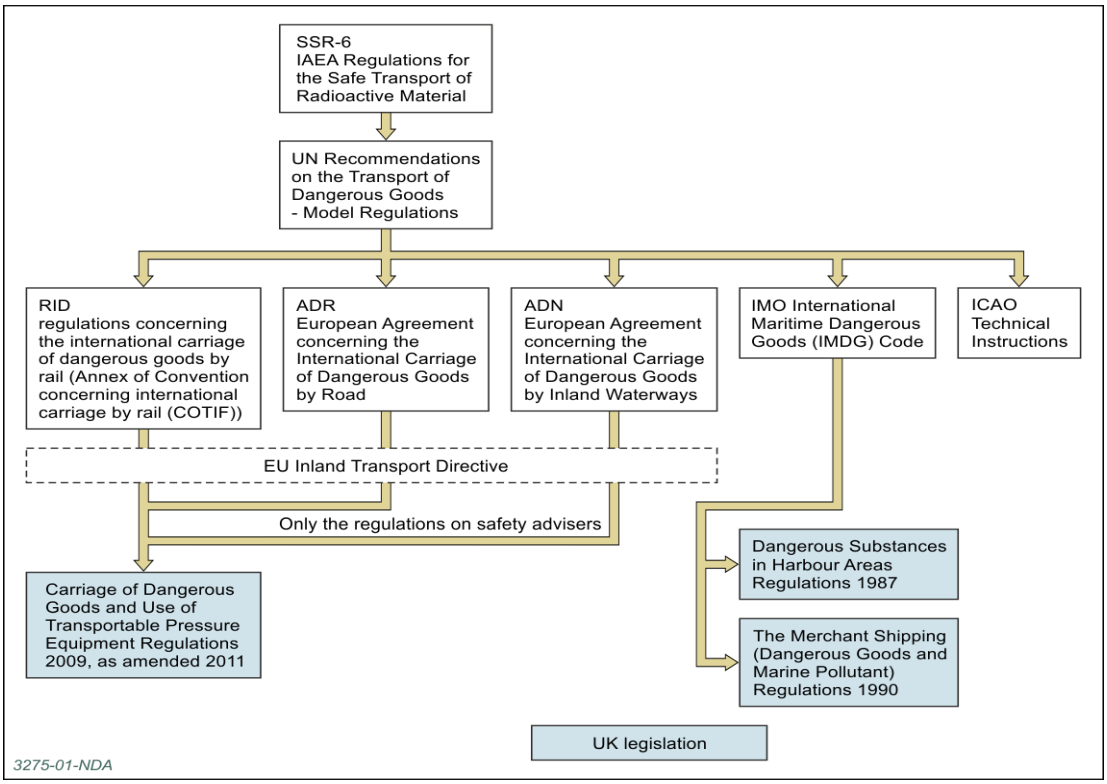
- the United Nations Economic Commission for Europe Agreement concerning the International Carriage of Dangerous Goods by Road (generally referred to as 'ADR')
- the Inter-Governmental Organisation for International Carriage by Rail Regulation concerning the International Carriage of Dangerous Goods by Rail (generally referred to as 'RID')
- the United Nations Economic Commission for Europe Agreement Concerning the International Carriage of Dangerous Goods by Inland Waterways (generally referred to as 'ADN')

The transportation of radioactive wastes and materials by sea has to meet the requirements of:

- the Merchant Shipping (Dangerous Goods and Marine Pollutants) Regulations 1997 (SI 1997/2367)
- the Dangerous Substances in Harbour Areas Regulations 1987 (SI 1987/37)

The international guidelines for the safe transportation or shipment of dangerous goods or hazardous materials by sea is provided by the International Maritime Dangerous Goods. The international agreements, the United Nations Economic Commission for Europe Agreement concerning the International Carriage of Dangerous Goods by Road, the Inter-Governmental Organisation for International Carriage by Rail Regulation concerning the International Carriage of Dangerous Goods by Rail, the United Nations Economic Commission for Europe Agreement Concerning the International Carriage of Dangerous Goods by Inland Waterways and the International Maritime Dangerous Goods, are based upon the Recommendations on the Transport of Dangerous Goods Model Regulations published by the United Nations, of which the requirements for the transport of radioactive material are based upon the IAEA Transport Regulations. The full structure of the regulations and legislation is shown in Figure 2.

Figure 2 Hierarchy of Regulations and Legislation for Transport of Radioactive Materials



Within the UK, the competent authority for the transport by road and rail of radioactive materials, including waste, is the Office for Nuclear Regulation (ONR). The ONR carries out a range of regulatory activities to assure the safe transport of radioactive materials. Approval is granted for the designs of transport packages used to carry high-hazard radioactive materials to ensure they meet exacting international safety standards, the packages are built to robust quality assurance plans and are correctly used and maintained.

However, since the primary requirements originate in the IAEA Transport Regulations, these will be referred to in this document (whilst acknowledging that they are enabled through UK legislation).

The IAEA's requirements are satisfied by the implementation of transport package inventory limits and design performance standards which ensure an appropriate level of safety against assumed radiological transport event models. These are supplemented by requirements on the operation and maintenance of the transport packages, as well as rigorous administrative controls and the making of arrangements for effective emergency response in the event of accidents.

Testing requirements for transport package designs are defined to reflect challenges to the package integrity from routine, normal (involving minor mishaps) and accident conditions. The robustness required, and hence the stringency of the test criteria, reflects the magnitude and nature of the inventory permitted in the particular transport package type. Routine criteria encompass ambient conditions whilst the normal conditions criteria encompass ambient physical conditions and minor mishaps such as impacts typical of normal handling, stacking and water spray. Criteria defined for accidents include impact, thermal challenge and water immersion criteria to a degree determined by transport package type.

The IAEA Transport Regulations define four main types of transport package:

- Industrial Packages (IP): packages are used to transport material comprising low specific activity or surface contaminated objects; IPs are defined at three levels (IP-1, IP-2 and IP-3) based on the allowed content.
- Type A: radiological material that is below a prescribed hazard threshold can be transported as a Type A package which is not accident resistant and may not withstand events beyond those anticipated during normal transport with the provisos:
    - the wastes that are to be transported to the GDF exceed the prescribed hazard thresholds
    - Type A packages are not part of the GDF disposal concept hence these cannot be accepted by the GDF and are not considered further
    - this will also be the case for any excepted packages
- Type B: packages intended for transport of high-hazard radiological materials, providing an appropriate level of containment in the event of specified events, such as an engulfing fire of a specified temperature and duration or impact of a specified severity with the following provisos:
    - the majority of the waste transported to the GDF is such that it will need to be transported as a Type B package and these materials include spent fuel, HLW and some ILW
    - Type B packages may either be unilaterally approved (B(U)), or multilaterally approved (B(M)), and there are specific additional requirements placed on fissile material or uranium hexafluoride
- Type C: these packages are used to transport certain radiological materials by air; air freight of material that would require transport as a Type C package does not comprise part of the GDF concept, hence cannot be accepted by the GDF and are not addressed further.

In the UK and elsewhere, it is accepted that compliance with the requirements of the IAEA Transport Regulations ensures acceptable levels of safety for transport of radioactive materials. Thus the primary approach to the demonstration of safety and justification of transport operations will be a deterministic demonstration that the packages used for transporting radioactive waste comply with these requirements. In addition, RWM ensures that any transport requirements applicable to waste packages are incorporated into the waste package specification and guidance material.

Compliance with the requirements of IAEA Transport Regulations is required for all packages used for the transport of radioactive materials. Given that the containers in which radioactive material is transported form the primary protective system for transport workers, members of the public and the environment, the IAEA Transport Regulations concentrate on the design and performance of the transport containers and these have to be formally substantiated. This demonstration takes the form of a Design Safety Report (DSR) for each transport package type which has to be approved by the competent authority prior to the package being employed for transport of radioactive materials. The DSR effectively provides the engineering design substantiation for the transport packages against IAEA Transport Regulations requirements. The competent authority will issue a package design approval certificate for the package when they are satisfied that the DSR meets the requirements of the IAEA Transport Regulations with the exception of IPs which are self-approved.

Prior to transporting waste, the organisation responsible for waste transport will prepare consignor shipping procedures which will comprise detailed procedures for ensuring that

the packages prepared for shipping meet the requirements of the package design approval certificate.

The IAEA Transport Regulations also require the production of a Radiation Protection Programme (RPP). The purpose a RPP is to establish and document, in a systematic and structured way, the framework of controls applied by a transport organisation (that is to say any organisation involved in transport, including the consignor, the carrier, the port operator and the consignee) to satisfy the radiation protection requirements and provisions established in the IAEA Transport Regulations namely to limit both normal and potential exposures of workers and members of the public and to provide adequate emergency planning arrangements.

In addition, it is a requirement of CDG 2009 that a written emergency plan should be in place prior to the shipment of any package containing radioactive material. This plan should set out the arrangements to cope with any radiological incident involving the package or packages.

The details of the plan are likely to depend on the nature of the shipment. However, it should be based on the general principle, as laid down in CDG 2009, that intervention should be undertaken only if the damage from the radiation is sufficient to justify the potential harm and cost of the intervention.

In addition, the IRR 1999 place limits and other requirements on radiation exposures, requiring, amongst other things, that exposures are restricted to be as low as reasonably practicable (ALARP). Under the HSAWA 1974, there are general duties on employers to ensure, so far as is reasonably practical, the health, safety and welfare of their employees and that persons not in their employment are not exposed to risks to their health or safety. These duties apply to both radiological and non-radiological risks. The MHSWR 1999 requires employers to make a *"suitable and sufficient assessment"* of the health and safety risks to employees and others potentially affected by their undertakings in order that appropriate control measures will be identified and put in place.

3.2 Construction

The safety of construction activities at the GDF will be subject to the legal framework of the HSAWA 1974 which places duties on all employers, including those in the nuclear industry, to look after the health and safety of both their employees and the public. In addition, the MHSWR 1999 requires employers to make a *"suitable and sufficient assessment"* of the health and safety risks to employees and others potentially affected by their undertakings in order that appropriate control measures will be identified and put in place.

Within the UK, the Construction (Design and Management) Regulations 2015 cover the management of health, safety and welfare when carrying out construction projects. These regulations will become applicable to RWM once the GDF enters the formal design process.

The key elements, include:

- managing the risks by applying the general principles of prevention to design, construction, maintenance and operational activities, namely:
    - avoiding risks where possible
    - evaluating those risks that cannot be avoided
    - putting in place proportionate measures that reduce them and/or control them at source

- appointing the right people and organisations at the right time such that anyone responsible for appointing designers (including principal designers) or contractors (including principal contractors) to work on a project must ensure that those appointed have the skills, knowledge and experience to carry out the work in a way that secures health and safety, including where appropriate, sufficient organisational capability
- appointment of duty-holders such as principal designers and principal contractors as soon as is practicable and before the start of the construction phase, so they have enough time to carry out their duties to plan and manage the pre-construction and construction phases respectively
- planning, managing and coordinating health and safety in the pre-construction and construction phases of a project so the risks involved are managed from start to finish
- making sure everyone has the information, instruction, training and supervision they need to carry out their jobs in a way that secures health and safety
- duty-holders cooperating and communicating with each other and coordinating their work to make sure everyone understands the risks and the measures to control those risks
- consulting the workforce and engaging with them to promote and develop effective measures to secure health, safety and welfare

3.3 Emplacement and operations

The legal framework for the operation of a nuclear site/facility is based around the HSAWA 1974, the Energy Act 2013 and the NIA 1965. The HSAWA places duties on all employers, including those in the nuclear industry, to look after the health and safety of both their employees and the public. However, because of the particular hazards associated with the nuclear industry, including the potential for accidents to cause widespread harm and social disruption, some legislation is targeted at the nuclear industry, specifically the NIA 1965. Additionally, there are nuclear regulations made under the Energy Act 2013 that are also relevant, as well as regulations under the HSAWA such as IRR 1999 and the Radiation (Emergency Preparedness and Public Information) Regulations 2001.

