Radioactive Waste Management

NDA Report no. DSSC/202/01

Geological Disposal

Generic Operational Safety Case - Main Report

December 2016

Radioactive Waste Management

NDA Report no. DSSC/202/01

Geological Disposal

Generic Operational Safety Case - Main Report

December 2016

Conditions of Publication

This report is made available under the Radioactive Waste Management (RWM) Transparency Policy. In line with this policy, RWM is seeking to make information on its activities readily available, and to enable interested parties to have access to and influence on its future programmes. The report may be freely used for non-commercial purposes. RWM is a wholly owned subsidiary of the Nuclear Decommissioning Authority (NDA), accordingly all commercial uses, including copying and re publication, require permission from the NDA. All copyright, database rights and other intellectual property rights reside with the NDA.

Applications for permission to use the report commercially should be made to the NDA Information Manager.

Although great care has been taken to ensure the accuracy and completeness of the information contained in this publication, the NDA cannot assume any responsibility for consequences that may arise from its use by other parties.

ISBN 978-1-84029-541-2.

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 consent-based 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

Introduction

The aim of the generic Operational Safety Case (OSC) is to demonstrate, as part of the generic Disposal System Safety Case (DSSC), that the Geological Disposal Facility (GDF) will be safe and risks will be ALARP during the project's operational lifecycle. This includes consideration of hazards that could be present during the project from the first construction activity up to final closure. The operational safety assessment does not deal with the issues related to transport of waste to the GDF or the post-closure phase; these are addressed in the generic Transport Safety Case (TSC) and the generic Environmental Safety Case (ESC) respectively.

The generic DSSC remains in the early stages of development as the site and design have not yet been chosen. For these reasons, the DSSC and the associated implementation strategy are termed 'generic' because they must:

- cover a range of possible geological environments, and
- recognised that the facility concept designs have only nominal levels of definition

This document is the generic OSC Main Report. It summarises the findings of the safety assessment work undertaken as part of the 2016 generic OSC, and reported in the following volumes:

- Volume 1: Construction and Non-Radiological Safety Assessment
- Volume 2: Normal Operations Safety Assessment
- Volume 3: Accident Safety Assessment
- Volume 4: Criticality Safety Assessment

The assessments are structured around key claims with supporting arguments and evidence in relation to each of the four supporting volumes. The principal claims are related to requirements in the GDF Disposal System Specification derived from the International Atomic Energy Agency (IAEA) Fundamental Safety Principles (SF-1) and adopted into UK regulatory guidance by the Office for Nuclear Regulation (ONR):

IAEA SF-1	Principle 5: 'Optimisation of protection' Protection must be optimised to provide the highest level of safety that can reasonably be achieved.
ONR TAST_GD_004	Fundamental Principle 3, 'Optimisation of protection' Protection must be optimised to provide the highest level of safety that is reasonably practicable.
	Fundamental Principle 4, 'Safety Assessment' Duty holders must demonstrate effective understanding and control of hazards through a comprehensive & systematic process of safety assessment.

Fundamental Principle 3 is aligned to the following principal safety claims (SC) made in this assessment:

Volume 1:	OSC.SC1	All reasonably practicable steps will have been taken to implement design provisions whose function is to prevent or minimise the risk of injury due to conventional hazards.

Volume 2:	OSC.SC2	All reasonably practicable steps will have been taken to implement design provisions whose function is to prevent or minimise routine exposures to radiation sources.
Volume 3	OSC.SC3	All reasonably practicable steps will have been taken to implement design provisions whose function is to prevent or mitigate the consequences of radiation accidents.
Volume 4	OSC.SC4	All reasonably practicable steps will have been taken to implement design provisions whose function is to prevent or mitigate the consequences of nuclear accidents (ie unplanned criticality).

The process adopted in developing the safety assessment is built around the Health and Safety Executive (HSE) ‘five steps’ process for undertaking risk assessment. These are detailed below:

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

The assessment reported here has been undertaken in accordance with the RWM Nuclear Operational Safety Manual (NOSM), the need for which is aligned to Fundamental Principle 4. A full and definitive assessment will be prepared prior to seeking regulatory approval for construction, as required by Site Licence Conditions (in particular LC14), when a specific site has been selected. The contents and methods of the NOSM are similar to those in place at operating civil nuclear sites and meet industry best practice for the assessment of normal operations, radiological faults and criticality. At this generic stage, its application has two aspects:

- top-down – the focus is on identifying significant issues and what needs to be addressed in the developing design
- bottom-up – a demonstration that the assessment process has been followed systematically

Additional steps have been identified for implementation by RWM including safety case documentation management and production, interaction with the design process and continued maintenance of safety.

The detailed assessments discuss the nature and origin of hazards and the means by which safety of workers or members will be ensured. The solutions are derived from consideration of the following hierarchical principles:

- can the hazard or risk of harm be eliminated by modification of the engineered design or the process itself?
- if the hazard or risk of harm cannot be eliminated, what measures could be incorporated into the developing design to:
    - provide a means of preventing the outcome
    - provide a means of protecting those affected
    - provide a means of reducing the consequences

The systems that will ensure safety may be engineered or operational/procedural, and active or passive in their delivery of the safety function. Engineered systems are preferred to procedural controls; equally, passive systems are preferred to active systems.

It is important to recognise the role and the status of the generic OSC; it is not a safety case as would be expected to ensure compliance with the requirements of a nuclear site licence (e.g. LC14 - Safety Documentation). Full compliance with all relevant criteria will require collation of detailed requirements and acceptance criteria prior to commencing design development, development into structured design principles and demonstration of compliance in a Design Justification Report.

The production of safety case documents to meet the requirements for a nuclear site licence will occur in line with the permissioning requirements set out in UK law when a specific site has been identified and will be supported with the commensurate level of design and substantiation. Thus the current OSC represents a demonstration of capability and provides a foundation for future development that will follow the major steps in the GDF Programme.

A systematic and proportionate hazard identification study has been undertaken based on the current Basis of Assessment, which describes the GDF as a functional process flow description (PFD) and a high level description of activities, plant, equipment and tasks, which could be used to implement the required functions. The following structured approach has been followed:

- development of a functional process flow description (PFD) to task level for emplacement of all waste package types
- application of a systematic assessment to identify operability requirements, inherent hazards (Volume 1 and Volume 2) and potential faults (Volume 3 and Volume 4)
- development of a hazard listing and fault set which without controls could result in harm to operators or members of the public
- qualitative or quantitative assessment
- development of hazard management strategies and conceptual safety functions to demonstrate that safe operation is feasible
- review of the illustrative designs to identify priorities for optimisation to support the full and definitive assessment

The nature and scope of the assessment is consistent with the current stage of the GDF programme. At the current generic stage, the plant and task design is not expected to be sufficiently detailed to support a full and definitive assessment. As such conclusions can only be drawn consistent with the nature of the assessment. This precludes any definitive statement in relation to final acceptability. Rather, the current objective is to demonstrate that the control of all hazards is credible and the means of control is feasible to implement. This underpins the fundamental claim that a GDF will be safe to operate and construct in the future when a suitable site has been identified.

The generic DSSC builds on more than 30 years of experience studying geological disposal and undertaking safety assessments in the UK. It also recognises the UK's excellent safety record relating to the safe movement and interim storage of radioactive waste packages in existing facilities on nuclear licensed sites. Furthermore, it also draws on the extensive body of knowledge and experience in other countries gained through similar radioactive waste management programmes.

During its construction and operation, the GDF will share many features not only with large-scale sub-surface operations but also with other large-scale construction projects undertaken for high-hazard industries in the UK and overseas. As such, the GDF needs to consider potential hazards common to many industrial operations subject to a 'permissioning regime' (for example, nuclear, railways, offshore and onshore major hazard industries).

The approach to the specific assessments, and their findings and forward actions, are described in the following sub-sections.

Construction and Non-Radiological Safety Assessment

The focus of the conventional safety assessment is on development of credible hazard management strategies. Early identification of such issues and planning for resolution will ensure adoption of design principles to inform future design development and optimisation. Twelve high-level conventional generic fault sequence groups (CgFSGs) have been derived and considered in the assessment:

- C1: workplace transport
- C2: working and load at height
- C3: structural collapse
- C4: plant/machinery
- C5: fire and explosion
- C6: projectiles and blast, over-pressure
- C7: airborne hazardous substances and air quality (including asphyxiation)
- C8: flooding
- C9: electrical
- C10: noise and vibration
- C11: concurrent activities (also referred to as ‘conflict hazards’)
- C12: occupational

The safety assessment concludes that the following conventional fault groups are the most significant in terms of potential for harm during the construction phase:

- structural collapses underground including rockfalls
- fire and explosions (in particular in the underground environment)
- flooding (in particular in the underground environment)
- transport accidents
- air quality underground

For CgFSGs, the relevant legislation (or relevant good practice) and high level health and safety requirements have been compiled. These will form the basis from which the hazard management strategy will be developed, with the emphasis being on hazard elimination. This will also include consideration of design provisions that allow the GDF to be designed to be ‘passively safe’ during the operational phase. Work during the construction phase, such as installing rock support systems, will also ensure the facility is ‘passively safe’. Compiling the high level health and safety requirements has also identified general expectations, placed on the duty holders under the key legislation and recognises the role of relevant good practice and/or guidance from the HSE or industry bodies.

Normal Operations Safety Assessment

The focus of the normal operations safety assessment is on identifying activities that need to be optimised or supported with engineering design features to ensure safe operation. The standard mechanisms by which the GDF operators, other on-site workers and members of the public could receive a radiological dose as a result of normal operations are:

- external radiation in the form of a direct dose
- internal radiation such as inhalation of particulate material or gaseous discharges as a result of activities on the site

The assessments have been undertaken for bounding throughput years and assumptions regarding worker groups and the tasks in the PFD that they undertake.

The key findings of worker dose assessment are:

- The assessment of doses to workers can now be clearly linked to tasks, worker group, waste stream, package, location and schedule through the structure of the PFD. This represents a significant improvement in capability since the 2010 generic DSSC.
- There is now the capability to identify those areas of the GDF where effort most needs to be focussed on optimising the design, and those areas where there is lack of clarity related to process needs, such as definition of task requirements to be performed by the operators.
- No requirements have been identified that cannot be satisfied through implementation of standard nuclear industry solutions.
- Annual doses to a member of the public from aerial discharges, based on peak gas releases during the operational period, are predicted to be acceptable.

The key finding of the public dose assessment is:

- The total dose to members of the public from peak gas releases during the operational period is predicted to be significantly below the legal limit for members of the public. This is based on the Basis of Assessment report, with conservative assumptions appropriate to this generic stage.

As a result of this assessment a number of areas of work have been identified to further underpin the claims of feasibility. All identified work areas relate to formal design development to be completed at later stages of the GDF programme. The general themes are summarised as:

- Design optimisation including ‘time and motion’ studies to demonstrate that the assumed design throughput is viable. The output from this study is linked to the accident safety assessment assumptions (ie the initiating event frequencies)
- Development of a set of normal operations design safety principles

The GDF will require a full and definitive assessment to support selection of suitable sites and gain regulatory approval for the initial site specific investigation, this will include:

- An assessment of anticipated operational occurrences when supported by the appropriate level of process and design definition

A detailed site-specific offsite (public) dose assessment reflecting the combination with local environmental factors and the location and habits of exposed groups.

Accident Safety Assessment

The accident safety assessment has included seven Hazard Analysis (HAZAN) groups derived from the preliminary fault schedule. Each assessment considers the most significant potential faults for all waste types (if relevant). The fault set assessed within the generic OSC represents scenarios of significance and relevance to the current stage of the GDF programme, demonstrating feasibility. In addition, this fault set informs the development of the basis of disposability. The HAZANs cover the following issues:

HAZAN 1: Loss of Shielding, due to system or operator error resulting in unintended exposure to waste package contents

HAZAN 2: Loss of containment, due to disturbance, accumulation or transfer of contamination

HAZAN 3: Dropped load and impacts, resulting in loss of integrity of shielding and loss of containment due to impact of waste packages or facility

HAZAN 4: Fire, initiated by process or system failures

HAZAN 5: External hazard, initiated by offsite failures (not under the control of the operator (air/ground/offsite))

HAZAN 6: Internal hazards, initiated by onsite failures (under the control of the operator (including fire)) that impact on delivery of other safety functions

HAZAN 7: Criticality, faults initiated by geometry changes, addition of moderator or additional reflection, movement and accumulation of fissile material and out-of-specification packages

Options for risk reduction have been identified for all faults subject to Design Basis Accident Analysis (DBAA). They are presented in terms of engineered safety measures already implemented, planned for use or in use for comparable operations. This demonstrates that the means of meeting risk reduction targets are credible and feasible to implement and can be used to influence the direction of travel of the developing design activities.

The baseline set of external hazards applicable to the GDF in the UK has been identified and, where possible, illustrative design basis event magnitudes defined. In addition, combinations which occur simultaneously or nearly simultaneously (correlated hazards) have been identified. The external hazards, including correlated hazards, provide a basis that will be taken into account as the siting process and GDF design develops. The bounding external hazards fall into the following groups:

- external (natural) hazards, such as high wind load, high precipitation, snowfall and extreme temperatures
- external (man-made), such as hazards presented from adjacent site or facilities
- seismic events
- flooding of sub-surface facilities induced by, for example, a seismic event

As a result of this assessment a number of areas of work have been identified to further underpin the claims of feasibility. These relate to the most significant hazards which will require control during construction and operation. The general themes relate to:

- technology transfer and design development of shaft and drift systems
- optimisation of vault designs to eliminate or reduce potential for faults
- optimisation to eliminate or reduce deleterious effects of fires and explosions
- management and control of sources sub-surface flooding and minimisation of secondary effects (loss of services or damage)
- understanding and proving stability and longevity of sub-surface structures
- development of a strategy for limiting risks from concurrent construction and operational activities

The GDF will require a full and definitive assessment to support selection of suitable sites and gain regulatory approval for the initial site specific investigation, this will include:

- detailed assessment of internal and external hazards at an appropriate stage of design maturity aligned to regulatory expectations
- assessment of all faults and definition of all safety functions required to satisfy all hazard management strategies

Criticality Safety Assessment

The criticality safety assessment is focussed on identifying those areas that could introduce a risk of criticality during the operational phase. The assessment is qualitative and limited to consideration of failures controls on the packaging of wastes in combination with faults during the operational phase that could result in a criticality event.

Design basis fault scenarios have been reviewed and only double contingencies of failure (requiring two unlikely, independent, concurrent changes in the conditions essential to criticality safety to occur) could result in criticality. The likelihood of such scenarios is currently judged to be very low. The packaging design (which includes the waste quantity, form, configuration and its behaviour in accident scenarios) aims to reduce the risk of a criticality event. The failure of controls on waste packages would not be reasonably expected to result in a critical configuration arising in the GDF, either in individual packages or in combination. The nature of normal operations would not reasonably be expected to result in a change of configuration from sub-critical to critical, not least because of the relative immobility of waste inside most packages and the robustness of the packages themselves.

The preliminary assessment also indicates that a criticality warning system is unlikely to be required in the GDF. However it is acknowledged that the design will need to be further developed in order to optimise criticality safety provisions within the GDF.

Overall, this assessment concludes that the likelihood of criticality events during normal operations and under design basis fault scenarios is acceptably low. Based on relevant good practice and UK nuclear site licence operational experience, no significant obstacles have been identified where claims of future compliance against targets, tolerability of risks and ALARP are being made. This will be further considered as part of the design development which will include the requirement to ensure that appropriate optioneering, design optimisation and risk reduction have been applied throughout the design development process. This claim is subject to further design development and safety assessment and the resolution of the Forward Action Plans (FAPs).

Summary of findings

The generic OSC concludes that the GDF will be safe to construct and operate. The main findings that support this claim are:

- credible hazard management strategies can be developed to ensure that risks to workers and members of the public will be tolerable and ALARP
- the means of meeting these needs are not novel; they are based on technology available now that delivers tried and tested above ground solutions in a below ground environment
- the means of ensuring packages meet GDF requirements is already in place and operating through the Disposability Assessment process

Areas of future work to support design development and the preparation of the full and definitive assessment are defined in the FAPs. The general themes, which act as signposts for future design development, relate to establishing design requirements and assumptions, developing hazard management strategies and setting detailed design principles. Specific findings for each area of the assessment are:

Construction and non-radiological assessment:

- Hazard management strategies will need to be developed and design principles defined, and these will be implemented by means of the design and safety integration approach. It is expected that the identified hazards will not warrant further consideration as design basis accidents in the operational phase.
- Sufficient confidence has been gained that the most significant conventional and non-radiological hazards have been identified, and that it will be possible to put in place sufficient and adequate controls and arrangements for the management of these hazards. As such no challenges to the feasibility of constructing and operation the GDF are expected.

Normal operations safety assessment:

- Optioneering and design development will be required to optimise normal operational procedures. This will required improvements in the data and assumptions used in the assessment.
- The assessment has provided a high level of confidence that a means of meeting the safety demands placed on the GDF are feasible (with today's technology) and that the GDF will be safe to operate.

Accident safety assessment:

- Optioneering and design development will be required to provide confidence that RWM accident safety criteria will be met. The design development will include the adaptation of existing technology to GDF underground facilities.
- The most challenging internal hazards identified are internal fires and explosions leading to damage to infrastructure, structures, waste packages or loss of services; internal flooding resulting in loss of services and rockfalls as a result of construction activities. The hazard management strategies will set out the safety requirements to be implemented in the design, such as exclusion, segregation and minimisation to ensure that potential impacts are removed entirely or, in the event that they cannot be eliminated, are negligible.

Criticality safety assessment:

- The GDF will be designed and operated safely with regard to criticality hazards and plans for resolution of identified issues are in place. The nature of the waste material is inherently unfavourable to criticality and the failure of controls on waste packages would not result in a critical configuration, either in individual packages or in combination.
- Further work has been identified to confirm that procedures, processes and controls are sufficiently comprehensive and robust, and that base assumptions related to package criticality limits can be verified from measurements or records.

In broad terms the processes and operations conducted at a GDF are functionally the same, or very similar, to those undertaken at numerous HAW Storage and Handling Facilities in operation in the UK ie the sites that will be consigning packaged wastes to the GDF. Safety cases and ALARP arguments for the operation of such existing facilities are mature, the engineered systems required to reduce risks are well understood and as such future work will be focussed on implementing a proven solution within an engineered underground facility. This current UK experience, along with international GDF experience, gives very high confidence that a suitable design solution can be developed such that the GDF can be operated safely. The design will need to consider the specific requirements of operating a nuclear facility in the sub-surface environment, which may present certain challenges which are relatively unique but are not expected to require novel technological solutions. The areas which require further work to fully underpin the principle claim are largely related to actual design development and the resolution of the FAPs.

List of Contents

Preface iii

Executive Summary v

1 Introduction 1
1.1 The generic Disposal System Safety Case 1
1.2 Introduction to the generic Operational Safety Case Main Report 2
1.3 Objective 4
1.4 Scope 4
1.5 Document structure 6

2 Regulations and Criteria 9
2.1 Regulatory context 9
2.2 RWM safety objectives 10

3 Safety Strategy and Approach 13
3.1 Summary 13
3.2 Stages of the safety case 14
3.3 Data underpinning the safety assessment 15
3.4 Design and safety integration 16
3.5 Application of the safety case to waste packaging 18

4 Safety Assessment Basis 19
4.1 GDF design 19
4.2 GDF operations 19
4.3 Scope and status of assessment 21

5 Safety Assessment 27
5.1 Volume 1: Construction and Non-Radiological Safety Assessment 27
5.2 Volume 2: Normal Operations Safety Assessment 34
5.3 Volume 3: Accident Safety Assessment 41
5.4 Volume 4: Criticality Safety Assessment 53
5.5 Multiple or paired consequences from accidents 59
5.6 Relevant industry experience 60

6 Implementation 63
6.1 Packaging advice 63
6.2 Forward actions 63

7 Conclusions 67

References 71

Glossary 73

Appendix A Forward Action Plan Listing (Volumes 1 to 4) 75

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 References to Government mean the UK Government including the devolved administrations of Wales and Northern Ireland. Scottish Government policy is that the long term management of higher activity radioactive 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.

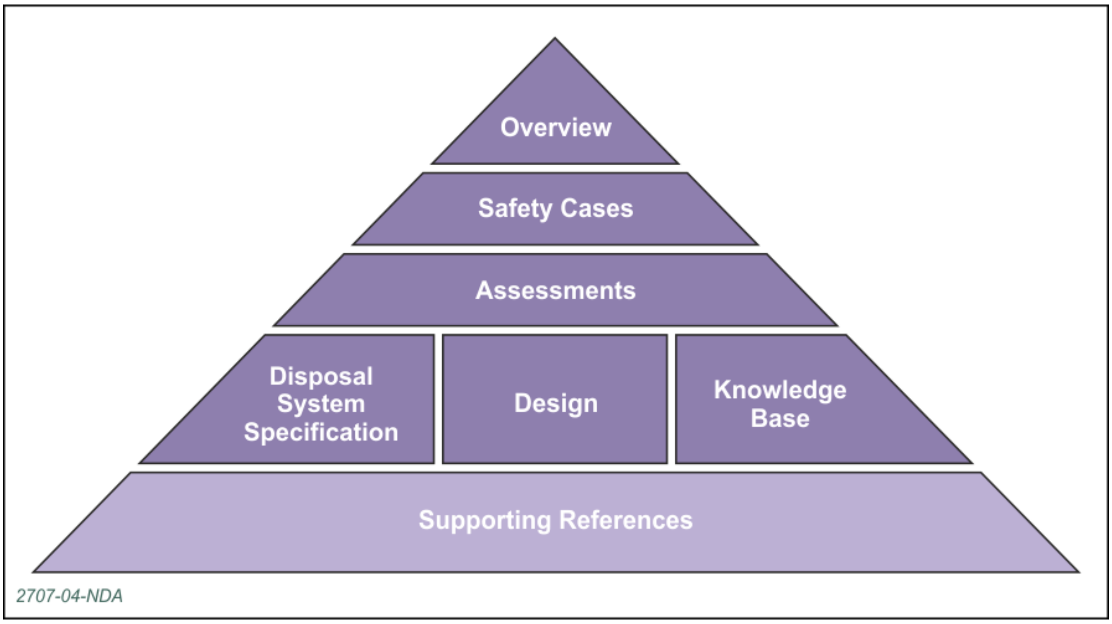
High-level information on the inventory for disposal, the illustrative disposal concepts and other aspects of the disposal system is collated in a technical background document (the Technical Background) [3] that supports this generic Disposal System Safety Case.

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 generic Operational Safety Case Main Report

This document is the generic Operational Safety Case Main Report. It summarises the findings of the safety assessment work undertaken as part of the 2016 generic OSC, and reported in the following volumes:

- Volume 1: Construction and Non-Radiological Safety Assessment [4]
- Volume 2: Normal Operations Safety Assessment [5]
- Volume 3: Accident Safety Assessment [6]
- Volume 4: Criticality Safety Assessment [7]

This Main Report and the 4 volumes make up the generic OSC. The Main Report acts as a 'head document' for the generic OSC, providing sufficient detail to inform the reader of key hazards, design requirements and other safety case outputs so that the reader does not need to review the detailed safety analysis reported in the underpinning reports.

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

This document updates and replaces the 2010 generic OSC published as part of the 2010 generic DSSC.

This report is supported and informed by:

- the Engineering Design Manual (EDM) [8] and associated procedures
- the safety case manuals which includes the Nuclear Operational Safety Manual (NOSM) [9] for the generic OSC
- the generic Disposal Facility Designs [10] and generic Transport System Designs [11]
- revised policies and procedures governing the collection, use and management of models and data for the assessments

The generic OSC considers the GDF at its generic stage of development. It has been developed in accordance with the NOSM, the need for which is aligned to Principle 4 of the International Atomic Energy Agency (IAEA) Fundamental Safety Principles [12] (see below). In the future, site-specific OSCs will be required to demonstrate compliance with Site Licence Conditions (LC14). The contents and methods of the NOSM are similar to those in place at operating civil nuclear sites and meet industry best practice for the assessment of normal operations, radiological faults and criticality. At this generic stage, its application has two aspects:

- top-down – the focus is on identifying significant issues, what needs to be done and addressed in the developing design
- bottom-up – a demonstration that the assessment process has been followed correctly albeit on a smaller scope

The assessment is structured around key claims derived from requirements in the GDF Disposal System Specification, derived from the IAEA Fundamental Safety Principles (SF-1) and adopted into UK regulatory guidance by the Office for Nuclear Regulation (ONR):

IAEA SF-1 [12]	Principle 5: 'Optimisation of protection' Protection must be optimised to provide the highest level of safety that can reasonably be achieved.
ONR TAST_GD_004 [13]	Fundamental Principle 3, 'Optimisation of protection' Protection must be optimised to provide the highest level of safety that is reasonably practicable.
	Fundamental Principle 4, 'Safety Assessment' Duty holders must demonstrate effective understanding and control of hazards through a comprehensive & systematic process of safety assessment.

Fundamental Principle 3 is aligned to the principal claims made in the generic OSC, as listed in Section 5.

Volume 1:	OSC.SC1	All reasonably practicable steps will have been taken to implement design provisions whose function is to prevent or minimise the risk of injury due to conventional hazards.
Volume 2:	OSC.SC2	All reasonably practicable steps will have been taken to implement design provisions whose function is to prevent or minimise routine exposures to radiation sources.
Volume 3	OSC.SC3	All reasonably practicable steps will have been taken to implement design provisions whose function is to prevent or mitigate the consequences of radiation accidents.
Volume 4	OSC.SC4	All reasonably practicable steps will have been taken to implement design provisions whose function is to prevent or mitigate the consequences of nuclear accidents (ie unplanned criticality).

Each volume presents supporting arguments and detailed evidence in relation to derived and subsidiary claims.

1.3 Objective

The generic OSC is not presented as a full safety case in the context of the Nuclear Installations Act (NIA). Rather, the generic OSC is a feasibility study to inform future design development and identify any challenges to feasibility that require resolution in order to give high confidence of successful permissioning at the site selection stage.

The objective of the generic OSC Main Report is to summarise the process by which safety arguments have been developed and the manner in which claims will be demonstrated and substantiated. Where hazard management strategies have been identified but are not yet adopted evidence is presented that implementation will be feasible at the appropriate time. This is achieved through a structured set of claims, arguments and evidence through which the Main Report concludes that the GDF, when constructed and operated, will meet regulatory expectations and RWM safety criteria, as set out in the Radiological Protection Criteria Manual [14] and adopted in the NOSM.

Thus, the generic OSC does not undertake a full and definitive assessment that would be required to support regulatory permissioning. Its scope is limited to illustrative assessments for normal operations and accidents. These are based on the identification and assessment of the most significant hazards, which are those associated with the most demanding design requirements. In addition, ‘pinch points’ in the emplacement process are identified, where current assumptions in the design and throughput requirements would require an unfeasible number of operator hours to complete a task. This identifies areas where the greatest benefit can be realised in terms of risk reduction and demonstration of feasibility.

Issues will require recording, prioritisation and management, for example where the evidence to support a claim is reliant on a feasible risk mitigation strategy. Evidence in many cases will be derived from GDF projects being undertaken by international Waste Management Organisations. RWM is engaged in many international collaborative projects focussed on the safety of geological disposal. Issues identified at the generic stage to be addressed at an appropriate later stage are collated in Forward Action Plans (FAPs) for resolution as part of detailed design developments and assessment. FAPs are presented in Section 6.2 and Appendix A .

1.4 Scope

The scope of the 2016 generic OSC covers:

- process or task-related hazards during construction
- process or task-related hazards during receipt of transport consignments onto the GDF site through to emplacement of disposal units (see Figure 2)
- other events on or offsite that could challenge safety systems or introduce additional hazards through domino effects

The scope does not cover operations associated with:

- active or inactive commissioning of as-built systems prior to approval for operation
- backfilling, decommissioning, sealing and closure which do not involve the handling of waste packages (the backfilling process has however been considered within the hazard identification studies as a potential hazard initiator, for example, by introducing the potential for flooding)

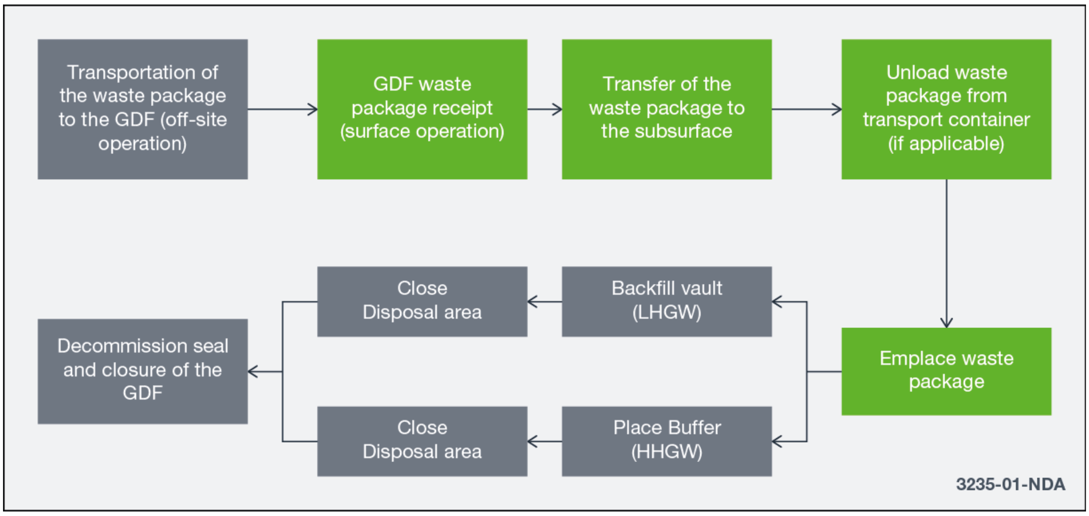
Any meaningful consideration of backfilling and decommissioning requires the decommissioning strategy to be available and the means of backfilling to be specified; this is currently planned for the Preliminary Safety Report stage. The opportunity to challenge the safety functions during this phase of GDF operation is very limited, the facility being passively safe if all other design requirements were implemented. RWM is currently working to improve the state of knowledge on backfilling, sealing and closure which will ensure that optimisation is able to minimise the operational safety impacts of the selected backfilling strategy.

Transport of radioactive waste packages to the GDF is assessed within the generic Transport Safety Case [15] and post-closure evolution of the GDF is covered in the generic Environmental Safety Case [16]. These topics are therefore not within the scope of the generic OSC.

The generic OSC does not assess operational activities relating to surface-based investigations, for example, office safety or borehole investigations, which will be dealt with by workplace risk assessments prepared in accordance with the Management of Health and Safety at Work Regulations 1999.

In addition, the generic OSC does not address security requirements; a security assessment will be addressed through specific documentation as part of the security justification required for the GDF.