3.3.1 Health and Safety at Work Act 1974

The HSAWA 1974 is essentially an ‘enabling’ act under which many sets of specific health and safety regulations are formed. However, it does introduce the specific requirement for employers to safeguard the health, safety and welfare of employees and anyone else who might be affected by their activities *“so far as is reasonably practicable”*. It is an important function of the safety case to demonstrate that this is the case.

3.3.2 Nuclear Installations Act 1965

Under the NIA 1965, sections of which are relevant statutory provisions under HSAWA 1974, no site may be used for the purpose of installing or operating any nuclear installation unless the ONR, as the regulatory body, has granted a nuclear site licence. Facilities for the storage or disposal of radioactive waste fall within the definition of nuclear installations and so any site intended to contain the GDF will require to be licensed.

The NIA 1965 requires the ONR to attach conditions to each nuclear site licence that it believes are necessary or desirable in the interests of safety or with respect to the handling, treatment and disposal of nuclear materials (including radioactive wastes).

A standard set of 36 licence conditions has been developed which are attached to all nuclear site licences. Of these, a number contain requirements relating to safety cases. Licence condition (LC) 14, requires that the licensee sets up arrangements for the preparation and assessment of safety cases to justify safety during design, construction, manufacture, commissioning, operation and decommissioning of facilities on the site. The requirement to demonstrate the safety of operations via a safety case then arises from LC 23 which requires the identification of limits and conditions necessary for safe operation. Further licence conditions then extend the requirement for justification via safety cases of all phases of the life-cycle of a nuclear installation. These are LC 19 (Construction and Installation), LC 20 (Modification to Design of Plant under Construction), LC 21 (Commissioning), LC 22 (Modifications) and LC 35 (Decommissioning).

The licence conditions do not specify the contents of the safety case in detail or the nature of the arrangements for its production beyond the basic requirement for *"adequate documentation to substantiate the safety of the proposals"*. They do, however, specify requirements for review and categorisation.

Other licence conditions are also relevant to the assessment of the safety case or to key outputs of the safety case necessary for the delivery of nuclear safety. The requirement for the establishment of a nuclear safety committee (LC 13) to consider and advise upon, among other things, the adequacy of safety cases, recognises the desirability of having an internal check on the licensee's decision making processes such that safety considerations are adequately and proportionately addressed.

3.3.3 Management of Health and Safety at Work Regulations 1999

The relevance of the MHSWR 1999 to the production of safety cases lies in Regulation 3, which requires employers to make a *"suitable and sufficient assessment"* of the health and safety risks to employees and others potentially affected by their undertakings in order that appropriate control measures will be identified and put in place. This requirement covers all types of hazard including nuclear and radiological hazards, as well as non-radiological hazards, and applies to both the transport and movement of radioactive waste and operation of static nuclear facilities.

The MHSWR 1999 and the associated code of practice define three levels of risk associated with undertakings and require that the risk assessment is appropriate in detail and sophistication with the level of risk. The operation of nuclear plant is specifically identified as being at the upper end of this spectrum of risk with the risk assessments for such activities requiring the *"most developed and sophisticated techniques"* that is to say the quantitative safety analysis techniques and rigorous examination of engineering expected of the nuclear safety case.

3.3.4 Ionising Radiations Regulations 1999

The applicability of the IRR 1999 includes the processing, handling, storage, transport and disposal of radioactive wastes on or between nuclear licensed sites since these fall within the IRR 1999 definition of *"work with ionising radiation"*. Their importance to the safety case production process lies primarily in their statement of the legal requirements on 'radiation employers' for:

- Production of "suitable and sufficient" prior risk assessments [Regulation 7] which must be produced prior to the commencement of operations to justify that all reasonably practicable steps have been taken to identify radiological hazards and risks associated with the operations and to restrict the risks associated with both normal and potential accident conditions so far as is reasonably practicable – the development of the prior risk assessments will then lead to an identification of those operational and engineered measures necessary for radiological safety:

  - for nuclear operations and facilities posing a significant nuclear or radiological hazard, the safety case required by the site licence may be taken to fulfil the requirement for a prior risk assessment
  - for transport, the RPP will include the requirements for the prior risk assessment
- Restriction “so far as is reasonably practicable” of the radiation exposure of employees and other persons [Regulation 8(1)] in order to protect people so far as is reasonably practicable and make it a specific legal requirement for exposure to ionising radiations; since the IRRs apply wherever employees are exposed to ionising radiations including a nuclear licensed site, a primary function of the safety case is to demonstrate that worker exposure to ionising radiation from normal operations is or will be ALARP.
- Restriction of the radiation exposure of employees and other persons to within specified annual doses limits [Regulation 11(1)]; while the primary legal requirement for normal operation doses is that they must be restricted so far as is reasonably practicable, absolute legal limits are set by the IRR 1999 for annual radiation doses for all potentially exposed groups.
- RWM safety cases show compliance with these legal limits for both GDF and transport operations

3.4 Environmental safety (operational phase and post-closure)

UK environmental legislation sets out the process that will be followed to develop and maintain environmental safety arguments and analyses to demonstrate environmental safety of the GDF during the operational period and the period after surrender of the environmental permit, often referred to as the post-closure phase. EPR 2010 controls the accumulation and disposal of radioactive waste in England and Wales. These regulations have replaced the Radioactive Substances Act 1993. In Northern Ireland, the Radioactive Substances Act 1993 still applies but the requirements are essentially the same.

The environmental permitting regime within EPR 2010 requires operators to obtain permits for some facilities, to register others as exempt and provides for ongoing supervision by regulators. The aim of the regime is to:

- protect the environment so that statutory and UK Government policy on environmental targets and outcomes are achieved
- deliver permitting and compliance with permits and certain environmental targets effectively and efficiently in a way that provides increased clarity and minimises the administrative burden on both the regulator and the operators
- encourage regulators to promote best practice in the operation of facilities
- continue to implement European legislation

Under Schedule 23 of the EPR 2010, a permit is required to dispose of radioactive waste. As a result, a permit from the EA will be required prior to accepting radioactive waste for disposal at the GDF. The Environment Agency (EA) has the power to grant these permits and to attach any limitations and conditions to the permits that they think fit. An environmental permit will also be required for any intrusive site investigation operations on a proposed site, such as the drilling of boreholes or underground site characterisation.

RWM will be required to develop and deliver environmental safety documents to support submissions for environmental permits throughout the life-cycle of the GDF. These submissions will include an ESC which addresses the requirements of EPR 2010 and relevant guidance issued by the environmental regulators in the form of guidance on requirements for authorisation (GRA) [10]. The GRA sets out the fundamental protection objective for the disposal of solid radioactive waste on land that forms the basis of the

guidance. It also sets out five principles, consistent with internationally accepted standards and recommendations that the developer/operator of a disposal facility and the environment agencies should follow. The fundamental protection objective relates to outcomes in the future after a disposal facility has been closed. It ensures that all disposals of solid radioactive waste to facilities on land are made in a way that protects the health and interests of people and the integrity of the environment, at the time of disposal and in the future, inspires public confidence and takes account of costs.

The principles set out in the GRA are:

- Principle 1: Level of protection against radiological hazards at the time of disposal and in the future; solid radioactive waste shall be disposed of in such a way that the level of protection provided to people and the environment against the radiological hazards of the waste both at the time of disposal and in the future is consistent with the national standard at the time of disposal.
- Principle 2: Optimisation (as low as reasonably achievable); solid radioactive waste shall be disposed of in such a way that the radiological risks to individual members of the public and the population as a whole shall be as low as reasonably achievable under the circumstances prevailing at the time of disposal, taking into account economic and societal factors and the need to manage radiological risks to other living organisms and any non-radiological hazards.
- Principle 3: Level of protection against non-radiological hazards at the time of disposal and in the future; solid radioactive waste shall be disposed of in such a way that the level of protection provided to people and the environment against any non-radiological hazards of the waste both at the time of disposal and in the future is consistent with that provided by the national standard at the time of disposal for wastes that present a non-radiological but not a radiological hazard.
- Principle 4: Reliance on human action; solid radioactive waste shall be disposed of in such a way that unreasonable reliance on human action to protect the public and the environment against radiological and any non-radiological hazards is avoided both at the time of disposal and in the future.
- Principle 5: Openness and inclusivity; for any disposal of solid radioactive waste, the relevant environment agency shall:
    - establish ways of informing interested parties and the public about regulatory goals, processes and issues
    - consult in an open and inclusive way

4 Key Elements of Safety Case Production

This section identifies what RWM considers to be the key elements and characteristics of the process for the production of nuclear safety cases. The information in the section is primarily applicable to safety cases that are produced to satisfy the requirements to justify the safety of operations on nuclear licensed sites. Nevertheless, the general aspects of these elements are also applicable to the production of transport and environmental safety cases. However, there is no regulatory requirement for a safety case for the transport operations. The safety of the transport operation is assured by the regulatory approval of the safety of the transport packages themselves (for example, by means of the DSR) and by the RPP.

Many of the key elements and characteristics of nuclear safety cases have been specifically identified in guidance published by the nuclear regulators and, as a prospective licensee, RWM has discussed expectations with the ONR and the EA.

RWM as an organisation has knowledge and understanding of the radioactive wastes for disposal and the geological and hydrogeological aspects of geological disposal with over 30 years of experience, first of all as (UK) Nirex and more recently as RWM within the NDA. This experience underpins the current competence of RWM as an organisation capable of the management and production of safety cases.

4.1 Fundamental expectations

The IAEA safety standards, requirements and guides provide the benchmark for the nuclear industry as a whole and, together with guidance published by the Western European Nuclear Regulators Association, are recognised by the regulators as the basis for relevant good practice. Under the UK's nuclear site licensing regulations, the licensee is legally responsible for the safety case and its adequacy. Those who have direct responsibility within the licensee organisation for delivering safety should have 'ownership' of the safety case. As RWM is operating as a prospective site licence company (SLC), it is imperative that this requirement can be demonstrated to be valid for the development of the generic DSSC.

Ownership is not merely a 'figurehead' role based on placing contracts with the supply chain in order to procure a safety case. It requires RWM to have a thorough understanding of the safety case and the limits and conditions derived from it, to ensure that the design implications are understood and applied together with the responsibility to ensure it is adequately managed and maintained. It is essential that not only are the arrangements for the production of safety cases an integral part of the safety management system, but also of the business arrangements such that safety and environmental issues are given appropriate consideration in the business decision-making process of RWM as an organisation.

In addition, the regulatory bodies in the UK have published guidance on their expectations for safety cases. For example, the ONR Safety Assessment Principles (SAPs) [11] and the ONR Technical Assessment Guide for safety cases [12] together with 'learning from experience' including the aftermath of the RAF Nimrod accident and the subsequent inquiry led by Charles Haddon-Cave QC [13] set out the key principles which would be expected in a safety case for a nuclear facility. The SAPs present principles together with supporting guidance and numerical safety criteria. It should be noted that the SAPs are primarily for internal ONR use but are available as a source of guidance to the industry and are used as the basis for the assessment of the safety of nuclear facilities and are therefore relevant to the information contained in safety cases for nuclear facilities. They relate only to nuclear safety and radioactive waste management.

The SAPs generally reflect the non-prescriptive nature of the UK's nuclear regulatory system, in that they are not mandatory and they need to be adapted to the type of nuclear facility in question such as radioactive waste facilities. However, in some cases, the principles and numerical criteria include specific regulatory requirements, and, in those cases, they are mandatory. The principles, of which there are approximately 300, are structured in separate sections, as follows:

- fundamental principles – these principles are founded in UK health and safety law and international good practice and underpin all those activities that contribute to sustained high standards of nuclear safety
- leadership and management for safety – this section sets out principles that form the foundation for the leadership and management for safety in the nuclear environment
- regulatory assessment of safety cases – this section sets out the principles applicable to the assessment of the production and nature of safety cases
- regulatory assessment of siting – this section provides principles applied in the assessment of a site, since the nature of a site can have a bearing on accident consequences
- engineering principles – this section comprises the major part of this document and covers many aspects of the design and operation of nuclear facilities
- radiation protection – this section provides a link with the IRRs
- fault analysis – this section sets out the expectations for the assessment of faults
- numerical targets and legal limits – this section sets out the targets to assist in making ALARP judgments
- accident management and emergency preparedness – this section provides the links to assessing compliance with licence conditions and the Radiation (Emergency Preparedness and Public Information) Regulations 2001
- radioactive waste management – this section sets out principles for radioactive waste management
- decommissioning – this section sets out the principles for planning and carrying out decommissioning
- control and remediation of radioactively contaminated land – this section sets out sets out principles for the safe management of radioactively contaminated land on nuclear licensed sites

Not all of the principles will be relevant to every facility. For example, a number are directed primarily at the safety of nuclear reactors and have very limited or no relevance to radioactive waste management facilities.

Under the conditions of a nuclear site licence, safety cases are required for all phases of an activity on a nuclear licensed site. The SAPs contain principles relevant specifically to the design process and to the safety cases for construction, commissioning, operation and decommissioning.

Approximately two thirds of the principles are engineering principles showing that safety should primarily be delivered by robust engineering. A primary purpose of RWM's safety case is to demonstrate that such a philosophy has been adopted in the design and operation of the GDF.

Technical Assessment Guides

As with SAPs, the material in these guides represents internal ONR guidance and is not intended to be mandatory for nuclear site licensees but they represent what ONR considers to be relevant good practice. Their primary function is to provide additional guidance to inspectors on the interpretation and application of the SAPs as an aid to the assessment of licensees' safety cases. They contain a greater depth of guidance in specific areas than that provided in the SAPs and are therefore of considerable value to licensees. A secondary role is to supplement the Technical Inspection Guides (TIG).

Technical Inspection Guides

The purpose of this guidance is to provide assistance to inspectors in carrying out inspection of licensee's compliance with nuclear site licence conditions including their arrangements for safety case production.

Within the SAPs, under the heading of *Regulatory Assessment of Safety Cases*, ONR has set out its key principles which address not only the necessary content and characteristics of the safety case but also the process for its production.

The SAPs and TIGs make it clear that the regulatory assessment will not only be of the safety cases themselves but also the process for their production. This process must be defined by the licensee's arrangements for compliance with LC 14. As such, for the claims made in the safety case that a facility is highly reliable and unlikely to fail and to be adequately robust to be justified, then the system employed to derive the claims must, itself, have high reliability. Thus, there is the need for safety cases produced by the system to be of consistent quality and fitness for purpose through the application of robust management arrangements.

Certain essential attributes of such a system are identified. Each element of the process must be clearly defined in relation to its purpose, standards and expectations. Consideration should be given to identifying vulnerabilities of each element of the process and potential ways they could fail to meet their defined objective identified. Threats that could cause failure should then be identified and suitable defences against them put in place.

High reliability of the process should then be ensured in a manner analogous to that required for high reliability engineered systems through multiple protections affording defence in depth. Many of the protections afforded will take the form of checks, verification and reviews, endorsement and approval procedures. However, multiple controls of this type, if they lack mutual independence, will not produce the necessary high levels of reliability. The SAPs therefore expect an element of diversity to be included in such controls in that there must be independence between those individuals conducting the required reviews and those involved in the production of the safety case and the development of the design. This expectation for multiple levels of protection is amplified in the TIG for LC 14 [14], which expects there to be in place arrangements for verification, peer review and independent assessment of safety documentation and that the arrangements include an endorsement and approval process commensurate with the safety significance of the documentation. The TIG also expects that the arrangements contain a system to ensure that the licensee maintains and controls all documentation to support its safety cases.

A crucial success factor for any safety case is the competence of the individuals involved in the production. The key requirement is that all individuals with roles within the process are *"suitably qualified and experienced persons"* (SQEPs). The SAPs expect the definition of training and qualification requirements for all roles. The LC14 Technical Assessment Guide and TIG clarify that this should include not only authors and analysts involved in writing the safety case but also those involved in its review, verification, independent assessment and approval. In particular, it is expected that there will be a robust system of

control where elements of the production process (including review functions) are contracted out to external agencies.

4.2 RWM's safety case production and management process

4.2.1 Acceptance criteria

A key element in the safety case production process is the definition of acceptability criteria against which the output/conclusions of the safety analysis may be judged. The ONR guidance in the LC14 TIG expects that licensees will develop their own safety principles, criteria and standards for this purpose as part of their LC 14 compliance arrangements. These criteria must meet any legal requirements and take due account of regulatory guidance.

In its publications The Tolerability of Risk from Nuclear Power Stations [15] and Reducing Risks, Protecting People [16], the Health and Safety Executive (HSE) sets down its views on the tolerability of risk, providing numerical criteria for the judgement of the acceptability of risks and explaining their philosophy for decision-making based on risk and the concept of ALARP. These concepts have subsequently been developed by ONR as specific criteria for nuclear facilities and are detailed in the SAPs.

RWM has published its numerical safety assessment criteria for normal operations and accident conditions. The numerical targets defined in the RWM documents are based on the criteria in the SAPs and are consistent with the philosophy described in the regulatory guidance. These are:

- The RWM Radiological Protection Criteria Manual [17] which includes a statement of RWM's policy on radiological protection and provides radiological criteria for the assessment of the following:
  - nuclear and radiological safety of the GDF up to the point in time where institutional control is withdrawn that is to say the operational phase, closure and probably a period of time after closure
  - nuclear and radiological safety of the GDF after institutional control has ceased (post-closure)
  - nuclear and radiological safety of off-site waste transport operations
- The NOSM which includes a procedure detailing the acceptability criteria for the following:
  - normal operational exposures to the workforce and members of the general public
  - criteria for the assessment of design basis accidents to the workforce and members of the general public
  - criteria for probabilistic safety assessment to the workforce and members of the general public
  - criteria for severe accidents involving the workforce and members of the general public

4.2.2 Safety case production

Within RWM's management system, the safety case manuals (transport, operational and environment) set out the approach to the management and production of safety cases. The application of this process aims to ensure that safety cases are produced using a high reliability process that will ensure the output will deliver the required safety. This includes:

- ensuring that there is a clear production and delivery strategy for each safety document covering the objectives and success criteria, the activities that will be undertaken as part of the document management and production process as well as identifying risks and detailing mitigation strategies
- ensuring that responsibilities for safety documentation are clearly defined and understood
- ensuring that the requirements and scope for safety cases are clearly understood and complied with
- ensuring that appropriate and suitably qualified and experienced resources are utilised, in accordance with the safety case strategy
- ensuring that safety cases are produced to a consistent format and quality including the use of specifications of safety cases to assess whether they have met the pre-defined objectives
- provision of suitable and sufficient barriers which are put in place and implemented against failure of the management process including an appropriate and proportionate level of scrutiny is applied to safety case documents through due process
- ensuring that responsive feedback mechanisms are applied to detect underlying weaknesses in the process and to facilitate continuous improvement

4.2.3 Safety case strategy

Production of a safety case strategy plays an essential role in ensuring that the approach to safety cases and the associated assessments is set out and clearly understood by all the appropriate stakeholders. It is linked to the concept of the ‘right first time’ safety case. Therefore, it concentrates on the process for production rather than just the technical content. The strategy should:

- clearly state the objectives of the project and the roles, purpose, standards and expectations of the safety case
- identify the key roles and their responsibilities and accountabilities for producing the safety case
- identify the resources that will be required to ensure successful delivery of the safety case
- identify project delivery risks that could jeopardise the quality of the safety case and define appropriate prevention and mitigation strategies including designing in sufficient defence in depth provisions to minimise project risks
- define the success criteria and approval plan for the safety case
- define the scope and extent of the safety document assurance process to be undertaken, commensurate with the harm potential

These points are discussed in the following paragraphs.

Alongside the requirement to develop the safety case strategy is the need to define the responsibilities for all aspects of safety document management and production. This is in order to ensure that the requirements to ensure compliance with each aspect of the safety case process are clearly assigned and each of these roles has clear responsibilities and accountabilities.

In order to ensure the safety case is produced to the required quality, linking to the concept of the right first time safety case, it is necessary to ensure that the resources required for

producing the safety case are clearly specified. This includes ensuring that any risks of unavailability are acknowledged and suitable contingency measures put in place if required. As part of ensuring that the success criteria are met for safety documentation, it is necessary to ensure SQEP are utilised in its production and management, including the assurance and due process elements.

Of particular importance in terms of success measures for the generic DSSC are those listed in Table 1.

Table 1 Safety Case Objectives

Topic Area	Requirement	RWM Means of Assurance
Intelligibility	The safety case should be intelligible and structured logically to meet the needs of those who will use it. It must avoid the use of long, bureaucratic, repetitive and impenetrable detail and documentation using language which is obscure, inaccessible and difficult to understand.	Internal verification (and independent external advice) will include the requirement to review all deliverables to ensure that they satisfy this requirement.
Validity	The safety case should accurately represent the current status of the GDF design in all physical, operational and managerial aspects and should demonstrate that the GDF will remain safe throughout a defined life-time.	The generic DSSC was developed from first principles based on an outline design in order to develop safety functions. Later updates of the safety cases will contain additional design detail which will justify that the design solutions chosen meet the safety functional requirements.
Completeness	The safety case should comprehensively analyse the activities associated with normal operations, identify and analyse the faults of potential safety concern and demonstrate that risks will be ALARP including explanation of the options for alternative designs or approaches that were considered at the initial stages. It should contain the information necessary to show that the facility will be adequately safe and what will be needed for it to remain so over the period for which the safety case is valid.	At this stage of the GDF design, the requirement is for safety functions and conceptual safety functional requirements and some conceptual safety measures to be identified and specified for the designers to find a suitable design solution. Internal verification and independent expert advice include the requirement to review all deliverables to ensure that they satisfy this requirement.
Evidential	The arguments developed in the safety case should be supported with verifiable and relevant evidence (documented, measurable, etc).	Internal verification includes a review of all deliverables to ensure that they satisfy this requirement.

Topic Area	Requirement	RWM Means of Assurance
Robustness	The safety case should demonstrate that the GDF will conform to good nuclear engineering practice and sound safety principles, including defence-in-depth and adequate safety margins.	Internal verification and independent expert advice includes a review of all deliverables to ensure that they satisfy this requirement.
Balanced	The safety case should present a balanced account, taking into consideration the level of knowledge and understanding and taking into account proportionality in terms of the hazards and risks and the level of attention and analysis applied.	Internal verification and independent expert advice includes a review of all deliverables to ensure that they satisfy this requirement.
Ownership	RWM should retain ownership as the intelligent customer particularly where reliance is placed on the external supply chain to ensure that the safety case meets the aims and objectives defined in the strategy.	Arrangements are in place to ensure ownership within RWM through management of the DSSC elements.
Questioning	RWM should ensure that the safety case provides challenge to the design rather than argue to justify the status quo for the design.	Internal verification and independent expert advice includes a review of all deliverables to ensure that they satisfy this requirement.
Learning	The monitoring and auditing of the safety case should examine both the process of safety case production and the substance of the documentation and should ensure that learning from experience is facilitated and applied such that future developments take cognisance of the lessons learnt.	Learning from experience is built into the project management and review process and was applied on completion of the 2016 DSSC update.