Figure 2 Overview of Operations Covered by the generic OSC



1.5 Document structure

The suite of documentation prepared for the generic OSC provides the underpinning evidence in support of principle claims. This includes:

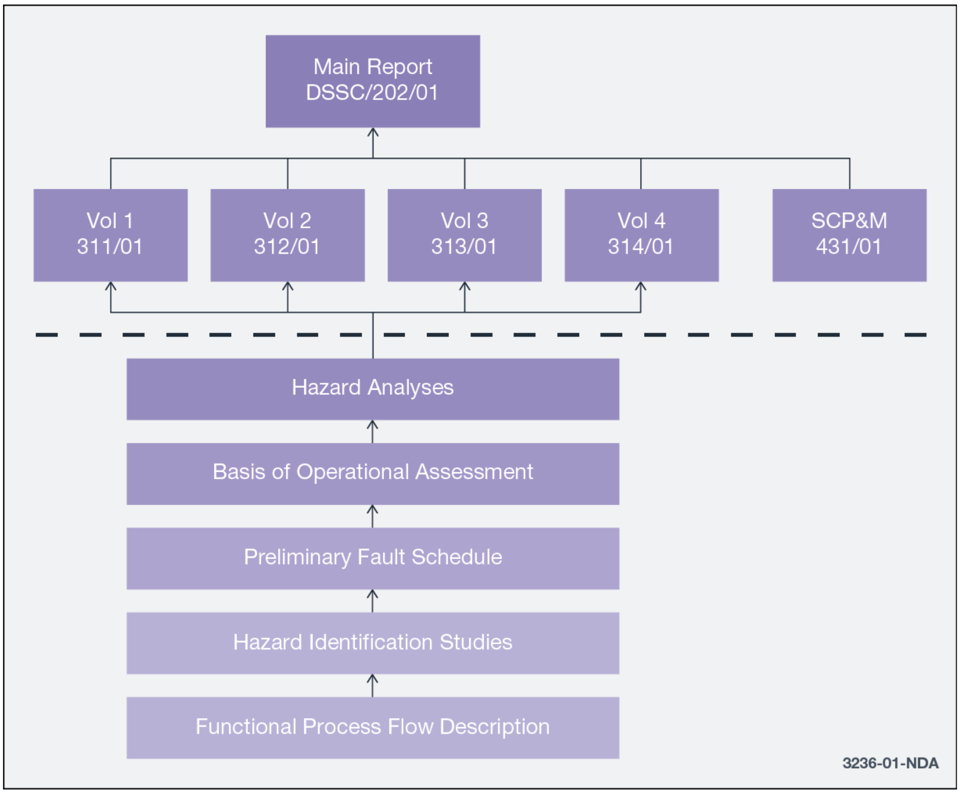
- Basis of Assessment
- Hazard Assessment Summary
- Hazard Analysis
- Fault Schedule with Integral HAZID records

This provides an auditable trail so that the conclusions drawn in this Main Report can be linked back to the nature and reason for the assessment and any evidence provided in relation to a claim of feasibility. The high-level development steps that have been followed are shown in Figure 3 and aligned to the process defined in the NOSM. The documents above the dotted line represent the published documents of the generic OSC while those below the dotted line contain the underpinning information and detailed technical safety assessments. In particular, these documents underpin volumes 2 and 3 as the detailed safety assessments. These underpinning documents have not been published as they carry an enhanced security classification.

The remainder of this report is summarised, by section, below:

- Section 2 presents the principal regulatory requirements relevant to the generic OSC and the criteria against which success will be measured, both for the safety case and the underpinning safety assessments.
- Section 3 describes the role of the generic OSC in the operational safety strategy in the context of a design and safety integrated (DASI) approach to GDF implementation.
- Section 4 describes how the safety assessment has been structured and derived from a functional process flow description (PFD) of the GDF, and details the nature of any limitations of the safety assessments, given the current stage of GDF programme.
- Section 5 presents the results of the construction and non-radiological, normal operations, accidents and criticality safety assessments. It links fundamental principles to claims, arguments and evidence. The assessments are supported by relevant experience from UK licensed waste handling facilities and international geological disposal projects.
- Section 6 describes how the generic OSC assessments will provide the basis for packaging advice given by RWM through the Disposability Assessment process, and input to future design development.
- Section 7 summarises the assessments undertaken, the results and conclusions.

Figure 3 Overview of the generic OSC Structure



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

2 Regulations and Criteria

2.1 Regulatory context

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

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 Management of Health and Safety at Work Regulations 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.

The Construction (Design and Management) Regulations 2015 cover the management of health, safety and welfare when carrying out construction projects, including the design. These regulations are not yet applicable to the GDF as the project has neither been notified nor are formal design activities are being undertaken. However relevant good practice will be adopted to support ongoing work activities.

In addition to these regulations, there may be specific legislative drivers specific to sub-surface operations which may impact on the GDF, including aspects of UK mining regulations which may form part of 'relevant good practice'.

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. As with construction activities, 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 certain nuclear operations some legislation is focussed on and specific to the nuclear industry, notably the NIA 1965. Additionally, there may be nuclear regulations made under the Energy Act 2013 that are also relevant, as well as regulations under the HSAWA such as the Ionising Radiations Regulations 1999 and the Radiation (Emergency Preparedness and Public Information) Regulations 2001.

Furthermore, regulatory bodies in the UK have published guidance on their expectations for safety cases for nuclear facilities:

- Office for Nuclear Regulation (ONR) Safety Assessment Principles (SAPs) [17]
- ONR Technical Assessment Guide for safety cases [18]
- 'learning from experience' including the aftermath of the RAF Nimrod accident and the subsequent inquiry led by Charles Haddon-Cave QC [19]

The ONR SAPs present the key principles expected in a safety case for a nuclear facility, with supporting guidance and numerical safety criteria and targets. These are used as the basis for the assessment of the safety of nuclear facilities and relate specifically to nuclear safety and radioactive waste management.

2.2 RWM safety objectives

2.2.1 Safety case objectives

The safety case objectives are set out in the generic DSSC Safety Case Production and Management report [20] with statements on how the requirements will be met. A summary of the general requirements of safety cases is provided in the following paragraphs:

- the safety case shall be intelligible and structured logically to meet the needs of those who will use it
- the arguments developed in the safety case shall be supported with verifiable and relevant evidence (documented, measurable, etc)
- the safety case shall demonstrate that the GDF will conform to good nuclear engineering practice and sound safety principles, including defence-in-depth and adequate safety margins
- the safety case shall present a balanced account, taking into consideration the level of knowledge and understanding, and the level of attention and analysis applied shall be commensurate with the hazards and risks
- the safety case shall accurately represent the current status of the GDF design in all physical, operational and managerial aspects and will demonstrate that the GDF will remain safe throughout a defined life-time:
    - o the generic OSC is being developed from first principles in order to identify safety functions, associated conceptual safety functional requirements and illustrative risk reduction measures which would be expected to meet the targets set out in the NOSM
    - o subsequent updates of the safety cases will contain additional design detail which will justify that the selected design solutions meet the RWM safety criteria
- the safety case, for the determined period, shall 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:
    - o at this stage of the GDF design the requirement is to identify: safety functions, conceptual safety functional requirements and some conceptual safety measures. This enables the follow on development of suitable design solutions
    - o a demonstration is required that it will be feasible to make an ALARP case when the safety case and design are sufficiently mature
- RWM shall retain ownership of the safety case as the design authority and intelligent customer, notably so where reliance is placed on the external supply chain to ensure that the safety case meets its objectives:
    - o arrangements have been made and implemented to ensure ownership within RWM through management of the safety case elements

It should be noted that some of these objectives are directly relevant to the generic OSC while others will be more relevant to later safety cases.

As part of RWM's management processes, assurance that these requirements are met is delivered through:

- RWM ensuring that the safety case provides challenges to the design rather than arguing to justify the status quo for the design:
  - the means of assurance is internal verification and independent expert advice, which includes the requirement to review all deliverables to ensure that they satisfy this requirement
- the monitoring and auditing of the safety case, which examines both the process of safety case production and its content and ensures that learning from experience is facilitated and applied to future development:
  - learning from experience is built into the project delivery and review process and will be applied to the 2016 generic DSSC update
  - a formal change process to control the development of the DSSC between major safety campaigns

2.2.2 Safety assessment criteria

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

- the RWM Radiological Protection Criteria Manual [21] which sets out 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, 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 sets out the safety criteria and targets for:
  - normal operations doses for operators, other on-site workers and members of the public
  - design basis accident criteria and targets for operators and members of the public
  - probabilistic safety assessment criteria and targets for operators and members of the public
  - severe accident analysis criteria for societal risk (if appropriate for the GDF)

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 GDF Design Principles [22] which were developed to conform to current best practice, including:
  - the IAEA Fundamental Safety Principles [12]
  - the IAEA Safety Requirements for the Geological Disposal of Radioactive Waste [23]
  - the ONR SAPs

    - the Environment Agency's Guidance on Requirements for Authorisation for geological disposal facilities on land for solid radioactive wastes [24]
    - review of previous Nuclear Design Safety Principles [25]
- the RWM EDM which describes the process to be used to establish, maintain and update engineering designs for the development of the GDF

RWM has developed safety case manuals to demonstrate to the regulators an auditable and controlled process for producing safety cases and the associated safety assessments. The NOSM provides standard procedures, methodologies, criteria and guidance for use in the safety assessments that underpin OSCs for the GDF and takes due account of regulatory guidance and expectations. It applies to the design, development, construction, operation and closure of the GDF.

The NOSM does not fully cover conventional hazards; it does however cover the identification of hazards and generation of hazard management strategies and design principles, and this is appropriate for this stage. A requirement for a conventional safety manual has been identified to support detailed design and full assessment, and is addressed within FAP.2016.MR.02.

3 Safety Strategy and Approach

3.1 Summary

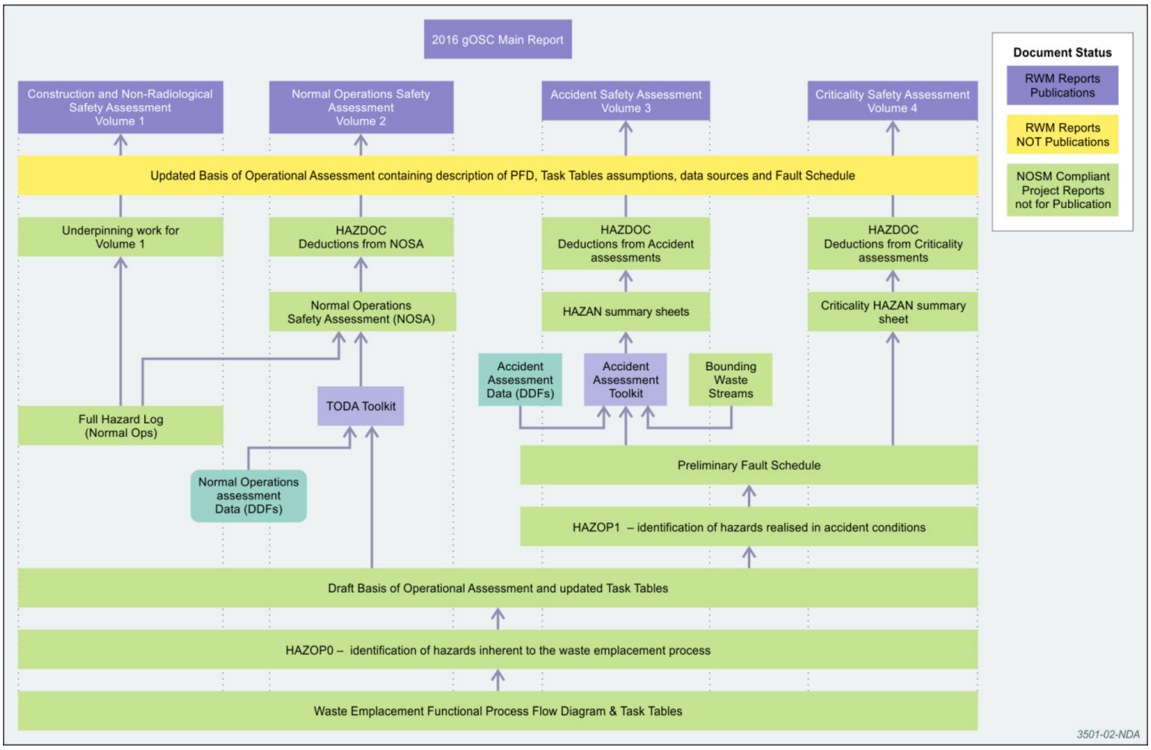
The safety assessment process adopted within the NOSM is built around the Health and Safety Executive (HSE) 'five steps' process for undertaking risk assessment [26]. These steps and the relevant sections of the NOSM and generic OSC which address them are detailed in Table 1.

Table 1 Safety Assessment Process

<table>
<tr><th>HSE Step</th><th>RWM Process</th><th>Generic OSC Reports</th></tr>
<tr><td>Step 1: Identify the hazards</td><td>Hazard identification (NOSM N2.1)
Screening and grouping (NOSM N2.2)</td><td>HAZOP 0 & 1 Study Reports (radiological hazards)
Full Hazard Log
Preliminary Fault Schedule (radiological hazards)
Consolidated Hazard Log (conventional hazards)</td></tr>
<tr><td>Step 2: Decide who might be harmed and how</td><td>Conventional and radiological fault analysis (NOSM N2.3 and N2.4)</td><td rowspan="2">Underpinning work for Volume 1 (construction and non-radiological hazards)
HAZANs (covering radiological accidents)
HAZAN Summary Sheet (covering criticality accidents)
Normal Operations Safety Assessment (covering radiological hazards)</td></tr>
<tr><td>Step 3: Evaluate the risks and decide on requirements and precautions</td><td>Fault analysis including definition of safety requirements and/or hazard management strategy
(NOSM N2.3, N2.4 and N3)</td></tr>
<tr><td>Step 4: Record findings and implement them</td><td>Definition of safe operating envelope (NOSM N3)</td><td>HAZDOC (see Figure 3)
Volume 1 (construction and non-radiological hazards)
Volume 2 (normal operations radiological hazards)
Volume 3 (radiological accidents)
Volume 4 (criticality accidents)
Main Report
Forward Action Plan Schedule</td></tr>
<tr><td>Step 5: Review the assessment and update if necessary</td><td>Safety case and design development in line with the project lifecycle
Review and maintaining safety case in line with the design and project lifecycle
(NOSM N1 and N4)</td><td>Forward Action Plan Schedule</td></tr>
</table>

The generic OSC consists of the Main Report and the four supporting volumes as detailed in section 1.2 and summarised in Figure 4 below.

Figure 4 Detailed Operational Safety Case Structure



For the 2016 generic OSC, the high-level structure of the Main Report and Volumes 1 to 4 has been retained from the 2010 generic DSSC. This presents the key issues, at a suitably high-level, that underpin RWM's confidence in the feasibility of the GDF. The underpinning documents for Volumes 1 to 4 conform to the hierarchy of documentation required by the NOSM and contain the details of the assessment. This enables a flexible and more easily maintained document structure for future updates and the subsequent production of a Preliminary Safety Report. The hierarchy of the documentation aids navigation, traceability and clarity of presentation of the process, data, assessments and outputs of the safety case.

The production of the generic OSC documents has taken due account of the specific requirements as set out in the NOSM. The methodologies and procedures set out in the NOSM have been applied appropriately and proportionately; limited to those areas relevant to the project phase. Procedures related to developing final ALARP arguments and supporting detailed substantiation of claims based on actual designs or fixed design requirements are not applicable at this stage. Reconciliation of the NOSM with the refinements of the process adopted for the 2016 generic OSC will be subject to a Forward Action Plan (FAP.2016.MR.09).