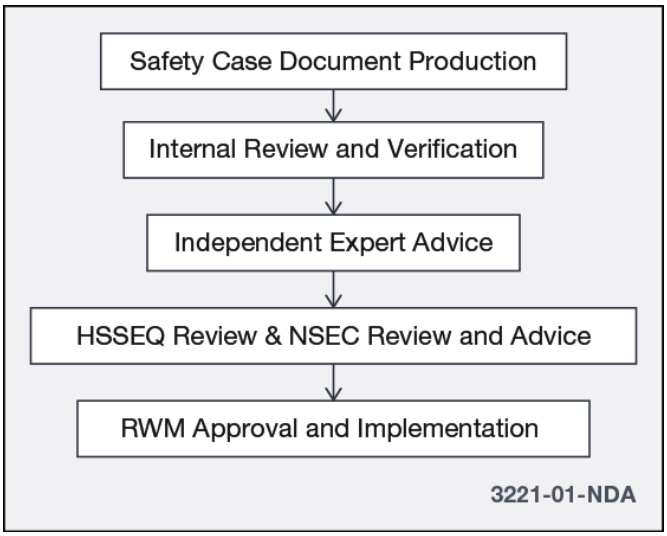
The process for the management and production of right first time safety cases should be based on the same concepts as those applied to high reliability engineered systems. For a safety case to claim that the facility under consideration is reliable or highly unlikely to fail, the process used to derive such claims needs to have commensurate levels of reliability. As part of this process, potential weaknesses or failure modes in the safety case management and production process need to be identified so that suitable defences or barriers in response to the identified potential failures or weaknesses can be determined and implemented. In order to achieve a high reliability organisational competence in this area, some form of diversity in the elements and their defences, not just redundancy, may be appropriate. This should include safety case review by people who are independent of those involved in its production.

The independent review function seeks to review the safety case and to identify any defects present in the safety case process. For the independent review function to be truly effective, this requires it to be informed and authoritative to provide a robust independent challenge capability providing sufficient diversity, redundancy, checks and balances to ensure that suitable and proportionate barriers are provided to protect against erroneous decision making and action.

Within RWM, the safety document assurance process (Figure 3) provides the challenge and the necessary barriers through due process to ensure that safety cases are adequate and fit for purpose through:

- ensuring that the independent quality assurance verification and validation resources are SQEP
- internal checking review undertaken by RWM as the intelligent customer
- internal verification performed by SQEP and supported by specialist expert advice where it is deemed necessary
- independent expert advice which confirms that adequate safety arguments have been developed in the document under review and that RWM standards have been met through an independent professional view of the robustness and validity of the safety arguments presented in the document being reviewed and whether the safety arguments, methods and data are acceptable when compared with RWM and other relevant modern standards
- review by the RWM Health, Safety, Security, Environment and Quality (HSSEQ) department
- consideration by the Nuclear Safety and Environment Committee for review and advice (if required)

Figure 3 RWM Safety Document Assurance Process



4.3 RWM's approach for the generic DSSC

RWM's management strategy is based on the premise that it will remain a small organisation with specialist staff operating as an 'intelligent customer' that works with external contractors to design, construct and operate the GDF. This includes the development of the required safety case documentation. The term 'intelligent customer' is defined [18] as:

"*As an intelligent customer, in the context of nuclear safety, the management of the facility should:*

- *know what is required*
- *fully understand the need for a contractor's services*

- *specify requirements*
- *supervise the work*
- *technically review the output before, during and after implementation*

The concept of intelligent customer relates to the attributes of an organisation rather than the capabilities of individual post holders."

With respect to the role of RWM as an 'intelligent customer' under the site licensing regime, there are some broad principles which underpin ONR's expectations of a licensee's arrangements for the use of contractors and for retaining control of nuclear safety [18]. These are summarised below:

- the licensee should maintain a core in-house staff to ensure effective control and management for nuclear safety
- the licensee should retain overall responsibility for, and control and oversight of, the nuclear and radiological safety and security of all of its business, including work carried out on its behalf by contractors (note that this is a legal requirement)
- licensee choices between sourcing work in-house or from contractors should be informed by a company policy that takes into account the nuclear safety implications of those choices
- the licensee should maintain an 'intelligent customer' capability for all work carried out on its behalf by contractors that may impact upon nuclear safety
- the licensee should ensure that it only lets contracts for work with nuclear safety significance to contractors with suitable competence, safety standards, management systems, culture and resources
- the licensee should ensure that all contractor staff are familiar with the nuclear safety implications of their work and interact in a well-coordinated manner with its own staff
- the licensee should ensure that contractors' work is carried out to the required level of safety and quality in practice

As stated above, RWM intends to operate as a small organisation, meeting the requirement to be a 'capable organisation' and an 'intelligent customer' by recruiting and retaining SQEP within its staff complement to ensure that effective control and management of nuclear safety is maintained. At the current early design stages, this can be achieved with a relatively small RWM organisation with support from the supply chain but as the design becomes more developed, there will be the need for RWM to recruit sufficient SQEP to provide assurance to itself and to the regulators that it is capable of acting as the design authority for the GDF. Regulators such as ONR and EA currently expect that every operator maintains a complete understanding and knowledge of the design of every licensed facility under their control. The IAEA safety standard SSR-2/1 [19] calls for the nuclear operator to maintain design integrity and knowledge within their own organisation in the form of the design authority which includes:

- responsibility for ensuring the design authority and intelligent customer roles are discharged throughout the nuclear operator's organisation
- responsibility for the overall design of the disposal system including package development, the transport system and the GDF
- accountability for the engineering design process, including management and review of updates to the EDM which provides the means by which RWM demonstrates that it meets the requirements of IAEA SSR-2/1

This will include the maintenance of corporate knowledge and capability throughout the lifecycle of the GDF.

For the development of the generic DSSC the nominated RWM intelligent customer is responsible for the following activities:

- acting as intelligent customer for safety case services in the appropriate safety disciplines
- acting as intelligent customer for operational safety input to disposability assessments
- responsible for representing RWM in technical fora relating to disposal systems safety

Within the context of the update and future development of the generic DSSC, the intelligent customer role will ensure that all aspects of the safety case development are undertaken in accordance with RWM quality requirements and processes such as the safety case manuals by ensuring that the following specific requirements have been put in place and implemented:

- all members of the supply chain appointed to support the development of the generic DSSC will be contracted through framework agreements which provide for continuity of work and resource
- all members of the supply chain shall have sufficient staff with the necessary competencies and experience to fulfil their duties; the supply chain shall provide details of all staff working on activities related to the generic DSSC in order to demonstrate that they are, and will remain, SQEP to perform the designated activities
- ensure that all activities performed by the supply chain are subject to a level of technical monitoring and control commensurate with the importance of the activity with regard to nuclear safety
- members of the supply chain shall provide evidence of the quality management and assurance arrangements to be applied to the work which may be subject to audit and inspection by RWM
- an independent review and verification activity will be provided for all generic DSSC related deliverables which forms part of the RWM quality assurance arrangements
- active promotion of a learning from experience culture as part of the generic DSSC update so that members of the supply chain and RWM proactively contribute to ensuring that any best practice, lessons learnt and process improvements are identified, discussed and taken forward into the RWM continuous improvement process

4.4 Modelling and data

Quantitative analysis of the performance of the GDF requires the use of computer modelling and data. The approach to the development, verification and application of data which underpin the safety assessments is a very important part of the quality assurance applicable to the DSSC development.

The safety assessment will require the use of computer codes, models and toolkits in order to undertake complex calculations and/or to ensure that calculations are performed using standardised approaches and models.

Where proprietary or industry codes, models or toolkits are used, RWM requires that evidence of the verification and validation carried out is provided. For any codes, models or

toolkits developed specifically for application on the GDF design and safety cases, these shall be verified and validated in accordance with the suite of RWM management system documents governing the management and control of models and data:

- RWP31 – Computer Modelling Aims and Principles
- RWP102 – Data Management Aims and Principles
- subsidiary procedures, work instructions and forms

In addition, a published framework [20] describes and explains RWM's strategy and principles for the application of modelling.

5 Management of Safety Documents

5.1 Future nuclear licensing

Since December 2009, RWM has operated as a 'prospective SLC', which provides a stable and accountable framework to meet the immediate needs of the business, its regulators and other stakeholders. As part of the transition of the organisation towards SLC status, RWM is putting in place the management organisation, arrangements and other requirements necessary to demonstrate to the regulators that it is a capable organisation.

As part of the transition towards becoming a SLC, RWM has embarked on a programme to plan the development of arrangements for meeting all the 36 licence conditions required under the NIA 1965. The first step of this process is to understand what is needed and to develop a skeleton structure to inform discussions. These arrangements will include the production of safety cases to seek approval, for example, for the construction, testing, commissioning and operation through licence instrument applications. The nuclear regulator (ONR) will expect RWM to have such arrangements in place well in advance of granting a site licence and will expect to scrutinise the developing design safety cases produced as required by the said arrangements under approved procedures, eventually as formal licence instrument applications. RWM's current planning basis is that it will have applied for, and been granted, a nuclear site licence before excavation work for underground investigation begins.

In addition, RWM will need to demonstrate to the regulators that it is a capable organisation and can take the role of being an intelligent customer for those activities on which it relies on external organisations for support. Being a capable organisation requires the retention and use of knowledge within the organisation so that safety requirements are understood and risks are controlled throughout all activities, including those undertaken by contractors at all levels within the supply chain. This means that the organisation should be capable of sustaining a 'design authority' capability that includes suitable and sufficient experts with a detailed and up-to-date understanding of the safety of the GDF and the design, operation and safety cases. The intelligent customer capability must therefore be maintained to ensure that the use of contractors in any part of the organisation does not adversely affect its ability to manage safety.

As part of the transition from a prospective SLC to a full SLC, RWM will be required to both put in place and demonstrate compliance with (through regulatory audits) the appropriate management arrangements, systems and processes. This will be required to demonstrate that RWM has developed and implemented a management system to comply with all relevant requirements of the UK nuclear licensing system as well as the requirements of general health, safety, environment and other relevant legislation prior to the granting of a site licence. As part of its application for a nuclear site licence, RWM will have to demonstrate to the ONR that the management arrangements it has in place to manage the 36 standard licence conditions have been made and fully implemented.

These management arrangements also include the required organisational structure and staffing baselines to deliver nuclear safety, together with the process for the management of any changes. A nuclear licensed site also has to be compliant with other regulatory requirements administered by other bodies; for example, the UK environment agencies regulate the disposal of radioactive waste from nuclear sites under the EPR 2010. Thus RWM's management system also includes arrangements to implement the regulatory requirements of industrial safety, security, the environment or other parts of RWM's remit. The key objectives of RWM's management system are to:

- effectively manage and demonstrate legal compliance
- satisfy regulatory expectations

- demonstrate health, safety, security and environment commitment and achieve continuous improvements
- reduce health, safety, security and environment risks with due regard to proportionality
- improve performance
- maintain public confidence

RWM has commenced the process of developing an architecture for a hierarchical management arrangements framework which sets out the flow down from all regulatory requirements and licence conditions applicable to RWM in its future role as a SLC, to the high level documents that would be required to set out the management arrangements to demonstrate compliance. In addition, the framework sets out the relationship to the lower tier documents (processes and procedures such as the safety case manuals). The second phase of this project will be to develop specifications (purpose and scope) for each of the high level documents proposed in the framework and a schedule to produce all the required documentation. The third phase will be to develop fully the suite of documents for all the strands in the framework, in particular, the strand that starts with LC 14, and other related legislative requirements and licence conditions, through to the NOSM. This will then allow the arrangements necessary for application for the site licence to be demonstrated to the regulators as part of the application process.

5.2 Safety management

At future stages in the programme, under current legislation, RWM will need to apply for environmental permits and a nuclear site licence. For example, an environmental permit will be required before the commencement of intrusive site investigation and a nuclear site licence and a revised environmental permit will be needed before RWM commences any construction activities related to the GDF. Safety documentation (such as DSRs) justifying the transport of waste in specific transport containers will need to be produced and submitted to the competent authority, the ONR, or to the internal self-approval process for IPs.

The ONR and the EA have published their respective expectations for safety management in relation to nuclear installations. The ONR's expectations are contained in the SAPs. These set out and explain four top-level principles for leadership and management of safety that inspectors would expect a licensee to satisfy. The four principles are:

- Principle MS.1. Leadership: directors, managers and leaders at all levels should focus the organisation on achieving and sustaining high standards of safety and on delivering the characteristics of a high reliability organisation
- Principle MS.2. Capable Organisation: the organisation should have the capability to secure and maintain the safety of its undertakings
- Principle MS.3. Decision Making: decisions made at all levels in the organisation affecting safety should be informed, rational, objective, transparent and prudent
- Principle MS.4. Learning from Experience: lessons should be learned from internal and external sources to continually improve leadership, organisational capability, the management system, safety decision making and safety performance

The EA has published its equivalent guidance in the GRA. Requirement R4 of this document requires:

"The developer/operator of a disposal facility for solid radioactive waste should foster and nurture a positive environmental safety culture at all times and should have a management system, organisational structure, and resources sufficient to provide the following functions:

(a) planning and control of work; (b) the application of sound science and good engineering practice; (c) provision of information; (d) documentation and record keeping; (e) quality management."

Principle MS.1 of the SAPs requires an organisation to have a strong safety culture which is promulgated down from directors, managers and leader at all levels in the organisation. This safety culture is set out in RWM's safety and environmental policy statement [21].

An important aspect of the maintenance of a positive safety culture is learning from experience. The HSE defines key characteristics of a learning organisation as follows [22]:

- encourages challenge across the organisation and reflects on information and experience to strive toward continual improvement
- has an effective knowledge management process, managing the three fundamental components of people, processes and technology as an integrated resource
- has an effective process for monitoring the performance of its management systems and the standards achieved
- shows willingness to learn from the performance of other comparable organisations
- has performance measures that reflect actual performance and are consistent with the 'Learning from Experience' SAP MS.4
- has an effective process for the identification of the best improvement option and its effective implementation

RWM fosters a learning organisation culture through the following mechanisms.

Learning from Other Organisations

RWM learns from its interactions with other organisations in the UK such as nuclear site licensees and the regulators with whom there are close and frequent links. RWM also works with a number of overseas organisations to identify areas of common interest where mutual benefit can be gained through cross fertilisation of ideas and sharing of experience.

Enhancing Learning Culture

The NDA is positively committed to providing learning opportunities and to encouraging its employees to undertake such activities as part of their career development. The NDA recognises that individual learning and development needs may include external support, for example further education, as well as internal support to provide broader experience and other experiential learning opportunities. The NDA's learning and development policies and procedures apply equally to RWM.

In order to demonstrate that its management system meets the regulatory requirements, including that of being a 'learning organisation', RWM has produced a Safety and Environmental Management Prospectus (SEMP) [23]. The SEMP demonstrates that RWM has an adequate management structure, safety management arrangements and resources to meet the nuclear safety and environmental aspects of its current and near future stages of work; one of which is the production of the DSSC.

The SEMP is supported by the Organisational Baseline Document [24] which describes the organisation that is needed to implement the management systems described in the SEMP. It includes an organisational baseline compliance assessment that assesses the extent that RWM complies with the requirements set out in the Organisational Baseline Document. Any changes to the organisational structure that could affect the key safety and environmental safety related activities are controlled in accordance with RWM's management of organisational change procedure [25].

5.3 Current RWM safety management structure

With respect to safety management, the RWM Managing Director is accountable to the NDA Executive and Board for all aspects of safety including the production of safety cases. The Managing Director is supported in this respect by the HSSEQ Director who provides advice on HSSE issues to the Managing Director. The HSSEQ Director also, through his staff, sets the standard for safety cases discussed elsewhere in this document and provides an independent review function as discussed below.

A key component of the safety management system is the RWM internal regulation system. This function is provided by the HSSEQ Director and provides an audit and review function independent of executive decision-making. The objective of this function is to provide assurance to senior managers and regulators that RWM complies with all relevant safety legislation and that key safety related decisions are subject to robust challenge. The responsibility of production of the DSSC rests with Science and Technology Director; this ensures that there is management separation between production and assurance. In the future, when the organisation completes the transition to a SLC, the HSSEQ team will be responsible for ensuring that the licensed organisation meets the requirements of the site licence conditions under the NIA 1965 and the environmental permits issued under the EPR 2010. The HSSEQ team also acted as independent reviewer of the safety cases, thereby providing internal challenge. They also act as the formal interface between RWM and the regulators.

5.4 Configuration and change management

The management of change is a key part of the design and safety process of the GDF and for other changes that may affect transport, operational and environmental safety. For example, waste consignors, carriers and consignees have a duty to ensure that no modification to the transport system such as packages, inventory, procedures and how the packages are handled at the GDF before they are taken underground, which may affect safety is made except in accordance with adequate arrangements defined for this purpose.

The general principles of change control and associated configuration management are as follows:

- recognition of change
- understanding the safety impact of change
- agreement of change at the correct authority level including appropriate review, verification and validation
- controlled implementation and communication of change
- update of necessary documentation

RWM has an iterative process for the development of the geological disposal system. This process is currently applied in a generic, non-site-specific manner. The process for the management of each potential change is defined in the generic disposal system concept change management procedure RWPR40 which ensures that all proposed changes to the GDF concept are recorded, assessed and implemented at an appropriate time, in a consistent way. This applies to any changes to requirements, designs, assessments, safety cases, testing, acceptance and operations processes under configuration control.

The RWM change management procedure applies to all elements of the generic DSSC together with the supporting processes and procedures that underpin it, such as safety case manuals. This is an important part of safety case configuration management whereby RWM maintenance of the safety cases is controlled to ensure that they are, and continue to be, an accurate reflection of the disposal concepts.

6 Safety Principles, Methodology and Guidance

6.1 RWM principles and criteria

In addition to the regulatory expectations, RWM has produced a number of policy and process documents that specify the standards to be applied across the design and safety assessment development, as part of the safety integrated design process. These include the following:

- the RWM Radiological Protection Criteria Manual
- the RWM GDF Design Principles [26] which were developed to conform to current good practice including the IAEA Fundamental Safety Principles [27], IAEA Safety Requirements for the Geological Disposal of Radioactive Waste [28], the ONR SAPs and the EA GRA for geological disposal facilities on land for solid radioactive wastes as well as being benchmarked against Nirex's (RWM's predecessor organisation) earlier Nuclear Design Safety Principles [29]
- the RWM EDM which describes the process to be used to establish, maintain and update engineering designs for the development of the GDF based on staging the design with each stage having a set of design outputs and a formal 'Engineering Stage Gate' review

The basic structure of the GDF Design Principles comprises the following elements:

- the 'fundamental principles' which are the nine high level principles to provide a basis for design and assessment of GDFs drawn from international and national guidance on the management of radioactive waste
- the 'design process principles' which are the 16 high level principles to be addressed by the design in terms of:
  - safety management
  - design management
  - quality and information management
- the 'design principles' which are used to underpin the design process in the form of 27 specific principles which address:
  - general design
  - protective structures and systems
  - containment systems and features
  - construction and operations
  - closure
  - security
  - safeguards

At this generic stage, illustrative designs have been developed for three types of host rock representative of host rocks found in the UK. These illustrative designs have been developed based on design approaches used for similar facilities in other countries. As the designs develop, the GDF will progress through the staged gate review process into the further design stages, namely adapted illustrative designs, conceptual designs, scheme designs, a preferred design and a detailed design before entering the construction stage.

The integration between safety, design and operations is a fundamental requirement for a new build nuclear facility. The process should aim to demonstrate that safety considerations are integral to the design process and that the formal safety justification, as evidenced by the relevant safety case, is fully coordinated with the design activity and should evolve in parallel. This is necessary to ensure the design arrangements leading into the operations and associated maintenance and inspection are adequate to fulfil the required safety functions. It is also necessary to establish that the hazards created by such arrangements are both tolerable and ALARP. This integrated design and safety approach has commenced development within RWM and will further develop as the design advances towards the scheme design phase. The integration of design and safety forms a key part of RWM's way of working for the future development of the GDF design and the safety and environmental assessment and documentation for the transport, operation and environmental aspects of the GDF life-cycle.

The approach taken to ensure the integration of design and safety utilises RWM's design processes, together with the safety case procedures developed as part of the safety case manuals and a gate review process approvals mechanism within the RWM EDM. The gate review process provides a formal decision before the project passes from the 'feasibility' testing phase to the 'design' phase if the necessary design and safety deliverables, commensurate with the stage of development, are available. The RWM EDM therefore, in conjunction with the safety case manuals, sets out the process by which design and safety will be integrated throughout the GDF life-cycle.

6.2 RWM assessment methodologies

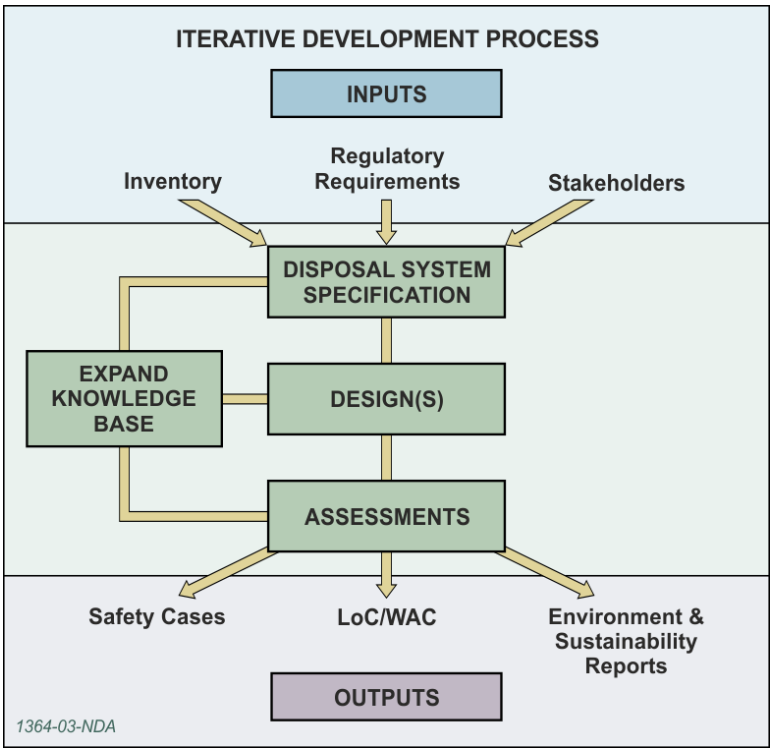
The generic DSSC presents the safety case for the generic illustrative designs which will be developed as the facility design is tailored to make best use of the selected site. For example, the aim of the generic OSC is to demonstrate that it is feasible to design and operate the geological disposal system within a well-defined, credible and verifiable safe operating envelope and that the GDF will remain safe after it is closed and will meet all applicable regulatory requirements. It must also ensure that it is possible to handover from the operational phase to the post-closure phase such that activities undertaken during construction, emplacement, backfilling and decommissioning do not compromise the requirements of the ESC. This will require the ESC, at some future date, to define the safety requirements needed to be satisfied under the OSC to ensure that the GDF remains safe throughout the post-closure period. Hence, the operational safety case documentation will need to state what can be achieved and justify that this is acceptable for the handover.

For the GDF, the approach taken to the development of the safety case is different to that for other nuclear safety cases. The safety case for the GDF is currently at an early stage of development, because the site and design have not yet been chosen. It is therefore referred to as a 'generic' safety case, and the strategy to demonstrate safety is also termed 'generic' because it must cover a range of possible disposal environments and illustrative facility designs.

6.3 Safety case manuals

The RWM work programme is based on iterative development of the GDF, as shown in Figure 4. The process starts with identification of requirements and constraints on which the system specification is developed. A disposal system design is then developed to meet the specification and this design is then subject to assessments of its safety and environmental impacts. Information from research and development is required to support these activities. The outputs from the safety assessments are used to identify where further research and development is required to iteratively inform the system specification and design.