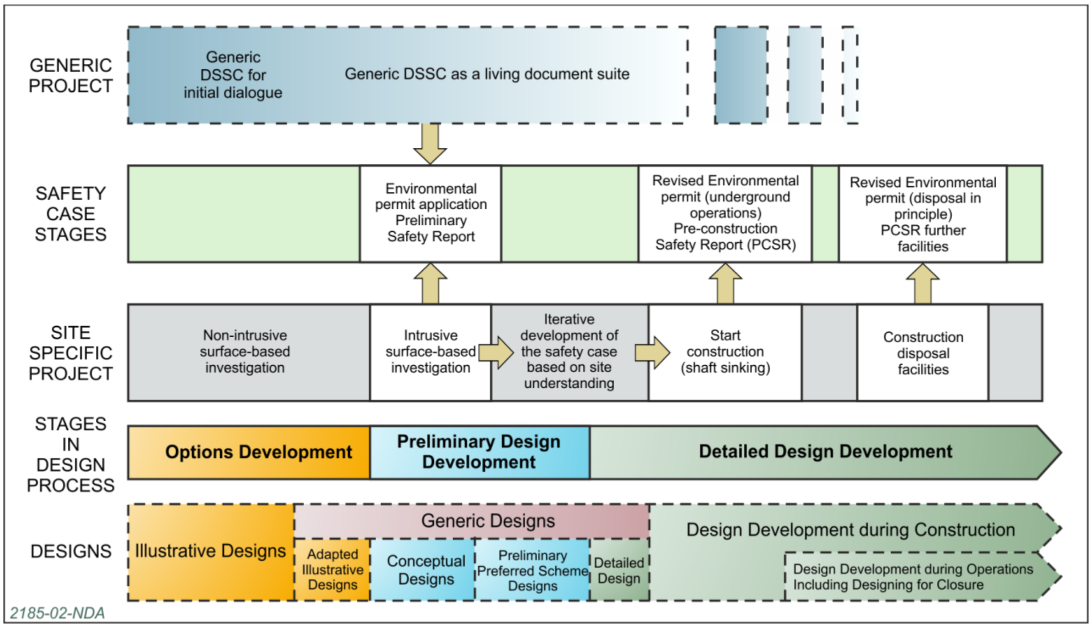
3.2 Stages of the safety case

The safety case strategy is set out in the Operational Safety Strategy [27]. RWM has adopted a staged approach to developing safety cases throughout the design process. At each stage, an appropriate safety case will be needed to allow the project to proceed through the site studies, surface investigation, underground investigation, construction, commissioning, operations, decommissioning and closure phases. The Safety Case Production and Management 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.

As GDF implementation progresses, the safety assessment approach will become more detailed to address the complexities of individual sub-facilities in different operational states, from concept design through to decommissioning and closure. The Operational Safety Strategy takes cognisance of these complexities. This includes future requirements for updates to the generic OSC and production of staged safety cases throughout GDF implementation, operation and closure.

Figure 5 maps the staged safety case delivery process to the corresponding phases of the GDF implementation process, as described in the RWM EDM. The EDM identifies the main gates, which are planned to occur at the end of each design stage (bottom row of Figure 5).

Figure 5 Design and Safety Case Stages



The gate review at each stage in the project life-cycle checks and confirms that the required deliverables, including safety assessments, are available and have been appropriately approved. The gate review process will ensure that a design and safety integrated process is properly implemented. A successful gate review is required before the project can progress to the next stage of the project life-cycle.

GDF implementation is currently at the ‘illustrative design’ stage. However, RWM produces illustrative concepts derived from international organisations at a greater level of technical maturity that would be expected when regulatory approval for construction is being sought. This is shown in Figure 5.

3.3 Data underpinning the safety assessment

RWM has undertaken a major review of its policies and procedures governing the management of models and data. This has resulted in the revision and update of relevant procedures which have significant implications for the way that RWM managed the update to the generic DSSC. All data used in the update have been captured on data definition forms (DDFs) (Figure 4) which are signed off by RWM competent data owners to confirm the provenance and validity of the data. Where required, agreement between data owner and data user on the applicability and use of the data is captured on a data use form.

A forward action has been identified to review the NOSM to ensure that it appropriately reflects the requirements for management of data and models (FAP.2016.MR.09).

3.4 Design and safety integration

RWM is currently reviewing its processes, including the requirement to develop and apply a design and safety integration (DASI) process, at the appropriate project phase, which is consistent with current industry standards and relevant good practice. The integration of RWM's design (EDM) and assessment procedures (NOSM) and a gated approvals mechanism will ensure a safety-informed and integrated design approach is applied through the GDF life-cycle (FAP.2016.VOL3.16). The DASI process as applied to radiological safety will be built around a structure to ensure:

- The assignment of safety functions, based on the principal functions to be implemented, to protect against the main radiological and nuclear hazards on site, namely:
    - prevent exposure to direct radiation
    - prevent the release of radioactive material
    - prevent exposure to uncontained radioactive material
    - prevent unplanned criticality
- Classification of radiological faults in terms of their harm potential (NOSM Section N3.1, Specification and Classification of Safety Measures). Classification is a function of the unmitigated radiological consequences and the initiating event frequency which then drives the category of safety function and the requirement for type, number and quality of safety measures.
- Identification of safety functions, that is, the specific function required to maintain the facility within the safe operating limits and conditions determined both for normal operations and the fault conditions. Safety functions are a high-level statement of the function to be delivered by the safety measures protecting against a particular hazard.
- Development of hazard management strategies for all significant hazards which includes the development of design principles to be implemented through the safety integrated design approach.

For the designers, the approach is summarised below:

- identification of design principles that the design is required to meet so that the safety functions and any legal or regulatory requirements are met
- definition of limits of engineering capabilities derived from safety requirements to ensure that a credible design can be developed
- application of the DASI process through the EDM and the NOSM including application of a structured hierarchy of risk controls and safety measures to design solutions
- assessment as to whether the identified design solutions, in the form of safety measures, will meet the requirement and, if not, identifying solutions that will be acceptable and capable of supporting claims in advance of a detailed design

Throughout this document, this approach is referred to as the development of a 'hazard management strategy'.

Production of the 2016 generic OSC has included a structural and systematic process to identify the safety functions, conceptual safety functional requirements and safety measures. This process considered the engineered provisions as they are currently planned. It also considered the capability to protect against the fault and identified areas for further work, either relating to design improvements or the need to better understand the fault and its progression as an input to optioneering.

The output from the safety assessments was then used to identify potential risk reduction measures based on the ‘eliminate, prevent, protect and mitigate’ hierarchy and to judge whether the options further up the hierarchy would be feasible to implement, as detailed in section 5.3.2. This exercise was undertaken to demonstrate that the hazards could feasibly be managed in accordance with the requirements of the fault analysis and the methodologies in the NOSM. It has also provided insight into areas where optimisation of the design and processes will be warranted at the appropriate project phase in support of ALARP arguments.

In order to advance the safety assessment to a more detailed analysis, the design will develop to include the preparation of plant layout drawings and technical specifications (captured within FAP.2016.MR.01). When the project enters formal design definition and development a robust change control process that includes configuration management will be required. This is a requirement under the NIA 1965 for any site licence company. The application of formal change control and configuration management ensures that there are documented and structured processes in place to ensure that the developing design is controlled and that any changes are assessed before implementation in the reference design.

3.4.1 Classification of safety measures

Any safety measure claimed as part of the safety justification will require a demonstration that it is adequate, fit for purpose and able to deliver its safety function under all operating conditions, including transient conditions. Such safety measures will be classified according to their relative importance in delivery of a safety function. This safety classification, in turn, will define the design requirements including the performance requirements (in terms of functional reliability or availability). As a result of the classification, the safety measures will require an appropriate level of quality assurance, commensurate with the harm potential, to be applied to all stages of the safety measure’s life-cycle. For the specific case of engineered safety measures and their constituent structures, systems and components (SSC), their design (including any associated analysis), fabrication, manufacture, assembly, inspection, installation, commissioning, operation and maintenance will be subject to a level of quality assurance commensurate with their safety importance, as defined in the NOSM.

The nuclear safety framework is founded upon the principle that a graded approach should be applied to the safety requirements, comprising a structured method by which the stringency of the application of requirements can be varied to reflect the relative safety, security and environmental importance. The graded approach is applied to all stages of the facility life-cycle with the proviso that any grading that is performed must be such that safety functions and operational limits and conditions are preserved and that there are no undue radiological hazards to facility operators, the general public or the environment. This includes the application of suitable codes and standards to all aspects of the life-cycles of the safety measures or SSCs.

The application of the most appropriate codes and standards aligned to the safety classification of engineered safety measures and their associated SSCs is one of the most important drivers in the design substantiation process for nuclear facilities. This alignment provides an important element for the demonstration of safety, based on deterministic requirements and the associated costs.

RWM’s approach is set out in the NOSM and the EDM and applies the graded approach to the application of codes and standards. For higher safety classifications of engineered measures, appropriate nuclear industry-specific, national or international codes and standards will be adopted in order to ensure a conservative design with suitable built-in safety margins. For lower safety classified equipment, if there is no appropriate nuclear industry-specific code or standard, an appropriate non-nuclear-specific code or standard will be applied instead.

It is possible that, during the course of the GDF design, there will be safety measures or features for which there are no appropriate established codes or standards. In this case, where possible, an approach derived from existing codes or standards for similar equipment under similar conditions will be applied, in accordance with principle ECS.4 of the ONR SAPs. In the absence of any applicable or relevant codes and standards, the approach will be either to derive an appropriate code or standard or to provide a robust demonstration through qualification and substantiation. This approach will require dedicated quality assurance programmes for each such requirement and will comprise a detailed quality assured record of all aspects of the safety measure/SSC as applicable to the delivery of the safety function. This includes analysis, material records, technical specifications, performance characteristics under all design basis conditions, ageing and environmental studies, tests, the results of experience, experiments or tests or a combination thereof, in accordance with principle ECS.5 of the ONR SAPs.

3.5 Application of the safety case to waste packaging

The generic DSSC, and the generic OSC, have an important role to play supporting the Disposability Assessment process. The is the process whereby waste packagers can seek advice from RWM on conditioning and packaging of higher activity waste in a disposable form so as to minimise the need for future re-work prior to transport and acceptance into the GDF. This is a risk-management process recognised by regulatory guidance and gives waste packagers and waste owners confidence that conditioning and packaging of waste can be carried out, that appropriate assurance has been sought and that the proposed waste packages will be consistent with the generic DSSC.

Definition of requirements on the package design following interim-storage and confirmation that those requirements have been met prior to shipment are an integral part of supporting the future GDF safety case. This is and will continue to be an ongoing area of collaborative working between RWM and current holders of the UK Radioactive Waste Inventory.

In the particular case of operational safety, a proposed waste package is evaluated to determine its radionuclide loading (inventory) and likely performance if subjected to the bounding fault scenarios identified in the generic OSC. Likewise, comparisons will be made regarding external dose and criticality. This process is iterative and may lead to changes to the waste package inventory or design, or conversely may lead to changes to the GDF design or safety case. This is described in further detail in section 6.1.

These waste packages are intended ultimately to be consigned to the GDF and to be covered by the final safety case. Therefore the Disposability Assessment process also addresses the data to be recorded regarding individual waste packages and defines the quality management standards to be applied. Since consignment for ultimate disposal may not occur for many years, the process is supported by periodic audits of the waste packaging process and intermediate storage conditions and by updates of the assessments to ensure that they remain based on the latest information.

It is the waste producer’s responsibility to ensure the package content is compliant with its Letter of Compliance issued through the Disposability Assessment process. However, there will inevitably be some uncertainty on the package inventory. Consideration is therefore being given to the arrangements that should be put in place to minimise the risk of receipt of waste packages that do not meet GDF acceptance criteria (FAP.2016.MR.05).

4 Safety Assessment Basis

4.1 GDF design

Three generic design illustrations have been developed based on six illustrative disposal concepts:

- one for each of LHGW and HHGW,
- in each of the three host rock environments, namely: higher strength rock, lower strength sedimentary rock and evaporite rock.

The generic OSC applies to all six illustrative concepts as it is developed from a functional description of the process needs, and not from consideration of the systems that will deliver the functions. It is therefore independent of the host rock.

The illustrative designs for the GDF and associated transport system are described in Generic Disposal Facility Designs and Generic Transport System Designs reports. When RWM reaches the stage of developing a design for a particular site, the disposal concept and design will be tailored to the characteristics of the final inventory for disposal and to the characteristics of the given site. At this generic stage, the illustrative concepts play an important role in visualising how the GDF might operate in practice, aiding in understanding the needs and challenges to be addressed.

4.2 GDF operations

Underpinning both the generic OSC and the illustrative designs is the functional Process Flow Description (PFD); the full PFD is provided in the Basis of Operational Assessment (BOA) [28]. The PFD describes the processes and systems required in any GDF from receipt of waste packages to final emplacement in vaults, deposition holes or tunnels. The PFD is independent of the geological environment and disposal concept hence a single PFD can be used to evaluate the six concepts identified above.

The overall process described in the PFD supporting the safety assessment is split into a series of 'nodes' to facilitate the interface with design (nodes N1 to N6), which are:

- surface receipt and on-site transfer (N1)
- waste package transfer facility: unloading of package from transport vehicle (N2)
- surface preparation of package for below ground transfer (N3)
- underground transfer of package to sub-surface receipt facilities (N4)
- underground preparation of package for emplacement (N5)
- emplacement of package (N6)

These nodes are likely to be invariant as the GDF progresses from illustrative to site-specific design and thus form a sound basis from which to build and maintain the PFD.

The PFD only covers activities related to package handling and emplacement but it is envisaged that it will be extended to include post-emplacement activities such as backfilling (Node 7 in the package handling PFD), as this represents the end of the functional process from an operational perspective. Any meaningful consideration of backfilling and decommissioning requires the decommissioning strategy to be available, processes to be optimised and defined and the means of backfilling to be specified; this is currently planned for the Preliminary Safety Report stage. Until then, the opportunity to challenge the safety functions during this phase is limited, the facility being passively safe if all other design requirements are implemented. The backfilling process has however been considered in this generic OSC within the hazard identification studies as a potential hazard initiator, for example, by introducing the potential for flooding.

A complete suite of PFDs to encompass all activities and support definitive safety assessment of the full life-cycle of the GDF is flagged as a necessary forward action within FAP.2016.MR.06, together with the requirement for improved plant layout drawings and information (FAP.2016.MR.01).

The BOA describes the scope of the generic OSC as covering all GDF operations from point of receipt of the transport unit to the final underground emplacement of the disposal unit. It presents a description of the GDF package handling concept, for which the PFD has been produced, with processes and descriptions of the systems as high-level tasks and notional worker groups for each task.

To explain the terminology, a transport unit could be a train or HGV carrying one or more transport packages, each containing one or more disposal units. A disposal unit may be a single waste package or a group, such as in a stillage.

The use of the PFD during the hazard identification exercises enabled the process to be systematic, and because it is function-driven, the identification of a hazard is decoupled from its magnitude. This allows the basis of the assessment to be flexible and helps in the identification of order of magnitude effects that are most likely to influence the design development. The PFD covers all the functional processes at task level for emplacement of all waste package types in the UK 2013 DI. Other considerations included in the PFD at this stage are:

- the PFD structure incorporates both a drift and a shaft as possible modes of transfer of waste packages underground to enable hazard identification for both
- waste packages are assumed to arrive in one of three transport configurations, namely: a transport overpack (IP-2) generally for shielded ILW/LLW, Standard Waste Transport Containers for ILW and Disposal Container Transport Container for HLW/spent fuel
- the PFD approach will be used as a tool to aid the understanding of the high-hazard areas of the GDF and their location
- the PFD aligned with the illustrative concepts; this enables any future design and assessment changes to be linked and controlled together
- it enables dialogue with the engineering team to ensure an integrated safety and design process going forward

At this functional level, any equipment required can be described in generic terms as shown in Table 2. This approach has the advantage that operability requirements and conceptual safety functions can be identified based on systematic hazard identification for the entire waste emplacement process. In addition, the subsequent analysis of normal operations and design basis fault sequences can also be used to specify safety requirements for the future GDF design.

Table 2 Operational Activities Considered

Process Type	Process Type Description
Moving	Transporting waste using vehicles (road/rail).
Lifting	Any tasks involving lifting equipment, including traversing, setting down and winching down shaft.
Unloading	Removing/putting a package on or disengaging/engaging from a vehicle.