Figure 4 Iterative Development of the Disposal System



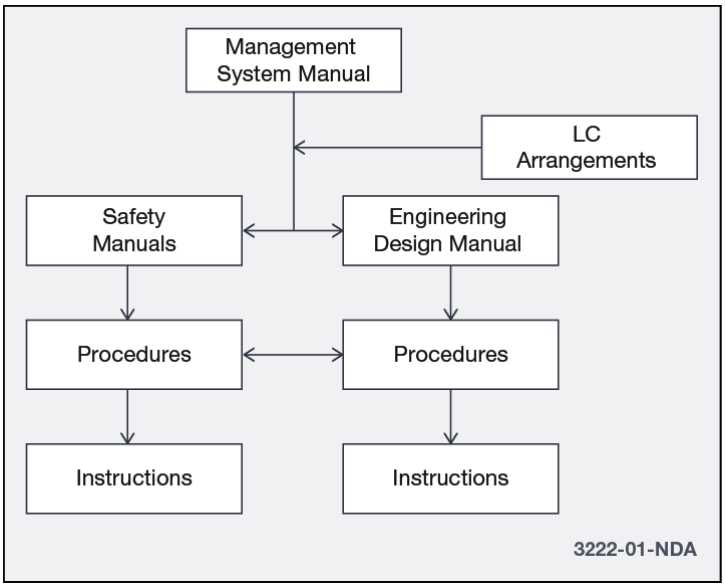
As the GDF designs progress from the current generic stage and, as the siting process progresses and more information about a specific site is obtained, it will be necessary to demonstrate to the regulators an auditable and controlled process for producing safety cases. In order to meet this requirement, RWM has developed a series of manuals, collectively referred to as 'safety case manuals' covering transport, nuclear operations and the environment.

The safety case manuals support the process of producing safety and environmental documentation and describe:

- the documentation required throughout the GDF project and the stages of the project at which these documents will be required
- the scope, content and format of the various staged documents so as to ensure consistency of approach and presentation
- the procedures, methodologies, guidance, techniques and base data to be used to undertake the assessments that underpin the documentation including the identification and assessment of hazards, the risk control and management processes and the demonstration of risk reduction, including ALARP

The safety case manuals provide an overview of the process to be followed to produce and maintain safety documentation throughout the life-cycle of the GDF. The manuals form part of a suite of documents that underpin the RWM management system including providing the safety case link to the design process through the RWM EDM and the LC 14 safety case arrangements as required by NIA 1965. It also provides a structure for lower tier procedures and work instructions. This is illustrated in Figure 5.

Figure 5 RWM Quality Management System



The safety case process adopted within the safety case manuals is built around the HSE 'five steps' process for undertaking risk assessment [30]. The HSE 'five steps' process is applicable to any situation that begins with a requirement to identify hazards and concludes with demonstrating that appropriate control measures have been implemented to reduce risks to ALARP, namely:

- step 1: identify the hazards
- step 2: decide who might be harmed and how
- step 3: evaluate the risks and decide on precautions
- step 4: record your findings and implement them
- step 5: review your assessment and update if necessary

The HSE 'five steps' process is iterative and the manuals are structured likewise but with the addition of 2 extra steps to cover specific requirements associated with the nuclear industry and are designed to be applied to the design stages defined in the EDM. The framework for all the safety case manuals uses three levels of the hierarchy within RWM's management system:

- The manual (tier I) – provides an introduction with reference to supporting procedures and work instructions and to other directly related parts of the wider management system.
- The procedures (tier II) – define business processes, often implementing aspects of a policy; in this case, they define the procedures that are required to meet the needs set out in the manual where procedures are mandatory.
- The work instructions (tier III) – detailed support documents, providing more detail than procedures presenting further guidance that could be used in meeting the requirements set out in the manual or in procedures, for example, in undertaking numerical assessments; work instructions are mandatory and must be followed unless the introduction or scope to the work instruction specifically says it is not mandatory to some aspect of work, or if an alternative approach is justified, documented and agreed as part of the doing of the work.

Each of the manuals is therefore structured around this framework with slight changes to reflect the specifics of the topic area.

Hence for the TSM, the top tier structure comprises the following topic areas:

- T1: Document management, production and assurance
- T2: Transport radiological safety assessment
- T3: Definition and substantiation of the transport safe operating envelope
- T4: Implementation of transport safe operating envelope
- T5: Transport radiological dose reduction
- T6: Interaction with design process
- T7: Maintenance of transport radiological safety

For the NOSM, the equivalent top tier manual is structured as follows:

- N1: Document management, production and assurance
- N2: Safety assessment
- N3: Definition and substantiation of the safe operating envelope
- N4: Implementation of the safe operating envelope
- N5: Risk reduction
- N6: Interaction with the design process
- N7: Continued maintenance of safety

For the ESM, the equivalent top tier manual is structured as follows:

- E1: Environmental safety document management and production
- E2: Environmental safety assessment
- E3: Environmental safety objectives and functions
- E4: Performance confirmation
- E5: Environmental risk reduction
- E6: Interaction with other RWM functions
- E7: Maintenance of ESC for an operational GDF

6.3.1 The Transport Safety Manual

The TSM has been developed and approved as part of the RWM management system. It describes the processes that will be followed to develop and maintain safety arguments and analyses to demonstrate the safety of the design, development and operation of a transport system for delivering packages of radioactive waste to the GDF.

The purposes of the TSM are to:

- direct the preparation and review of transport radiological safety documentation
- facilitate the maintenance and update of the extant transport safety documentation
- provide a flexible structure that will meet the needs of the GDF project throughout the development of illustrative and proposed transport system designs and the operational lifetime of the transport system

The scope of the TSM is the documentation relating to radiological safety of the transport of radioactive waste to the GDF. It covers the aspects of the transport system for which RWM is assuming responsibility. It begins at the point where transport packages are secured onto a transport vehicle at a consigning site for dispatch to the GDF and concludes at the point where responsibility for the transport packages is handed over to operators at the GDF. The TSM:

- provides assurance that the radioactive waste transport operations associated with the operation of the GDF can be achieved safely
- provides a benchmark against which to carry out disposability assessments of waste producers' packaging proposals
- informs the iterative development of the illustrative and site-specific design
- provides context to applications for intrusive site investigations and for site construction
- provides assurance of the safety of radioactive waste transport operations

The TSM structure comprises the following 'steps':

- T1 details the safety case management, production and assurance process which sets out:
  - how all transport safety case documents will be managed
  - how production will be in accordance with defined specifications for each type of safety case
  - how safety cases and the associated activities are categorised on the basis of harm potential
  - how the assurance process will provide the level of 'due process' that assures suitable challenge and barriers to failure that support the right first time safety case objective including specifying the approval route for different categories of document
- T2 sets out the safety assessment process for generic, site-specific and operational transport safety assessments based on the following approaches:
  - generic radiological dose assessments to support the argument that a safety case for the GDF is feasible and to support packaging advice to waste producers by demonstrating that the worst case dose will not exceed the design limits and that best estimate dose will not exceed the design targets
  - inform a Preliminary Transport Safety Report which provides context to regulators and other stakeholders when applying for permission to begin intrusive surface based investigations at the candidate site(s); it is anticipated that the Preliminary Transport Safety Report will be based on the generic TSC operator dose assessment and emergency planning arrangements requirements
  - site-specific radiological dose assessment of a site-specific design which is needed to inform iterative development of a site-specific design, demonstrate that the worst case doses will not exceed the design limits and demonstrate that the best estimate doses will not exceed the design targets
  - inform a Pre-Construction Transport Safety Report which provides context to regulators and other stakeholders when applying for permission to begin construction of the GDF; it is anticipated that a Pre-Construction Transport Safety Report will be based on a site-specific TSC operator dose assessment and emergency planning arrangements requirements

  - operational assessments comprising the RPPs which will be required during operations to cover the transport of waste to the GDF based on a prior dose assessment for workers and perhaps the same for the public and emergency planning arrangements requirements

- T3 relates to how the transport safe operating envelope is defined and substantiated through production of DSRs, to specify the analyses that must be undertaken in order to substantiate the DSRs and the methodologies for undertaking those analyses
- T4 relates to the means by which the transport safe operating envelope for designs (including packages, materials and other parts of the transport system) where RWM is the design authority is implemented including:
  - the role of the DSRs in setting requirements for the manufacture, use and maintenance of a package or material including the operating, maintenance and emergency instructions for the packaging, specification of the approved contents of the package, quality assurance requirements in the manufacture, maintenance and use of the package and the maintenance of archive records
  - the role of the RPP which sets out the requirements for prior dose assessment and dose monitoring, identification of key roles and responsibilities, setting of dose constraints and implementation of dose optimisation (through design and operational processes) to ensure that dose levels do not exceed specified limits, emergency response procedures for use in the event of accidents or incidents, requirements for appropriate training and the implementation of a management system which will be put in place in time for transport
- T5 relates to the application of a framework for optimising doses from the transport of radioactive waste to the GDF as applicable to all aspects of risk and therefore covers:
  - generic assessments
  - site-specific assessments including routine operations, anticipated operational occurrences and accident conditions
  - operational assessments
- T6 details how the transport safety documentation supports ensuring that safety and design are integrated through the GDF design development process, in particular, how safety interacts with the design process to ensure that the developing design is fully integrated through a safety assured design process (including human factors integration) for all phases of the GDF lifecycle
- T7 details how suitable arrangements will be required for reviewing ongoing safety and for making changes that may be needed on an immediate or a longer-term basis

6.3.2 The Nuclear Operational Safety Manual

The NOSM has been developed and approved as part of the RWM management system. It describes the processes that will be followed to develop and maintain safety arguments and analyses to demonstrate the safety of the design, development, operation and closure of the GDF. The manual:

- permits the preparation and assessment of safety case documentation required to support the operational phase of the GDF project
- facilitates the maintenance and update of the extant safety documentation as the GDF project develops

- facilitates production of assessments that support the disposability assessment process
- provides a flexible structure that will meet the needs of future licensing stages throughout the lifetime of the GDF up until closure when there will be a handover to the ESC

The purpose of the NOSM is to provide standard procedures, methodologies, criteria and guidance for use in operational safety assessments performed in support of the development of safety cases for the GDF. Beyond that basic remit, it also provides a framework for the management and control of safety cases and details requirements for their assessment. By defining a set of common analytical approaches and a robust safety case management system within the NOSM, the objective is to produce coherent and proportionate safety justifications throughout the GDF's life-cycle up to and including final closure.

Due to the long timescales associated with GDF construction and waste emplacement prior to final closure, the strategy for the development of the NOSM has recognised that, over such timescales, it is likely that regulatory requirements with regard to safety cases and safety assessment will change. As a result, the first issue of the NOSM is intended to support the production of safety documentation identified as being necessary for maintenance and further development of the generic OSC through to the production of site-specific Preliminary Safety Reports documentation for candidate sites. Later issues of the NOSM will therefore be required to cover the analysis required for safety documentation for more developed designs through the operational phase to closure.

The NOSM structure comprises the following 'steps':

- N1 details the safety case management, production and assurance process which sets out:
  - how all safety case documents will be managed
  - how production will be in accordance with defined specifications for each type of safety case
  - how safety cases and the associated activities are categorised on the basis of harm potential
  - how the assurance process will provide the level of 'due process' that assures suitable challenge and barriers to failure that support the right first time safety case objective including specifying the approval route for different categories of document
- N2 sets out the safety assessment process including the identification of hazards, the screening and sentencing of faults for detailed safety analysis, the analysis of faults and comparison of the results of the safety assessment with acceptability criteria based on the following approaches:
  - the assessment of normal operational exposures to the workforce and the public
  - design basis accident analysis which is the deterministic assessment of the design to confirm:
    - it provides sufficient protection against faults by comparison with target criteria
    - it provides a robust demonstration of fault tolerance of the design and of the effectiveness of its safety measures;
    - the basic principle is that, for each identified fault or group of faults, the GDF must have suitable and sufficient safety measures in place to protect against

it where the number and quality of safety measures are both relative to the potential for harm from the fault

- probabilistic safety assessment which allows an assessment of the strengths and weaknesses of a design with complex systems and interdependencies and provides an understanding of the residual risks associated with a design as it includes an assessment of the probability or frequency of failures on a best estimate basis over a wider range of faults for comparison against acceptability criteria and supports the identification of potential ALARP issues
- beyond design basis accident analysis for those faults with a frequency lower than the cut-off for being considered within the design basis and with an unmitigated radiological consequence less than a severe accident, in order to confirm that there is not a rapid increase in abnormal plant behaviour caused by an abrupt transition in the plant status and supports the probabilistic safety assessment to ensure that risks are reduced to ALARP
- severe accident analysis for those faults with the potential to realise very high radiological consequences to operators or members of the public in order to inform the probabilistic safety assessment and the accident management strategy

- N3 relates to the definition and substantiation of the GDF's safe operating envelope in the form of safety functions and requirements that must be met and the safety measures, both engineered and procedural, which prevent, protect against or mitigate the consequences of faults. This is equivalent to the incorporation of the general requirement to adopt the following hierarchy of control:
  - eliminate – the preference is that where possible the hazard shall be removed
  - reduce – hazard shall be reduced if it cannot be removed in that the material is required in order for the process to be undertaken
  - isolate – physical measures put in place to ensure safety
  - control – operating limits and conditions put in place to limit what can be done
  - procedures – written systems of work to tell staff how to keep themselves and others safe
  - discipline – ensuring that staff are trained how to work safely in environments where hazards are present
- N4 relates to the means by which the safe operating envelope is communicated to the users and is implemented including:
  - the engineered and procedural safety measures and the relevant requirements on them including availability, reliability and maintainability of these safety measures throughout the life-cycle
  - the required examination, maintenance, inspection and testing regimes for the engineered safety measures, including any arrangements for the substitution and acceptable outage time of safety measures during maintenance, inspection and repair activities
  - the operating limits and conditions required to ensure that the facility is kept in a safe condition in all plant and operating states and the operational documentation used to record and ensure compliance with these limits and conditions
  - procedural arrangements that demonstrate preparedness to respond to a nuclear or radiation incident

- N5 relates to the application of a robust risk reduction process by which doses and the risks associated with the GDF must be reduced to a standard defined as ALARP through a critical review of proposed or existing provisions to determine whether more can practicably be done to reduce risks. This applies to all aspects of risk and therefore covers:
    - normal operations
    - anticipated operational occurrences
    - fault conditions and accidents
- N6 details how safety and design are integrated through the GDF design development process, in particular, how safety interacts with the design process to ensure that the developing design is fully integrated through a safety assured design process (including human factors integration) for all phases of the GDF life-cycle.
- N7 details how the operators of the GDF will maintain nuclear operational and radiological safety. This includes ensuring that the facility remains adequately safe and that the safety cases are kept up to date throughout the entire facility life-cycle including the need to supplement the safety case by developing knowledge and experience attained subsequently. In addition, in order to demonstrate that all risks associated with a facility are ALARP, this will include the requirement to periodically reassess risks throughout the facility lifetime through the periodic review of safety process

6.3.3 The Environment Safety Manual

The ESM describes the process that will be followed to develop and maintain environmental safety arguments and analyses to demonstrate environmental safety of the GDF during the operational period and the period after surrender of the environmental permit, ie the post-closure phase. RWM will develop and deliver environmental safety documents to support submissions for environmental permits throughout the life-cycle of the GDF. These submissions will include an ESC which addresses the requirements of the EPR 2010 and relevant guidance issued by the environmental regulators (such as the GRA). The ESM sets out the process to be followed in developing and maintaining an ESC, which will be iteratively updated and, as appropriate, refined, to demonstrate that environmental safety requirements have been met at key stages in the planning, construction, operation and closure of the GDF. The ESM also applies to the production of any generic ESC (that is to say not based on specific site information) that is intended to be maintained prior to approval of disposal operations at the GDF.

It will be necessary to demonstrate to environmental regulators an auditable and controlled process for the production, management and review of successive ESCs. The ESM provides the framework supporting this process.

The ESM structure comprises the following ‘steps’:

- E1 details the overall framework for the production, management and control of ESC documents throughout the GDF life-cycle. This includes:
    - procedures for managing and maintaining the environmental safety documents that form an ESC
    - the necessary considerations regarding the structure and attributes of ESCs and the documents they comprise
    - a consistent and logical approach to demonstrating regulatory compliance in ESC documentation

  - a consistent and logical approach to demonstrating that an ESC considers uncertainties that could have a significant effect on the ESC
  - the structure, content and expected audience of ESC documents
  - a categorisation scheme for environmental safety documents that reflects their significance to the environmental safety of the GDF and specifies an approval route for different categories of document
- E2 sets out the overall framework for conducting operational and post-closure environmental safety assessments including the Post Closure Safety Assessment and Operational Environmental Safety Assessment
- E3 sets out the overall framework and sets out the principles to be considered in identifying and defining environmental safety objectives and functions
- E4 provides the framework for the substantiation of environmental safety functions through performance confirmation, taking account of information from monitoring and other operational activities
- E5 provides the framework for reducing environmental risk through optimising the safety of the GDF
- E6 provides the framework for the interaction of ESC processes with other RWM functions, and in particular, the disposal system specification, design, research and site characterisation
- E7 defines the requirements for assessing the impact of new information gained during GDF operations

6.4 Interfaces with the RWM disposability assessment process

The radiological risk posed to operators, the public and the environment during both transport to and operations within the GDF is predominantly from the waste package contents. In order to develop satisfactory transport and operational safety cases, it is essential to have a clear understanding of:

- the nature of the waste as the chemical and physical composition and the quantity and type of radioactive material
- the nature of the waste form in that how the waste is conditioned or treated and/or placed within the waste container to help ensure physical and chemical stability and containment under normal and accident conditions
- the nature of the waste container through its performance under impacts and when exposed to fire and its provisions for safe handling

This understanding is achieved through the Disposability Assessment process. The starting point is the production of generic waste package specifications for each of the different types of waste that will be placed in the GDF. These specifications provide an ‘envelope’ for waste packages that will be compatible with the systems and safety cases for transport to and operations within the GDF. The Disposability Assessment documents themselves will be staged with the assessment covering the conceptual, interim and final stages of submission reflecting the developing level of design and safety assessment.

The issue of a staged Disposability Assessment signifies that future stages of waste management have been considered as part of the waste packaging development process and that the proposed waste package has been assessed to be compliant with defined packaging standards and the relevant safety cases. It also confirms that appropriate records of waste package content and characteristics will be maintained and that packaging will be undertaken under an appropriate quality management system. When

completed, this process increases the confidence in the performance, under both normal and fault conditions, of all the different types of waste package that will be placed in the GDF.

As such, the Disposability Assessment process will specify performance requirements for waste forms and waste packages in order to determine the quality of package, as related to the hazard potential of its contents that can be accommodated within the defined safe operating envelope of the nuclear operational safety assessment. This process will be iterative in that feedback from the RWM operational safety assessment may lead to the identification of further research and/or development and, in some cases, may result in the need to redesign the package or to revisit the design of the GDF and any assumptions relating to its operation.

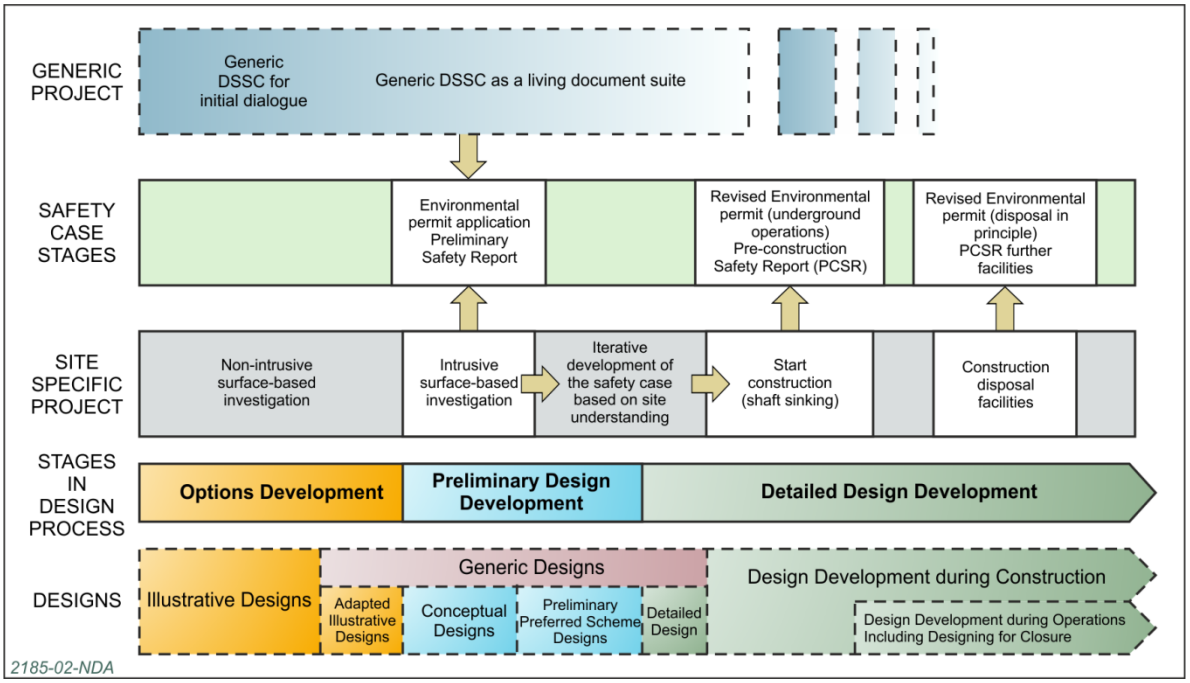
7 Future Safety and Environmental Documentation

7.1 The RWM design process

RWM's design process is set out in the EDM. This document describes the process for developing the engineering design for the GDF, from options development, through preliminary design development, to detailed design development (including design for construction, operation and closure).

The engineering design process has been developed from a review of good practice in design for large infrastructure projects in the nuclear, defence and civil construction industries as defined by the GDF design principles. The design process has been broken down into three main stages – options development, preliminary design development and detailed design development – under which different types of design will be produced. Figure 6 maps these stages to the corresponding phases of the GDF implementation process and to the staged safety case delivery process. The RWM EDM describes how safety considerations are addressed as part of design activities through a safety integrated design process.

Figure 6 Design and Safety Case Stages



Gate reviews provide assurance that the integrated safety and design process is followed, and therefore that every design meets the GDF design principles. These reviews ensure that no project can progress from one stage to the next unless all the key safety and design documentation required for that stage in the process has been produced and taken through due process or the risks associated with proceeding beyond the gate are clearly understood and accepted by the relevant management processes

The gate review at each stage in the project life-cycle checks and confirms that the required deliverables are available and have been appropriately approved. Such deliverables are likely to include design status reports and designs appropriate to the stage of GDF implementation and safety assessments based on the designs. A successful gate review is required before the project can progress to the next stage of the project life-cycle.

The EDM discusses the main gates, which are planned to occur at the end of each design stage (bottom row of Figure 6). The gate review process will include the relevant functional heads (including the Head of Disposal System Assessments), to ensure that design requirements are appropriately considered in safety assessments and that design requirements coming from safety assessments have been factored into the design as appropriate for the stage of the GDF implementation process.