Process Type	Process Type Description
Unpacking	Changing package configuration.
Stacking	Stacking for final emplacement.
Monitoring	Checking package identification/compliance.
Sentencing	At the onward-transfer end, checking a disposal unit is being sent to a disposal area designated for that disposal unit type and, at the receipt end, that the type of disposal unit received is correct for that disposal area.

4.3 Scope and status of assessment

During the course of development of the generic OSC, the safety assessment has highlighted a number of limitations of the safety case which are listed and justified in Table 3.

Table 3 2016 OSC Omissions and Limitations

Generic OSC Report	Type	Generic OSC Status	Justification
All	Operations	The following operations are included in the PFD and HAZID but no quantitative accident safety assessment has been undertaken: • surface receipt and on-site transfer (rail or road) (Node 1) • waste package transfer facility (WPTF) unloading of package from transfer facility (rail or road) (Node 2) • surface preparation of package for below ground transfer via a drift or shaft (Node 3)	All activities at the surface are carried out with the waste package in its transport configuration which includes design and performance requirements to meet the IAEA Regulations for the Safe Transport of Radioactive Material (the Transport Regulations). As a result, it has been judged that there are no radiological consequences arising from the design basis faults when in the transport configuration. The operations to be undertaken at the surface are tried and tested activities undertaken extensively on UK nuclear licensed sites with established codes and standards that apply to the buildings and equipment within which ensure that the risk of accidents is minimised.
Main Report, Vol. 3 and Vol. 4	Operations	Post-accident recovery activities are not considered.	It is not appropriate to undertake a review of post-accident recovery at this early generic stage of the GDF without an understanding of the challenges presented.

Generic OSC Report	Type	Generic OSC Status	Justification
Main Report and Volumes 1 to 4	Scope	Backfilling, closure and sealing and decommissioning operations	No assessment for these operations has been undertaken due to the level of design definition available at the generic stage.
Main Report and Volumes 1 to 4	Scope	With the exception of identification of construction and non-radiological hazards, the assessment is not specific to a geological setting.	No detailed assessment is required as no order of magnitude effects specific to the geological environment (or design assumptions made as a result) have been identified that influence the outcome of the accident safety assessment. Whilst both draft and shift transport is included in the PFD, neither are specific to a particular geological environment to ensure maximum flexibility and utility of the safety case.
Vol. 1	Hazards	The conventional hazards identified and assessed are restricted to an illustrative set of the most challenging hazards (that is, those with greatest potential for harm) and are generic in nature.	The key purpose of the study is to identify the major conventional hazards from the construction and operation of the GDF such that appropriate good practice and guidance can be embedded into the developing GDF design. As the design becomes more detailed, lower consequence conventional hazards will be considered.
Volumes 1 to 4	Safety Assessment	Comprehensive ALARP assessment and justification.	The level of detail within the illustrative concept does not yet support this, FAPs are identified to aid the development of the design to an ALARP solution. This is consistent with the requirements of the NOSM which states that at this generic stage, the ALARP consideration is limited to demonstration that relevant good practice will be applied and that optioneering has and will be undertaken to identify the appropriate design solutions.

Generic OSC Report	Type	Generic OSC Status	Justification
Main Report, Vol. 3 and Vol. 4	Operations activities	Maintenance operations are not considered.	Due to the level of detail available within the design, insufficient information exists as to the specific equipment which will be utilised, their locations, the schedule for maintenance or the frequency of maintenance based on regulatory requirements for a given equipment type. As a result, maintenance operations cannot be considered at this stage. As the design develops, the maintenance strategy and approach will be specified and maintenance activities can then be included in the assessment, such as the need to undertake a high-level maintenance functional analysis and requirements study. In addition, any safety related equipment identified as requiring maintenance will require studies to ensure that maintenance can be practically managed, for example, through safe access and egress (both these requirements are captured in FAP.2016.MR.03). The access and egress requirements will drive specific decisions for the design which will require optioneering to be undertaken which has not yet commenced.
Vol. 1	Risk Reduction Measures	Specific engineering or procedural controls have not been claimed in the conventional hazard assessment.	The level of detail at this generic stage does not yet support this and hence the review is limited to identifying appropriate good practice and guidance which can be embedded into the developing design.
Vol. 1	Hazards	Volume 1 does not consider the conventional hazards as a result of external events.	Detailed consideration of external hazards is site-specific and will be addressed as the design of the GDF develops for a particular site.
Vol. 2	Hazards/ Scope	Volume 2 does not provide an assessment of anticipated operational occurrences.	Additional details are required on the specific operations and plant design in order to assess anticipated operational occurrences.

Generic OSC Report	Type	Generic OSC Status	Justification
Vol. 2	Safety Assessment /Claims	Volume 2 has not performed a normal dose assessment for an optimised design.	An illustrative dose assessment has been undertaken to demonstrate that regulatory compliance is feasible based upon the current illustrative concepts and has identified forward action plans. The level of design definition available at this stage does not permit an assessment of an optimised design.
Vol. 2	Hazards	Natural radon gas as a contributor to doses to workers from the airborne release pathway has not been assessed within the OSC.	It is acknowledged that the contribution from natural radon gas may be significant, but this assessment is anticipated when there is more design detail available, as stated in the NOSM. The emanation rate will be highly dependent on the precise nature of the host rock and equilibrium air concentration dependent upon the local air change rate provided by the underground facilities extract ventilation system (not yet designed). In any case, there are specific legal requirements for the management of radon that will need to be met in the design. There is currently too much uncertainty associated with these factors for meaningful detailed assessments of doses due to radon to be made until site characterisation data are available.
Vol. 3	Hazards	Potential radiological consequences arising from injection and/or contaminated wound pathways have not been calculated.	Information for the specific tasks undertaken by operators is insufficient at the generic stage to permit meaningful assessment of faults involving injection or wound pathways.
Vol. 3	Faults	The assessment undertaken has been limited to an analysis of a set of representative faults considered to be the most challenging.	At the current generic stage, there is insufficient definition in terms of the design provisions and the activities to be undertaken within the GDF to be able to perform a detailed assessment. As such, the assessment is limited to those faults which are considered to be the most challenging in terms of feasibility. As the design develops further, more detailed assessments will be performed.

Generic OSC Report	Type	Generic OSC Status	Justification
Vol. 3	Hazards/ Safety Assessment	No quantified analysis of internal hazards has been undertaken.	There is insufficient definition in terms of the design provisions and their relative locations to permit quantified analysis of internal hazards. Hence, a qualitative approach has been applied based on identifying the key principles the design will need to consider. As the design develops further, more detailed assessments will be performed based on the methodologies set out in the NOSM.
Vol. 3	Hazards/ Safety Assessment	No quantified analysis of external hazards has been undertaken.	Detailed consideration of external hazards is site-specific and will be addressed later as the design of the GDF develops. The hazard analysis has been limited to a qualitative assessment of potentially credible external hazards and the relevant parameters. As the design develops further, more detailed assessments will be performed based on the methodologies set out in the NOSM.
Vol. 4	Safety Assessment	Volume 4 provides a high-level review of criticality safety during the operation of the GDF and the identification of key issues to be addressed for the development of a safety case. No detailed criticality calculations have been carried out.	The document summarises key aspects of criticality safety and presents specific arguments for fault conditions and criticality warning systems in order to demonstrate that criticality is very unlikely. This is considered to be appropriate at this generic stage where demonstrating feasibility is the principal objective.

5 Safety Assessment

The claims relevant to each Volume of the generic OSC are presented below:

Volume 1	OSC.SC1	All reasonably practicable steps will have been taken to implement design provisions whose function is to prevent or minimise the risk of injury due to conventional hazards.
Volume 2	OSC.SC2	All reasonably practicable steps will have been taken to implement design provisions whose function is to prevent or minimise routine exposures to radiation sources.
Volume 3	OSC.SC3	All reasonably practicable steps will have been taken to implement design provisions whose function is to prevent or mitigate the consequences of radiation accidents.
Volume 4	OSC.SC4	All reasonably practicable steps will have been taken to implement design provisions whose function is to prevent or mitigate the consequences of nuclear accidents (ie unplanned criticality).

The safety assessment has, in certain cases, considered waste category sub-divisions, as set out in Table 4. This approach has been taken because radiological safety assessment is often specific to a waste category sub-division and hence needs to be assessed on this basis to align with the PFD. It also gives a more useful discrimination and structure between the faults, the wastes and the process combinations.

Table 4 Waste Groups and Categories

Waste Group	Waste Categories
HHGW	Spent fuel , HLW, Pu and HEU component of uranium
LHGW	ILW, LLW and DNLEU component of uranium

5.1 Volume 1: Construction and Non-Radiological Safety Assessment

5.1.1 Safety justification

The safety claims, arguments and evidence related to construction and non-radiological hazards are summarised in Table 5.

Table 5 Construction and Non-Radiological Safety Claims, Arguments and Evidence

Reference	Safety Claim	Argument	Evidence
Principal Claim			
OSC.SC1	All reasonably practicable steps will have been taken to implement design provisions whose function is to prevent or minimise the risk of injury due to conventional hazards.	The development of hazard management strategies will set out the requirements that the design will be required to implement through suitable design principles, from which suitable and sufficient safety measures will be identified to protect against the hazards.	The most likely conventional hazards with the greatest harm potential which could impact on the feasibility of constructing and operating the GDF have been identified. Suitable hazard management strategies and design principles will be developed and implemented in the design. The developing safety assessment will be facilitated by the issue and implementation of a conventional hazards safety manual as part of the RWM safety case manual suite, when appropriate for the project needs (FAP.2016.MR.02).
Supporting Claims			
OSC.SC1.1	The most significant conventional hazards associated with the GDF construction and operation activities have been identified through a systematic hazard identification process.	Application of industry standard hazard identification techniques to the PFD has provided the basis for a systematic process of identification of the principal hazards.	Hazard identification studies combined with information from the construction related studies for the 2010 generic OSC have been used to develop a consolidated hazard log. Hazards within the hazard log have been bounded and grouped into conventional fault sequence groups which are considered to be the most likely conventional hazards with the greatest harm potential.

Reference	Safety Claim	Argument	Evidence
OSC.SC1.2	There is an understanding of the legislative health and safety requirements and current best practice associated with the construction and non-radiological hazards relevant to the GDF.	The review of legislation undertaken identified the principal safety requirements which impact on the design. Potential risk reduction options for consideration in the design have been identified through a review of ways in which the ERICP hierarchy of controls can be applied.	For each conventional fault sequence group, relevant statutory legislation has been identified, together with an understanding of the principal requirements for the design through application of the industry accepted approach for the hierarchy of controls.
OSC.SC1.3	Arrangements will be in place to ensure that suitable hazard management strategies are developed which include the development of design principles to be implemented through the RWM design and safety integrated approach.	No hazards have been identified that could challenge the feasibility of designing, constructing and operating the GDF. It is therefore entirely feasible to implement adequate controls and arrangements into the GDF design to either eliminate or manage all potential hazards. Controls and arrangements will be established which complement those in place for radiological safety.	The development of the RWM DASI process will deliver this requirement (FAP.2016.VOL3.16).
OSC.SC1.4	Lessons learned from relevant incidents and recent major projects have been identified and assessed in order to ensure a continuous ‘learning from experience’ approach is implemented.	Learning from recent and future major projects and incidents will help the GDF design as part of the application of relevant good practice to ensure that the design is ‘right first time’.	A review has been undertaken of the lessons learnt from a range of applicable projects and incidents in order to provide input on learning from experience for the developing design. Any additional good practice guidance and measures to be carried forward and integrated into the GDF design to enhance safety during its construction and operation have been identified. Such learning from experience activities will continue as the GDF design develops.

Reference	Safety Claim	Argument	Evidence
OSC.SC1.5	A balanced design will be implemented through the hazard management strategies ensuring proportionality between the needs of conventional, radiological and environmental safety across all safety related hazards.	The developing design and safety assessment will consider the radiological, environmental and conventional hazards to ensure that a balanced approach is taken which does not disproportionately prioritise control measures.	The safety assessment has recognised the importance of ensuring that the design development ensures that undue prioritisation is not given to radiological hazards rather than the potential for fatalities or serious injuries from the associated conventional hazards. This requirement is built into the risk reduction process in the NOSM.
	There is high confidence that the GDF can be constructed and operated safely with risks to the workforce and members of the general public which can and will be tolerable and ALARP	The conventional and non-radiological risk assessment has shown that the conventional hazards have been identified and understood. Sufficient and adequate controls and arrangements are considered to be feasible and can be incorporated into the design. The design will need to be developed in order to undertake option studies and optimisation.	The assessment presents evidence related to: the process that has been followed, the scope of the assessment, nature of hazards identified requiring design provisions, regulatory expectation related to their control, and hazard management strategies that will need to be adopted to prevent or minimise the risk of injury due to conventional hazards.

5.1.2 Safety assessment

The principal safety claim (SC) to be demonstrated for the construction and non-radiological safety assessment is that:

OSC.SC1: All reasonably practicable steps will have been taken to implement design provisions whose function is to prevent or minimise the risk of injury due to conventional hazards.

At this stage of the project the focus of the construction and non-radiological safety assessment is on those ‘conventional’ hazards with significant harm potential. Such hazards will require a hazard management strategy and robust engineered design provision to ensure the safety of staff, the public and environment. This approach is appropriate where the aim is to demonstrate that the management of significant hazards is possible. The level of assessment is appropriate for the current design development stage of the GDF; it is a feasibility study. At this time, a detailed description of the specific site layout, design, operational activities and associated tasks is not available, or is expected to be available. The construction and non-radiological hazards safety assessment is therefore derived from the representation of the GDF as a PFD. This is a high level description of activities and the required plant and equipment or tasks that could be used to implement the required functions.

A systematic hazard identification exercise has been undertaken. The output of the hazard identification process was collated and recorded in the illustrative consolidated hazard log. As part of the screening process to identify the most likely hazards with the greatest harm potential, the complete consolidated hazard log was reviewed. The conventional hazards (ie construction and non-radiological) have been grouped into twelve high-level conventional generic fault sequence groups (CgFSGs).

A further screening of the hazards contained within the consolidated hazard log was undertaken to clarify the phase of construction (such as surface, surface-to-sub-surface or sub-surface construction) and the specific operations. This was developed into generic conventional hazard groups to be assessed:

- C1: workplace transport
- C2: working and load at height
- C3: structural collapse
- C4: plant/machinery
- C5: fire and explosion
- C6: projectiles and blast, over-pressure
- C7: airborne hazardous substances and air quality (including asphyxiation)
- C8: flooding
- C9: electrical
- C10: noise and vibration
- C11: concurrent activities (also referred to as ‘conflict hazards’)
- C12: occupational

For each generic conventional hazard identified (ie the CgFSGs), the relevant legislation (or relevant good practice) and high level health and safety requirements have been compiled. These will form the basis from which the hazard management strategy will be developed, with the emphasis being on hazard elimination where practicable. This will also include consideration of design provisions that allow the GDF to be designed to be “passively safe” during the operational phase. Work during the construction phase, such as installing rock support systems, will ensure the facility is “passively safe” in terms of the disposal of radioactive waste packages. Compiling the high level health and safety requirements has also identified general expectations, placed on the duty holders under the key legislation and recognises the role of relevant good practice and/or guidance from the HSE or industry bodies.

During its construction and operation, the GDF will share many features not only with large-scale sub-surface operations but also with other large-scale construction projects undertaken for high-hazard industries in the UK and overseas. As such, development of the GDF needs to consider potential hazards common to many industrial operations subject to a ‘permissioning regime’ (for example, nuclear, railways, offshore and onshore major hazard industries). These hazards can be present during construction and normal operations as inherent hazards and as a result of potential failure of process plant.