7.2 Future safety case requirements

At each stage of the GDF design development, the generic DSSC together with the future safety case documents within the facility lifecycle, will reflect available knowledge and understanding and will be used to identify where gaps in that knowledge and understanding need to be addressed through further work. The generic DSSC explicitly takes account of uncertainties that may arise from gaps in knowledge which will require further research and development and specific assessments. The generic DSSC will be used to inform the developing design through an integrated design and safety process. As the design and associated safety assessment develops and is based on increasingly more detailed information, the uncertainties will be expected to reduce. The level of confidence in the safety assessment and the generic DSSC will increase when RWM seeks full SLC status and, later on, when permission is sought through formal licence instruments to construct, commission and operate the GDF.

Future safety case requirements will be driven by the design development in accordance with the RWM design process, as set out in the EDM. The safety case requirements for transport, operations and environment are set out in the safety case manuals for the individual stages of the design and facility life-cycle. As such, the safety cases will be developed as the design is advanced in line with the safety case manuals to include more detailed safety analysis and ALARP demonstration and comparison with acceptability criteria. The safety case manuals will be kept under review to reflect changes in regulatory or industry requirements and practices and the developing safety cases will take any such change into account through either the programmed safety case developments or through the periodic safety review process. In addition, the developing safety cases will need to balance safety requirements and ALARP, for example, to ensure that measures applied in the operational phase do not present a challenge to the long term post closure safety case.

Transport safety case documents required from the TSM are:

- the generic TSC including any future updates
- site-specific TSC(s)
- the RPPs
- the DSRs
- context documents to support GDF licensing submissions by providing context on transport and transport safety to regulators and other stakeholders (Preliminary Transport Safety Report(s) and Pre-Construction Transport Safety Report(s))

The safety case strategy for transport is detailed in the transport safety strategy [31].

The safety case strategy for the operational phase of the GDF life-cycle is detailed in the operational safety strategy [32]. As the GDF progresses, there will be increased complexities due to the long period of time with individual sub-facilities in different operational states covering the full range from concept design through to decommissioning and closure. The operational safety strategy takes cognisance of these complexities. This includes future requirements for:

- the generic OSC including any future updates

- generic and site-specific Preliminary Safety Reports as licensing submissions to ONR
- the Pre-Construction Safety Reports as submissions to support and substantiate the detailed design phase and to permit construction activities to commence
- the Pre-Commissioning Safety Reports to permit safety related commissioning
- the Pre-Operational Safety Reports to demonstrate that, based on the design, construction and commissioning, it is safe to operate as a nuclear facility
- the Post Operational Safety Report which may be required at the end of the operational phase to justify a phase of care and maintenance to prepare the facility for decommissioning and closure, including an analysis of any potential impacts of operations on the post-closure ESC
- the Overarching Operational Safety Report which is the top level safety case for the whole of the GDF during the operational phase which identifies the risk from all facilities, operations and services on the GDF site and the controls in place to ensure that risks are reduced to ALARP
- the Decommissioning Strategy which presents the safety strategy for decommissioning, prepared at an early stage which will be subsequently developed into the Decommissioning Plan
- the Pre-Decommissioning Safety Report which demonstrates that the GDF decommissioning and back filling can be carried out effectively and safely; it also covers the potential impact of the decommissioning activities on the ESC for post-closure
- the Pre-Closure Safety Case which brings together all the safety documentation relevant to decommissioning, sealing and closure of the GDF and presents the 'handover state' of the environmental safety functions to the ESC including definition of the end state for the operational phase and demonstrating that it meets the initial state agreed requirements for the post-closure phase

The safety case strategy for environment is detailed in the environment safety case strategy [33] and covers the following safety case documents:

- the generic ESC, including any future updates
- the Initial Site Evaluation which presents mainly qualitative views on the feasibility of constructing the GDF at a candidate site and whether such a facility could meet the principles and requirements of the GRA, sets out how a site-specific ESC might be constructed and demonstrates that any proposed intrusive site investigation will not compromise the integrity of a site to the unacceptable detriment of post-closure safety
- the Preliminary Environmental Safety Evaluation which presents qualitative environmental safety arguments supported by quantitative assessment based on available site knowledge and data and specific designs, demonstrating consistency with the principles and requirements of the GRA and demonstrates that underground operations would not compromise the integrity of a candidate site to the unacceptable detriment of the ESC
- the initial ESC which provides full environmental safety analysis and demonstration through claims, evidence and arguments that the GDF, as designed, would meet the principles and requirements of the GRA

- the Pre-Operational ESC which confirms that the ‘as-built’ GDF meets the criteria defined in the initial ESC and can be commissioned and operated in accordance with the regulator’s waste disposal permit conditions
- the Operational ESC(s) which demonstrates that the GDF continues to meet the regulator’s permit conditions and that any operational changes do not adversely affect this position and it allows issue of variations to disposal permits
- the Post-Operational ESC which demonstrates that the GDF can be closed in a manner that ensures environmental safety and meets conditions for the issue of a closure permit by the regulator
- the final ESC which justifies the acceptability of surrender of the permit and provides full justification and confidence that the site will continue to be environmentally safe and that the risks to future populations will be as low as reasonably achievable for as long as required by the regulator

8 Conclusions

This report describes the process that RWM has used to produce the transport, operational safety and environmental safety cases that support the 2016 generic DSSC. It is considered that this approach is appropriate for the current generic stage of GDF implementation.

This report demonstrates that RWM understands the key aspects of safety cases, the regulatory requirements and expectations for safety cases, the key requirement for effective interfaces between the design team, the safety case team, independent reviewers and regulators. RWM expects to be able to fulfil these requirements as further, more detailed information on the GDF design becomes available as the project proceeds through the site selection process. The report shows where methods and data will be developed in order that the safety cases can fully meet the regulatory principles and requirements.

In order to develop the GDF, it will be necessary to develop a staged series of safety cases to demonstrate to the regulators that the project can proceed through the site studies, surface investigation, underground investigation, construction, commissioning, operational (waste emplacement), decommissioning and closure phases. This report demonstrates that RWM understands when safety cases will be required and the level of detail and scope required for each of these safety cases.

This report demonstrates that RWM understands the legislative and regulatory basis for ensuring the design, construction and operation of a safe facility and the regulatory process that is currently in place. It also demonstrates that RWM understands the regulatory standards and targets for both nuclear and environmental safety and how these will be addressed in the series of safety cases that will be produced for the GDF. The report also describes the methodology that has been used in producing the safety cases that support the DSSC.

In order to produce the safety cases, an appropriate safety management system will be required. This report demonstrates that RWM understands the regulatory requirements for safety management. RWM is currently putting in place a safety management system that will allow it to function as a SLC in the future, thereby satisfying the regulatory requirements for safety management.

A documentation management system will be required to maintain configuration control of the safety cases and supporting documentation. This report demonstrates that RWM understands the requirements for such a system and how it should be implemented. The production of safety cases must be carried out to a consistent format and scope using consistent data. This is achieved through the safety case manuals giving guidance, procedures, methods and data to be used in all safety cases.

Glossary

A glossary of terms specific to the generic DSSC can be found in the Technical Background document.

References

1 Radioactive Waste Management, *Geological Disposal: Overview of the Generic Disposal System Safety Case,* DSSC/101/01, December 2016.

2 Department of Energy and Climate Change, *Implementing Geological Disposal - A framework for the long term management of higher activity waste,* URN 14D/235, July 2014.

3 Radioactive Waste Management, *Geological Disposal: Technical Background to the generic Disposal System Safety Case,* DSSC/421/01, December 2016.

4 Radioactive Waste Management, *Geological Disposal: The 2013 Derived Inventory*, DSSC/403/01, 2016.

5 Radioactive Waste Management, *Engineering Design Manual*, RWM120, Rev 1, 2016 (unpublished).

6 Radioactive Waste Management, *Transport Safety Manual*, RWM14-01, Rev. 0, 2015 (unpublished).

7 Radioactive Waste Management, *Nuclear Operational Safety Manual*, RWM14-31, Rev 0, 2015 (unpublished).

8 Radioactive Waste Management, *Environmental Safety Manual*, RWM14-71, Rev 0, 2015 (unpublished).

9 International Atomic Energy Agency, *Regulations for the Safe Transport of Radioactive Materials*, SSR-6, 2012.

10 Environment Agency and Northern Ireland Environment Agency, *Geological Disposal Facilities on Land for Solid Radioactive Wastes: Guidance on Requirements for Authorisation*, 2009.

11 Office for Nuclear Regulation, *Safety Assessment Principles for Nuclear Facilities*, 2014 Edition, Revision 0, 2014.

12 Office for Nuclear Regulation, *The Purpose, Scope and Content of Safety Cases*, NS-TAST-GD-051 Revision 4, 2016.

13 Charles Haddon-Cave QC, *The Nimrod Review: An Independent Review into the Broader Issues Surrounding the Loss of the RAF Nimrod MR2 Aircraft XV320 in Afghanistan in 2006,* HC1025, 2009.

14 Office for Nuclear Regulation, *Guidance: Licence Condition 14 Safety Documentation, Site Inspection and Enforcement*, NS-INSP-GD-014, Revision 3, 2016.

15 Health and Safety Executive, *The Tolerability of Risk from Nuclear Power Stations*. The Stationery Office, ISBN 0 11 886368 1, 1992.

16 Health and Safety Executive, *Reducing Risks, Protecting People: HSE's Decision Making Process*. HSE Books, ISBN 0 71762151 0, 2001.

17 Radioactive Waste Management, *Radiological Protection Criteria Manual*, RWM02, Revision 2, 2016 (unpublished).

18 Office for Nuclear Regulation, *Licensee Core and Intelligent Customer Capabilities,* NS-TAST-GD-049, Revision 4, 2013.

19 International Atomic Energy Agency, *Safety of Nuclear Power Plants: Design Specific Safety Requirements*, Specific Safety Requirements Series No. SSR-2/1, 2012.

20 NDA, *Geological Disposal: Framework for Application of Modelling in the Radioactive Waste Management Directorate*, NDA/RWMD/101, 2013.

21 Radioactive Waste Management, *Health Safety and Environment Policy Statement*, RWP50, 2015.

22 Office for Nuclear Regulation, *Function and Content of a Safety Management Prospectus; Technical Assessment Guide*, NS-TAST-GD-072, Revision 2, 2013.

23 Radioactive Waste Management, *Safety and Environmental Management Prospectus*, RWSP01 Rev 4.0, 2011.

24 Radioactive Waste Management, *Organisational Baseline Document*, RWSP02, Rev 5.0, 2014.

25 Radioactive Waste Management, *Management of Organisational Change for the Geological Disposal Delivery Organisation*, RWPR01, 2009.

26 Radioactive Waste Management, *GDF Design Principles (Safety, Environmental, Security and Safeguards Principles for the Design Process)*, Technical Note no. 23677920, 2014.

27 International Atomic Energy Agency, *Fundamental Safety Principles*, Safety Fundamentals SF-1, 2006.

28 International Atomic Energy Agency, *Geological Disposal Facilities for Radioactive Waste*, Specific Safety Guide SSG-14, 2011.

29 Nirex, *Nuclear Design Safety Principles*, 1998.

30 Health and Safety Executive, *Risk Assessment – A Brief Guide to Controlling Risks in the Workplace*, INDG163, Revision 4, 2014.

31 Radioactive Waste Management, *Transport Safety Strategy*, NDA Report No. NDA/RWMD/106, 2014.

32 Radioactive Waste Management, *Operational Safety Strategy*, NDA Report No. NDA/RWMD/107, 2014.

33 Radioactive Waste Management, *Environmental Safety Case Strategy*, NDA Report No. NDA/RWMD/090, 2012.

Certificate No LRQ 4008580

Radioactive Waste Management Limited
Building 587
Curie Avenue
Harwell Oxford
Didcot
Oxfordshire OX11 0RH

t +44 (0)1925 802820
f +44 (0)1925 802932
w www.nda.gov.uk/rwm