This information will be used to inform the future Optioneering studies to be undertaken as the GDF design progresses to satisfy the hazard management strategy. This will ensure that an appropriate and balanced GDF design is implemented by ensuring legislative compliance, incorporation of relevant good practice and proportionality between the needs of conventional, radiological and environmental safety across all safety-related hazards.

The GDF design will be developed to ensure that all reasonably practicable steps to minimise and control conventional hazards have been taken. This will be achieved in line with the recognised hierarchical principle of ERICP:

- Eliminate
- Reduce
- Isolate
- Control
- Protect

This approach has been applied illustratively for all 12 CgFSGs to demonstrate that RWM understands the principal construction and non-radiological hazards that are relevant to the GDF. This gives high confidence that the processes and outcomes and the relationship to the design development are understood and will be demonstrated in the application of the RWM design and safety integration process. The RWM design and safety integration process is consistent with current industry standards and relevant good practice.

Further work has been identified by RWM to develop the safety management arrangements and ensure that appropriate consideration of construction and non-radiological hazards is undertaken throughout the lifecycle of the GDF. This work is captured in a FAP.

5.1.3 Learning from experience

As part of the development of the generic OSC, a review has been undertaken of incidents from other GDF and relevant major construction projects to identify additional good practice guidance and measures. This will be carried forward and integrated into the RWM GDF design process to enhance safety during both construction and operation.

Analysis of major incidents in other high-hazard industries generally finds that the root cause falls into one of four categories:

- an event occurs that was either deemed extremely unlikely or unknown/unidentified, such that no risk controls were identified or implemented to manage it
- the impact or severity of an unlikely event that occurs is in excess of that used in the design basis and is hence beyond the risk control system's capability to manage
- a facility is operated outside its design basis either intentionally or unknowingly
- individually unimportant errors and/or failures combine to result in a serious outcome

Additionally, the analysis of major incidents in high-hazard industries with different technical causes and work contexts has identified several common causal factors. These factors are related to leadership, attitudes and behaviours, risk management and oversight and can be measured through methods such as the international safety rating system. RWM is using this insight to ensure that a strong safety culture is at the heart of the GDF Programme.

5.1.4 Safety culture

Worldwide industrial incidents have demonstrated the importance of developing and maintaining a strong safety culture within the leadership and management teams to ensure that safety is given the highest priority. The safety culture in RWM is underpinned by the safety management system which ensures that all necessary processes and procedures are aligned to ensure that safety is a core aspect of normal business. This includes the development of integrated working arrangements through the design and safety integration process to deliver safe, optimised designs with suitable and sufficient management controls to ensure that safe working practices are applied. RWM has instilled a corporate safety culture within its management system and this is being implemented through initiatives such as 'see something say something', near-miss reporting, emphasising importance of day to day safety and the monitoring aspects such as staff surveys and safety-related performance indicators in each monthly management report.

RWM is committed to building on this good practice as the organisation moves forward, as would be expected from a prospective future nuclear site licence holder. In maintaining a strong safety culture RWM will continue to take account of learning from experience both from GDF projects and from other major projects worldwide. The safety culture, together with the associated safety management system, will be the basis for ensuring that RWM applies rigour to the assessment and implementation of the highest standards of construction and non-radiological safety to all its activities.

5.1.5 Concurrent activities and hazards

Over the long operational phase of waste emplacement (in excess of 100 years), it will be necessary for emplacement operations to be undertaken in parallel with construction activities (eg ongoing excavation and construction of disposal vaults). This strategy of parallel construction and emplacement is partly a practicality issue from working in a geological environment and also is required to minimise the duration of the operational phase. These parallel activities give potential for hazards termed as 'conflict hazards' in the safety assessment. There could be potential for these 'conflict hazards' to cause interactions between waste emplacement operations and construction. However early identification, and control, of 'conflict hazards' will ensure that the system is designed to ensure that there is no impact on the ability of engineered safety measures to deliver their nuclear safety function. Construction related hazards which may impact on delivery of safety functions required for safe nuclear operations (eg emplacement of waste), are assessed in the radiological accident safety assessment as an internal hazard, as required by the RWM Nuclear Operational Safety Manual.

The issues arising from this strategy have been identified and assessed relative to the design. For example, the illustrative underground layouts have been configured to minimise the amount of construction work required up to first waste emplacement. The safety of concurrent operation and construction can be assured by utilising the following illustrative options:

- airlocks and seals between different zones and areas underground
- the provision of independent ventilation circuits

The importance of ensuring a balanced design to manage safety hazards (both conventional and radiological) is fully recognised by RWM. The early recognition of 'conflict hazards' at this stage will ensure that the design and operation of the GDF is considered as a 'system' that minimises the potential for unsafe interactions. This need for a balanced design that takes account of the full GDF lifecycle has been recognised and is applied during all development work.

5.1.6 Concluding remarks

The extent to which the principal safety claim (OSC.SC1) has been demonstrated is summarised below.

This illustrative safety assessment presents evidence related to the process that has been followed, the scope of the assessment, nature of hazards identified requiring design provisions, regulatory expectation related to their control, and hazard management strategies that will need to be adopted to prevent or minimise the risk of injury due to conventional hazards.

The safety assessment concludes that the following conventional fault groups are the most significant in terms of potential for harm during the construction phase:

- structural collapses underground including rockfalls
- fire and explosions (in particular in the underground environment)
- flooding (in particular in the underground environment)
- transport accidents
- air quality underground

The hazard management strategies, future development of detailed design requirements and implementation in the design will ensure these hazards do not warrant further consideration as part of the 'design basis accident' in the operational phase. The nature of the construction will ensure that it is safe to operate for its intended purpose. Compliance with all safety requirements during the operational phase will be subject to ongoing regulatory review, commonly referred to as Periodic Review of Safety. The design and means of ensuring safety through life delivery will be an integral part of the design development process. The implication of different host rocks has also been assessed, including the differences between specific hazards associated with each host rock, together with the different techniques which may be applicable to the underground construction activities for each host rock.

It is concluded that this high level assessment has identified a representative set of conventional safety hazards and the associated risks from construction. This includes the potential hazards from construction in parallel with disposal and operational waste package handling and emplacement activities. In addition, the relevant good practice and requirements to manage the hazards have been identified and processes will be put in place to ensure the integration of these controls within the GDF design. This will be achieved through implementation of the hazard management strategy.

This assessment provides high confidence that RWM has an understanding of the conventional hazards that will need to be assessed and controlled during construction and operation. This will ensure that potential hazards will be adequately addressed in the design and managed throughout the GDF construction and operational activities. The areas which require further work to fully underpin the principal claim are largely related to actual design development, including the design of civil structures and construction plans and the resolution of the FAPs.

Following the completion of this illustrative safety assessment for construction and non-radiological hazards, a number of items of further work have been identified and designated as FAPs. The FAPs will be taken forward as part of the GDF design development process in order to facilitate the development of a balanced design based on relevant good practice and experience. As such, no significant obstacles have been identified which could challenge feasibility where there are claims of future compliance against targets, tolerability of risks and the ALARP principle associated with construction and non-radiological hazards.

5.2 Volume 2: Normal Operations Safety Assessment

5.2.1 Safety justification

Due to the requirement for routine storage, handling and movement of nuclear material within the GDF, radiological exposures to operators, other on-site workers and members of the public can occur from these routine operational activities. The safety claims, arguments and evidence related to normal operations radiological hazards are summarised in Table 6.

Table 6 Normal Operations Safety Claims, Arguments and Evidence

Reference	Safety Claim	Argument	Evidence
Principal Claim			
OSC.SC2	All reasonably practicable steps will have been taken to implement design provisions whose function is to prevent or minimise routine exposures to radiation sources.	It will have been demonstrated that it will be possible by credible means to ensure doses to the operators and public will meet legal and regulatory limits.	RWM has developed a significant capability for assessing doses with some confidence, together with an assessment of the viability of the process based on man-effort requirements and identification of any 'pinch points'. Areas and associated operations and locations have been identified for which engineered provisions will be required. As a result, demonstration that the GDF can be operated safely is considered feasible when the relevant design detail and associated safety analysis is developed.
Supporting Claims			
OSC.SC2.1	RWM has developed a significant capability for assessing normal operational doses based on a PFD.	Use of a computational toolkit for assessing normal operational doses in line with the PFD allows the contribution to the overall normal operational dose burden by waste stream, package and schedule to be assessed which permits effort to be focussed on design development.	Application of the toolkit generates a structured output that allows for simple visual interrogation of a very large data set, ensuring hazard areas and associated activities are easily identifiable. The use of the PFD as a common backbone for both the accident and normal operations assessment ensures that the highest hazard areas to be managed during normal operations will be known in advance of undertaking the accident safety assessment and consideration of fault scenarios.
OSC.SC2.2	The viability of the process based on man-effort requirements can be	Generic assumptions regarding the tasks to be undertaken by the operator, the duration of	The illustrative analysis identifies that the 'pinch points' relate to surface operations, particularly

Reference	Safety Claim	Argument	Evidence
	demonstrated and any 'pinch points' can be readily identified.	exposure and the anticipated throughput have enabled an illustrative assessment man-effort requirements and identification of 'pinch points'.	drivers (on-site and off-site) and the associated banksmen. For sub-surface operations, the 'pinch points' are much less marked for task operatives and banksmen. This indicates the need to focus on and refine operator occupancy data.
OSC.SC2.3	The required dose reduction factors can be achieved through standard nuclear industry solutions and any proposed solution will be derived through optioneering and appropriate task-design to ensure doses from normal operations in the GDF will be demonstrably ALARP.	Dose reduction factors required to meet the RWM dose criterion, below which process optimisation can be applied to further reduce exposures, are judged to be fully achievable using existing nuclear industry solutions. For example, the inclusion of a fully shielded inlet cell with remote handling emplacement for UILW and spent fuel is a technically feasible solution and currently included in the illustrative concept.	The illustrative dose assessment confirms that the majority of potential *unmitigated* doses are within an order of magnitude of the legal limit. This indicates that the required dose reduction factors can be achieved through standard nuclear industry solutions. Any proposed solution will be subject to optioneering and appropriate task-design to ensure doses from normal operations will be demonstrably ALARP and will meet RWM criteria.
OSC.SC2.4	There is very high confidence that it is feasible to design a GDF so that it can be operated safely, with any radiological exposures and doses to the workforce and members of the general public minimised and shown to be tolerable and ALARP	The majority of operations associated with the GDF are relatively standard in terms of the movement, handling and emplacement of waste packages and so will not be expected to require novel technological solutions. It is acknowledged that the transfer of waste packages to the sub-surface environment and operations deep underground are non-standard nuclear activities which require specific consideration.	The majority of activities undertaken at the GDF have illustrative doses which are below the legal and regulatory limits. For those activities where the illustrative doses are above the legal and regulatory limits, it may be possible to remove the need for any exposure by deleting the task or automation of the process. In addition, dose reduction factors required to meet the limits are within the capability of standard industry approaches, such as shielding.

5.2.2 Safety assessment

The principal safety claim (SC) to be demonstrated for the normal operations safety assessment is that:

OSC.SC2: All reasonably practicable steps will have been taken to implement design provisions whose function is to prevent or minimise routine exposures to radiation sources.

At this stage of the GDF programme the focus of the normal operations assessment is on those areas where: design provisions, engineered protection or process design and optimisation will be required. The approach is largely at the level of a proof of feasibility study which is appropriate for the current stage of the GDF design development. A detailed description of a specific site layout, design, operational activities and associated tasks is not yet available for the GDF, nor would it be expected, for this stage of the GDF programme. Hence this illustrative normal operations safety assessment is based on a representation of the GDF as: a functional PFD, a high-level description of activities and the required plant and equipment that could be used to implement the required functions. An illustrative normal operations safety assessment, covering operations in the GDF, has been performed for both operators and members of the public. The standard mechanisms by which the GDF operators, other on-site workers and members of the public could receive a radiological dose as a result of normal operations are:

- external radiation in the form of a direct dose
- internal radiation such as inhalation of particulate material or gaseous discharges as a result of activities on the site

The RWM Nuclear Operational Safety Manual (NOSM) specifies the methodologies and approaches to be adopted for the calculation of normal operations doses, to both operators and members of the public, in accordance with current nuclear industry standards and relevant good practice. However, at the current generic GDF stage, there is insufficient design definition in terms of normal operational activity to be able to perform a full safety assessment. As a result, the assessment is illustrative and a demonstration of feasibility. In identifying those areas of the GDF and the worker groups that are considered the most significant in terms of doses, this assessment prioritises those areas and activities that need to be managed, reduced and optimised through appropriate design provisions. This means that any calculated doses are used simply to signpost the assessment in terms of distinguishing the high potential hazard areas. This provides the focus for the development of suitable design solutions to ensure that RWM safety criteria will be met.

The dose rates which are used in the initial assessment to confirm correlation with the PFD are the fully unmitigated illustrative values. These dose rates, calculated in the absence of GDF safety measures, are therefore a measure of the maximum harm potential. The unmitigated values do not represent the likely dose rates that would arise in a real GDF which will include sufficient safety measures in the design.

The future assessment of the radiological risks arising from normal operations will require the calculation of radiological doses post-mitigation, ie with the inclusion of safety measures claimed in a full safety assessment. For the normal operations safety assessment the calculation of the doses received by GDF operators will include all passive safety measures and safety functions included in the design. At the current generic stage, the plant and task design is not expected to be sufficiently detailed to allow such analysis to be performed and as such conclusions can only be drawn consistent with the nature of the assessment. This precludes any definitive statement in relation to acceptability of mitigated doses. However what can be stated are the specific performance requirements, in terms of dose-rate targets that will need to be met by optimising time, distance and shielding. Illustrative assessments have been undertaken for:

- bounding throughput years for waste streams

- the receipt and handling of high heat and low heat generating wastes
- the different worker groups that undertake specific tasks

The assessment is on the basis of the following assumptions:

- Operator doses under normal operating conditions will be dominated by external direct radiation exposures for which the surface dose rates from waste packages are known and well understood. Compliance with the limits and conditions in the Transport Regulations supports this assumption on the nature of waste packages.
- Operator doses from the inhalation pathway have not been calculated as:
  - Transport packages have strict limits on removable contamination levels on their surfaces in order to comply with the Transport Regulations as limited by the waste package specification and the appropriate release rates in accordance with the A_2 values (whichever is the most onerous). The design intent is that the GDF will be operated as a 'clean' facility, thus at this stage the risk of a dose through an inhalation pathway is judged to be negligible.
  - Air change rates arising from the ventilation systems will be higher than required by codes and standards for nuclear facilities due to the requirement to retain a workable environment underground for GDF operators. This further reduces the potential airborne contamination levels associated with any minor entrained contamination.
  - The gaseous radioactive release from packages is assumed to be negligible when compared with the external dose contributor.
  - Natural radon gas has not been assessed at this stage as the emanation rate will be highly dependent on the precise nature of the host rock and equilibrium air concentration and upon the local air change rate provided by the underground facility extract ventilation system which will be assessed at the site-specific stage[2].
  - Ingestion and injection pathways - doses to operators and other on-site workers are considered to arise during fault conditions and are therefore not assessed within the normal operations safety assessment.
- Doses to members of the public have been calculated only from aerial discharges based on RWM generic data on the behaviour of waste packages and the waste form under emplacement conditions. As such:
  - The contribution from external radiation, including skyshine from back scatter of neutron sources, has not been assessed as the provision of shielding in the transport package will limit offsite dose potential to levels that will be managed through refinement of the site layout. This shielding is required to meet the requirements of Transport Regulations and will remain in place during all surface handling operations.
  - Further work is required to ascertain the off-site dose rate from transport packages located on the surface, for example, in the buffer storage park[3].

---

2 The management of natural radon gas is subject to specific legislative requirements for the protection of personnel and is known to be manageable through the provision of suitable underground facility extract ventilation systems, which will be designed specifically for the GDF.

3 It is assumed that the design and operating philosophy will be sufficient to ensure that the contribution of external radiation is insignificant.

  - Doses from authorised liquid discharge points will be calculated when there is an appropriate level of detail of the composition of effluents (post-treatment), design of the effluent handling systems, and information on the potential sites such as topography. These are not expected to be significant due to the nature of operations undertaken at a GDF.

- Doses to operators and other on-site workers from ingestion and injection pathways are considered to arise only during fault conditions and are therefore not assessed within the normal operations dose assessment.

The normal operations safety assessment should, in principle, provide an assessment of both normal operations and anticipated operational occurrences to fully satisfy the NOSM. An anticipated operational occurrence is an operational process deviating from normal operation which is expected to occur at least once during the operating lifetime of the facility but which, in view of appropriate design provisions, does not cause any significant damage to items important to safety or lead to accident conditions. However, at the current illustrative stage, this assessment is limited to consideration of normal operations only. Additional details would be required, on specific operations and plant design, to assess anticipated operational occurrences.

5.2.3 Illustrative operator dose assessment

The dose assessment for GDF operators has been limited, at this generic stage of the OSC, to an assessment which is illustrative and is based on the tasks identified from the PFD. The general processes required in the GDF have been grouped to aid understanding and assessment of activities. This gives a reasonable understanding of the aggregate dose burden and a means of identifying issues which may be sensitive to assumptions of this nature. The assessment has been performed where there is the likelihood of direct exposure to radioactive sources or to elevated dose rates in the absence of design provisions.

Detailed assessments have been carried out for a combination of waste streams in waste package types for a throughput defined by the transport schedule in the 2013 Derived Inventory report. Process-specific dose calculations for these general operations have been undertaken based on bounding throughput years for the receipt and handling of high and low heat generating wastes. A set of aggregated task times and distances, with generic assumptions related to which group undertakes the tasks, have been used for calculations at this generic stage.

These illustrative assessments provide the basis to develop understanding and to inform future GDF design development. This supports all future optioneering, for which system requirements will need to be derived and robust engineering solutions developed.

The illustrative assessment comprises the following steps:

- Association of the tasks in the PFD with operations and assumptions (time, distance etc.) to describe the task input to the assessment.

- Application of the transport and operational dose assessment (TODA) toolkit, which is a model developed by RWM to enable calculation of the dose from the illustrative tasks and allocation to worker groups supporting the process as defined above in the PFD.

- Review of the output from the assessment and the ‘effort profile’ in order to confirm that it is consistent with the PFD before interpretation of the results. This ensures that the data used in the assessment are correctly associated to the activities that they relate to in the PFD, and that the output is used and clearly linked to design requirements.

- Where the fully unmitigated illustrative assessment shows that the doses for a man year of effort require reduction:

- Calculation of the attenuation (dose reduction) factor required for the activity/area where design optimisation can be applied.
- Confirmation that it is technically feasible for the illustrative solution to achieve the specified dose reduction factors based on the consideration of time, distance and shielding provisions.
- Support for the claims made by reference to nuclear facilities currently in operation which have similar dose reduction factor requirements to the GDF, to further demonstrate feasibility.

It should be noted that the results from this illustrative assessment are closely linked to the baseline assumptions within the BOA report. Results should be interpreted in the context of the BOA assumptions regarding time, distance and the presence of workers during operations. Additional findings from this illustrative normal operations safety assessment are as follows:

- The identification of 'pinch points' (ie where collective hours allocated to an exposed group exceeds the maximum hours available in a year), and relationship to process viability confirms the need to focus on and refine the data in a 'time and motion' type study. This will be an integral part of future design work. This will ensure a robust basis for the design, assumptions and the full safety assessment.
- The remote handling areas of the GDF (ie those areas with a high radiological dose-rate or cumulative dose which currently include the sub-surface inlet cell) have been identified and confirmed as consistent with the PFD.

Mitigated normal operations dose rates have not been calculated at this stage as it is not meaningful or appropriate to do so.

5.2.4 Illustrative public dose assessment

The Operational Environmental Safety Assessment includes illustrative calculations of the annual doses to a member of the public from aerial discharges. The total dose to members of the public from peak gas releases during the operational period is predicted to be significantly below the legal limit for members of the public. This is based on the reference case, with conservative assumptions appropriate to this generic stage. As a result, design optimisation will be undertaken in accordance with the RWM integrated design and safety process. Any actual radiological dose from off-site discharges from the GDF will be determined by site-specific factors and will be a function of actual gaseous discharge rates during each year of GDF operation in combination with local environmental factors and the location and habits of exposed groups. As part of the development of the detailed design, safety measures could be introduced to reduce the potential for gaseous discharges from the GDF. This would further reduce the risk of any off-site doses to a member of the public.

5.2.5 Concluding remarks

The extent to which the principal safety claim (OSC.SC2) has been demonstrated is summarised below.

The illustrative normal operations safety assessment presents evidence related to the process that has been followed, the scope of the assessment, nature of hazards identified requiring design provisions, regulatory expectation related to their control, and hazard management strategies that will need to be adopted to prevent or minimise the routine dose exposure.

The illustrative normal operations safety assessment concludes that there is very high confidence that it is feasible that the GDF can be designed and operated safely with radiological exposures and doses to the workforce and members of the general public which will be tolerable and as low as reasonably practicable (ALARP). In addition, the specific findings are as follows:

- RWM has developed a significant capability for assessing doses based on a functional PFD of the GDF. This allows the contribution to the overall normal operational dose burden by waste stream, package, location and schedule to be rapidly and clearly assessed with confidence. This capability enables an assessment of the viability of the GDF process based on man-effort requirements and identification of any ‘pinch points’. This represents a significant improvement in capability since the 2010 generic DSSC.
- Process areas, and their associated operations and locations, requiring engineered provisions have been identified. For example, where unshielded Intermediate Level Waste is to be handled, provisions such as shielded remote handling facilities or ‘hot cells’ will be implemented (within the current illustrative concept, this facility is provided by the inlet cell).
- RWM now has the capability to identify those areas of the GDF where future effort needs to be focussed on:
    - optimising the design, and
    - increasing the understanding related to process needs such as definition of detailed tasks performed by the operators
- The required dose reduction factors can be achieved through standard nuclear industry solutions. Proposed solutions will be derived through optioneering and appropriate task-design to ensure doses from normal operations in the GDF will be demonstrably ALARP.
- Annual doses to a member of the public from aerial discharges, based on peak gas releases during the operational period, are predicted to be acceptable and significantly below the legal limit.

It should be noted that this safety assessment identifies illustrative safety measures to meet the dose reduction targets. It does not conclude that those measures are the correct solution as this assessment has not yet been supported by suitable optioneering, including application of the ‘eliminate, prevent, protect and mitigate’ hierarchy. Neither is it assumed that legal requirements have been met in full at this generic stage.

In broad terms the processes and operations conducted at a GDF are functionally the same, or very similar, to those undertaken at numerous High Activity Waste (HAW) Storage and Handling Facilities in operation in the UK. Safety cases and ALARP arguments for the operation of such existing facilities are mature, the engineered systems required to reduce risks are well understood and as such future work will be focussed on implementing a proven solution within an engineered underground facility. This current UK experience, along with international GDF experience, gives high confidence that a suitable design solution can be developed such that the GDF can be operated safely. The design will need to consider the specific requirements of operating a nuclear facility in the sub-surface environment, which may present certain challenges which are relatively unique but are not expected to require novel technological solutions. The areas which require further work to fully underpin the principle claim are largely related to actual design development and the resolution of the forward action plans.

5.3 Volume 3: Accident Safety Assessment

5.3.1 Safety justification

The safety claims, arguments and evidence related to accidents are summarised in Table 7.

Table 7 Accident Safety Claims, Arguments and Evidence

Reference	Safety Claim	Argument	Evidence
Principal Claim			
OSC.SC3	All reasonably practicable steps will have been taken to implement design provisions whose function is to prevent or mitigate the consequences of radiation accidents.	At this generic stage, it is not possible to make a definitive statement regarding the ability of the design to meet the RWM safety criteria, including the ALARP requirement. The feasibility study however provides a level of confidence that RWM safety criteria can be met when the design is developed.	The safety analysis of the representative set of faults and the risk reduction review demonstrate that it is feasible that the faults can be managed to meet risk reduction targets. As such, there are no design basis faults which are considered to present a challenge to safety criteria. Hence the developed safety assessment is expected to demonstrate that doses from accidental releases will meet RWM safety criteria and that risks will be tolerable and ALARP. The group of faults associated with transfer underground have not been assessed as design basis faults because there is considerable uncertainty on behaviour of the waste package in the event of impact. These faults have however been assessed through the risk reduction review process to demonstrate that potential solutions are feasible and this issue is subject to resolution though FAP.2016.VOL3.03.
Supporting Claims			
OSC.SC3.1	A systematic hazard identification process has been and will continue to be applied to the GDF design.	The application of a systematic hazard identification process will provide a demonstration that a suitable fault set has been identified.	HAZOP studies have been undertaken for the activities defined in the PFD. As the design develops, more comprehensive and detailed hazard identification studies will be performed.
OSC.SC3.2	Hazards have been screened, grouped and bounded in order to derive a representative set of faults which have the same functional	The representative fault set comprises the bounding and most challenging faults, regardless of location, thus making it a suitable basis for	The screening and grouping approach adopted has examined the initiating events to identify the list of representative faults which have the same functional requirement on the design

Reference	Safety Claim	Argument	Evidence
	requirement on the design, regardless of location.	disposability advice and the feasibility study for the GDF.	regardless of location.
OSC.SC3.3	An initial DBAA has been performed based on conservative unmitigated radiological consequences and initiating event frequencies for the representative set of faults.	At the current stage, it is not possible or appropriate to undertake a full DBAA or any probabilistic analysis as there is insufficient design definition. The application of the DBAA approach to the most challenging faults permits fault classes to be derived and safety functions (together with associated requirements) to be specified.	Conservative assumptions have been made with regard to the harm potential of the fault. Based on these assumptions, the safety assessment calculates the illustrative fully unmitigated radiological consequences to operators and members of the public and initiating event frequency. The assumptions will be revisited as the design develops in order to provide a DBAA which is conservative but more applicable to the fault scenarios.
OSC.SC3.4	Faults have been classified and the equivalent outputs (safety functional requirements and safety measures) identified.	The NOSM requires that faults are assigned a fault class which then drives the need for safety functional requirements and safety measures to deliver these requirements through the design.	The unmitigated radiological consequences and initiating event frequencies have been calculated and illustrative fault classes assigned. Where the fault lies near the boundary of fault classes, the higher class has been assigned to ensure that the assessment is bounding. Faults associated with use of a shaft and the drift have not been assessed at this time and are subject to further design evaluation. Conceptual safety functional requirements have been identified together with the identification and classification of potential safety measures in accordance with the 'eliminate, prevent, protect and mitigate' hierarchy.
OSC.SC3.5	It is feasible and credible that the representative set of design basis faults will be adequately protected in the developing design	The fault analysis as applied to the most challenging faults demonstrates that it is feasible and credible that suitable safety measures can be	Conceptual safety functional requirements have been identified for the most challenging design basis faults. The 'eliminate, prevent, protect, mitigate' review has identified a

Reference	Safety Claim	Argument	Evidence
	and that risk reduction measures can be identified in line with the NOSM risk reduction hierarchy (eliminate, prevent, protect, mitigate) as an input to future option development.	identified which will meet the risk reduction targets and can ensure that the conceptual safety functional requirements can be delivered.	number of options for safety measures, the majority of which are standard nuclear industry solutions, capable of meeting the risk reduction targets. As such, there are very few safety measures that are not at a high technical readiness level for implementation in the design.
OSC.SC3.6	There is an understanding of the uncertainties and variability issues which can impact on the results of the safety analysis.	This important understanding has been developed through the assessment work undertaken to date. It includes the uncertainties in inventory data, assumptions and underpinning assessment data and the impact that these could have on the initial DBAA, in particular the fault classes. This work provides assurance that the results of the fault analysis are not sensitive to these input data.	For each fault sequence group, an analysis has been performed of the variability issues (those issues under the control of RWM) and uncertainty issues (those outside the control of RWM) and how these could impact on the fault class. A sensitivity analysis has been undertaken of the initial fault analysis and shows that the results of the analysis are not sensitive to the input data. The exception to this is the use of release fractions and containment factors which have the ability to make several orders of magnitude change to the results and hence the classifications (and the demands on the design). This is subject to resolution through FAP.2016.VOL3.17.
OSC.SC3.7	There are no feasibility issues in terms of technical achievability and/or ALARP justification that will impact on RWM's ability to operate the GDF safely.	The safety assessment provides confidence that the demands placed on the design can be satisfied, thereby demonstrating the manner in which future ALARP arguments could be made and underpin the present claim of feasibility of the GDF, regardless of geological environment.	From the set of most challenging faults assessed, none present a potential challenge to the feasibility arguments. Application of the NOSM hierarchy of risk reduction measures shows that for all faults assessed, there are potential safety measures which can eliminate the fault, reduce the likelihood of occurrence or reduce the radiological consequences. As such the risk reduction review process has identified a number of potential safety measures which, in combination, may

Reference	Safety Claim	Argument	Evidence
			be able to meet the conceptual safety functional requirements and the associated risk reduction targets.
OSC.SC3.8	There is an understanding that there are potential complexities and differences between the safety requirements associated with a nuclear permissioning regime and relevant good practice that would be applied in underground facilities such as mines.	RWM recognises that there are likely to be challenges arising from the different premises associated with the nuclear and underground working (such as tunnelling and mining) related regulatory regimes and this will need to be incorporated into the optioneering and design review process.	The potential challenges associated with the non-prescriptive approach of nuclear permissioning may create complexities with regulations for underground working where the regulations are more prescriptive and rule based. The developing design, in particular the optioneering process to identify engineered safety measures, will take this into account in the criteria applied to any optioneering and to the design review process in accordance with the RWM DASI (FAP.2016.VOL3.16).
OSC.SC3.9	There is an understanding of the nuclear safety challenges associated with operating a nuclear facility underground, including the transfer of waste packages from the surface to a deep underground environment.	The ‘uniqueness’ of the GDF is the combination of sub-surface operations and radioactive material and their inherent hazards. Challenges are associated with, for example, use of a shaft, underground fires, flooding and structural collapse. The hazard management strategies will set out the safety requirements that the design will be required to implement to ensure that potential hazards are removed entirely or, in the event that they cannot be eliminated, are negligible.	RWM is working with other countries around the world that are developing similar projects to learn lessons and develop safe solutions, for example through the Organisation for Economic Co-operation and Development (OECD) Nuclear Energy Agency projects.

Reference	Safety Claim	Argument	Evidence
OSC.SC3.10	There is confidence that it will be feasible to make the justification that risks to workers and members of the public from accident scenarios can and will be tolerable and ALARP.	The illustrative accident safety assessment provides confidence that the GDF can be constructed and operated safely and that radiological risk to the workforce and members of the general public will be tolerable and ALARP.	A systematic and proportionate hazard identification, screening and grouping process has been completed. A representative set of faults which have the same functional requirement on the design regardless of location has been derived. Fault sequence groups were identified for qualitative or quantitative assessment. DBAA was performed on those identified for quantitative assessment and conceptual safety functions and safety functional requirements identified. Illustrative safety measures have been identified which could meet the risk reduction targets arising from the DBAA.

5.3.2 Safety assessment approach

The principal safety claim (SC) to be demonstrated for the accident safety assessment is that:

OSC.SC3: All reasonably practicable steps will have been taken to implement design provisions whose function is to prevent or mitigate the consequences of radiation accidents.

The objective of the accident safety assessment at this stage of the Geological Disposal Facility (GDF) programme is to demonstrate that the most significant hazards and associated faults have been identified. This information is used to develop hazard management strategies, inform optioneering and improve understanding of the design and means of ensuring safety. This supports the claim being made now that the GDF will be safe to construct and operate. As a result, risks to the workforce and members of the public will be tolerable and as low as reasonably practicable (ALARP).

This safety claim is underpinned by application of the following structured approach:

- development of the Process Flow Description (PFD) to ensure full coverage of the functional processes at task level for emplacement of all waste package types
- application of a systematic hazard identification (HAZID) process to the PFD to identify radiological hazards and faults
- development of the preliminary fault schedule as the comprehensive list of faults which could lead, either directly or in combination with other failures, to a radiological consequence
- screening and grouping of the fault set to identify a set of generic fault sequence groups

- identification of the fault sequence groups which should be subjected to qualitative or quantitative assessment
- performance of an initial Design Basis Accident Analysis (DBAA) to identify the fault class of the design basis faults subject to quantitative assessment
- development of the conceptual safety functions and safety functional requirements for the design basis faults
- application of the Nuclear Operational Safety Manual (NOSM) risk reduction hierarchy to identify illustrative safety measures which could potentially meet the risk reduction targets arising from the DBAA

This approach is consistent with the methodologies set out in the NOSM, which is consistent with nuclear industry best practice.

This volume includes the forward action plans (FAPs) to demonstrate the feasibility of implementing the illustrative safety measures in the developing design.

5.3.3 Hazard identification and fault schedule development

A systematic hazard identification study has been undertaken. The study is based on the current BOA which presents the GDF concepts as a PFD and includes a high level description of the activities, plant and equipment and tasks which could be used to implement the required operational functions.

From the initial list of initiating events derived in the hazard identification studies, a level of grouping and bounding has been applied to rationalise the list of faults to a representative set. These faults have the same functional requirement on the design regardless of location. The results from an individual assessment then have a broader application. As a result, the representative sets of faults carried forward to the illustrative assessment are the faults that are considered both to be credible and to place significant requirements on the design.

At this stage of the GDF programme, there is insufficient design definition to permit a complete safety assessment for all accident conditions. The level of design definition required to undertake a full and final assessment would not be expected. At this phase, the appropriate approach is to focus on the most significant faults to support this feasibility study. The most significant faults were identified through hazard identification studies and have been assessed either quantitatively or qualitatively, as appropriate.

The assignment of fault sequence groups to quantitative and qualitative assessment in a number of Hazard Analysis (HAZAN) groups is set out in the table below.

Number	HAZAN	Comment	Type of Assessment
1	Loss of shielding	Faults which result in loss of shielding due to system or operator error resulting in unintended exposure to waste package contents	Quantitative
2	Loss of containment	Faults that result in elevated levels of radioactive material in air due to disturbance, accumulation or transfer of contamination	Not assessed - results in much lower consequences than the energetic containment loss events such as dropped loads or impacts which are the bounding cases

Number	HAZAN	Comment	Type of Assessment
3	Dropped load and impacts	Faults for both loss of integrity of shielding and loss of containment due to impact of waste packages or facility	Quantitative (with exclusions where waste package is in transport configuration)
4	Fire	Fire faults due to process or system failures	Not assessed (see Exclusions)
5	External hazard	Faults initiated by external hazards (not under the control of the operator (air/ground/offsite))	Qualitative as the assessment requires site-specific data and information
6	Internal hazard	Faults initiated by internal hazards (under the control of the operator (including fire)) that impact on delivery of other safety functions	Qualitative as the assessment requires more detailed design such as plant layouts
7	Criticality	Criticality faults initiated by geometry changes, addition of moderator or additional reflection, movement and accumulation of fissile material and out-of-specification packages are assessed within the generic Operational Safety Assessment: Volume 4	Not assessed in the accident safety assessment but assessed as part of Volume 4 – Criticality Safety Assessment. The criticality assessment concludes that criticality is not credible so no quantitative assessment has been performed.

5.3.4 Exclusions

The following fault sequence groups have not been assessed in the 2016 generic OSC and the justification for their omission is summarised below. FAPs have been raised to manage future work associated with these hazards.

- Nuclear fire: Nuclear fires are defined as a thermal event which occurs as a result of a nuclear event such as criticality inputting sufficient thermal energy to initiate a fire. The exclusion of these faults requires resolution of other FAPs related to dropped loads and stability of the structures below ground.
- Contaminated wounds: Detailed information on specific tasks (including maintenance) and plant operating philosophy (such as permissible or expected levels of contamination) is required to undertake meaningful assessment of such faults.
- Loss of off-site electrical power: Faults associated with the loss of off-site electrical power (LOOP), including long-term failures and the associated potential for ‘domino effects’ as a secondary impact, have not been assessed at this stage. As the radioactive waste is contained at all times whilst at the GDF, it is not anticipated that LOOP will result in a significant radiological hazard.
- Loss of ventilation: Faults associated with failures of ventilation plant have not been assessed at the present time as there is insufficient design definition of the ventilation systems to permit a meaningful assessment. Other issues related to conventional safety (ie flammable and noxious gases) are discussed in Volume 1.

- Contaminated liquid releases: Work has been undertaken in support of disposability assessments considering inadvertent exposure to elevated dose rates due to a leak of contaminated liquids, and the consequences are found to be below the low consequence threshold.
- Pressurised waste packages: It is currently assumed that packages will remain below pressures for which systems are required to manage the hazard and to which the Pressurised System Safety Regulations, 2000 apply.
- Loss of containment (spread of contamination): The harm potential from releases of loose surface contamination will be bounded by the more energetic dropped load and impact faults assessed within HAZAN 3. All faults in this HAZAN group are expected to be low consequence but will still require an appropriate set of design features to manage the hazard and demonstrate compliance with the ALARP principle.
- Fire: The application of a safety integrated design process in support of developing the full assessment will ensure that the fire hazard management strategy focuses on elimination and preventing spread. This will be required to ensure compliance with conventional safety requirements as discussed in Volume 1. Until this level of design development is complete, meaningful assessment cannot be undertaken. The hazard management strategy and design principles being developed now give confidence that the hazard can be controlled and risks of radiological consequences will be very low.

5.3.5 Design Basis Accident Analysis Process

At this stage of the GDF programme, the level of design definition limits the scope of the DBAA. However, an initial DBAA analysis can be undertaken to give an indication of the safety requirements that must be provided by the design or areas that would benefit from optioneering to support more meaningful assessment and improve understanding of design requirements.

The initial DBAA includes the calculation of the unmitigated radiological consequences to workers and members of the public and an initial conservative estimate of the fault initiating event frequency. The unmitigated dose is used as the basis of this assessment. This ensures effort is concentrated on those faults that are considered both to be credible and will place significant requirements on the design. This enables the initial fault class (from A [highest class] to B, C or D [lowest class]) to be determined. Following this, the requirements on the design (in terms of conceptual safety functions, safety functional requirements and risk reduction targets) can also be determined.

The detailed assessments present the fault class, safety functions and conceptual safety functional requirements (CSFRs) for the faults subject to numerical assessment. A hierarchy of safety measure selection must be applied to support the eventual ALARP assessment. As part of the feasibility demonstration, for each design basis fault, the risk reduction measures which could meet the requirements have been identified based on the hierarchy:

- can the fault be eliminated by modification of the engineered design or the process itself?
- if the fault cannot be eliminated, what risk reduction measures could be incorporated into the developing design to:
  - provide a means of preventing the fault from challenging the safety function
  - provide a means of protecting against fault development by terminating the fault sequence prior to a radiological consequence being realised
  - provide a means of mitigating the radiological consequences of the realised fault

The illustrative safety measures provided may be engineered or operational/procedural, and active or passive in their delivery of the safety function. The hierarchy to be applied is:

- engineered is preferred to procedural
- passive is preferred to active

The fault analysis has only considered faults during the transfer process from the surface to the underground facilities and the operations undertaken in the underground environment. All activities at the surface are carried out with the waste package in its transport configuration. As such, at the surface, appropriate controls will be in place 'by design' to ensure that there are no faults requiring further DBAA provision (ie a passively safe argument) or that initiating events capable of challenging this are excluded either 'by design' or shown to be not feasible (risk-based arguments for external hazards, for example). In addition, the operations to be undertaken at the surface are activities undertaken extensively on UK nuclear licensed sites and other sites overseas. This gives a high level of confidence that these operations are well understood with established codes and standards that apply to the buildings and equipment used within them to ensure that the risk of accidents is minimised.

5.3.6 Faults related to surface to sub-surface transfer

A group of faults included in the fault schedule are related to the drop (or uncontrolled lowering) of a waste package down the shaft. It is recognised that the current illustrative concept only considers a shaft for transfer of waste packages underground in the evaporite host rock geological environment, however, for the purposes of a bounding generic safety assessment, the shaft has been assumed to be used regardless of geological environment. The equivalent fault set for all waste types related to a drift has also been identified.

In the case of the drop of a waste package down the shaft, the hazard management strategy to be satisfied by resolution of the FAP (FAP.2016.VOL3.03) will be to explore all options to minimise the fault initiating event frequency to a level that is ALARP. This will be achieved by implementing a 'de-risked' engineering design of the load path, coupled with independent protective and mitigating safety measures which will ensure that significant radiological consequences cannot be realised. As these systems are not novel, are in use, or planned to be in use for the same application in other GDF projects, it is concluded that the use of a shaft does not present a feasibility issue for the UK GDF.

Illustrative risk reduction measures have been identified for consideration as the design develops and due account will be taken of international experience in similar GDF projects currently underway. Shaft designs are implemented in current or planned GDFs world-wide, developed from conventional mine winding systems (shafts are a proven technology used extensively as a means of accessing deep underground mines). RWM has recently visited DBE Tec in Germany where a full scale demonstration shaft winding unit has been operating for many years. This demonstration unit has generated detailed reliability data and fault evaluation data from a fully prototypic facility design for large scale flask transfer in a vertical shaft. This full scale demonstration has enabled the production of a full modern standards safety case (including both deterministic and probabilistic analysis) that shows acceptable risk for both workers and members of the public. This type of overseas evidence gives RWM high confidence that a safety case can be made for the transport of waste in a vertical shaft, and that the activity can be demonstrated to be tolerable and ALARP.

A shaft system at the UK GDF would be based on relevant good practice and incorporate up-to-date control, monitoring and safety equipment to reduce the risk of, and mitigate accident situations. It is acknowledged that the use of shafts for waste package transfers will require detailed safety assessment and design substantiation in order to meet the UK nuclear regulatory requirements.

5.3.7 Results of Design Basis Accident analysis

The initial DBAA has identified and assessed a total of 11 bounding faults which comprise two class B, eight class C and one class D fault. The class B faults represent the most significant in terms of the DBAA and involve loss of disposal unit containment following stack collapse within a vault. The assessment has determined that there are no faults that would potentially lead to off-site doses to the public in excess of design basis thresholds.

The hazard management strategy to be applied to the developing design is that all faults designated as class A or B should be eliminated by design as a first priority. In the case of the class B faults identified above, options are available to eliminate the fault by a change of emplacement strategy or to introduce suitable preventative, protective and/or mitigative safety measures, which will be evaluated through the developing design.

For the class C dropped load and impact faults, credible design solutions have been identified to meet these requirements and are typical of those implemented in UK nuclear licensed facilities where comparable operations are undertaken.

The bounding design basis loss of shielding faults are all class C or D. The risk reduction targets could be achieved by design solutions typical of engineered safety measures already provided in UK nuclear licensed facilities (such as area gamma monitors/alarms and interlocks) where comparable operations are undertaken and are therefore considered feasible.

5.3.8 Feasibility of meeting RWM safety criteria

Options for risk reduction have been identified for those faults subject to DBAA. They are presented in terms of engineered safety measures already implemented or in use for comparable operations at currently operating facilities. This demonstrates that the means of meeting risk reduction targets are credible and feasible to implement.

5.3.9 External hazards

The methodology applied in the assessment of external hazards is appropriate for the generic stage at which the location of the GDF site is unknown. The baseline set of external hazards applicable to the GDF in the UK has been identified and, where possible, illustrative design basis event magnitudes defined. In addition, combinations which occur simultaneously or nearly simultaneously have been identified (correlated hazards). The external hazards (including correlated hazards) provide a basis that will be taken into account as the siting process and GDF design develops. The bounding external hazards fall into the following groups:

- external (natural) hazard, such as high wind load, high precipitation, snowfall, high/low temperatures
- external (man-made), such hazards presented from adjacent site or facility
- seismic events
- flooding of sub-surface facilities induced by, for example, a seismic event

The design basis event magnitudes were determined for the initial generic set of external hazards using applicable standards and methodologies as collated and referred to in the NOSM. As it is impractical to define external hazard design basis events for every possible GDF location, the assessment divides England and Wales into six regions. This division is based on those hazards for which the available data show regional variation.

The external hazards assessment demonstrates that those hazards applicable to the GDF are understood. The magnitudes of a range of external hazards (above-ground only) for England and Wales have been determined on a regional basis. The analysis shows that there is regional variation throughout England and Wales but there are no cases where the variation is sufficient to require different design standards to be applied or to present a challenge to the feasibility of implementing a GDF. The assessment will be extended to cover Northern Ireland as the siting process progresses.

Hazard management strategies will be developed for external hazards (FAP.2016.VOL3.02) which will set out the safety requirements that the design will be required to implement through suitable design principles. This will, in turn, drive the need for design development from which design solutions to manage external hazards will be developed.

5.3.10 Internal hazards

The assessment of internal hazards requires a greater level of design definition than is currently available. Recognising that internal hazards might lead to the loss of a structure, system or component providing a safety function, illustrative safety functional requirements have been reviewed to determine the nature of the vulnerability and potential effect on safety.

The conclusions from this will be used to inform the hazard management strategy and design development process.

The most challenging internal hazards identified in the preliminary fault schedule are as follows:

- internal fires and explosions, resulting in damage to infrastructure, structures, waste packages or loss of services
- internal flooding, resulting in loss of services such as electrical supplies or ventilation
- collapses, rockfalls and other structural effects as a result of construction activities or defects

The hazard management strategies will set out the safety requirements to be implemented in the design, such as exclusion, segregation and minimisation to ensure that potential impacts are removed entirely or, in the event that they cannot be eliminated, are negligible.

5.3.11 Concluding remarks

The extent to which the principal safety claim (OSC.SC3) has been demonstrated is summarised below.

The accident safety assessment provides confidence that RWM understands the most significant radiological hazards that could challenge claims of feasibility. These most significant hazards will form the basis of disposability advice by placing requirements on the package design supporting the future GDF safety case. This is an ongoing area of collaborative working between RWM and current holders of the UK Radioactive Waste Inventory. Many faults will be resolved by ‘designing out’ the hazard through implementation of industry-standard solutions, so do not warrant detailed consideration. Longer-term challenges such as those related to the drift and shaft will draw on international experience from projects at more advanced stages. There is clear evidence from a number of foreign waste management GDF programmes that credible and acceptable solutions already exist. As the design develops, further design-specific faults will be identified and addressed appropriately.

Operations at the GDF will be very similar in nature to those undertaken throughout the nuclear industry in the UK, Europe and worldwide. The operations are associated with the transportation, lifting and inspection of waste packages and radioactive material. The design will need to consider the specific requirements of operating a nuclear facility in the sub-surface environment, which may present certain challenges which are relatively unique but are not expected to require novel technological solutions. RWM is working with other countries around the world that are developing similar projects to learn lessons and develop safe solutions, for example through the Organisation for Economic Co-operation and Development (OECD) Nuclear Energy Agency projects.

This initial assessment provides a high level of confidence that the means of meeting the safety demands placed on the GDF are feasible (with today's technology) and that the GDF will be safe to operate. This claim is subject to further design development and safety assessment and the resolution of the forward action plans. A number of issues are unique to the GDF and are the subject of FAPs:

- optioneering and design development of technology currently in use to access or work in underground facilities, or planned for use in other GDF projects, to provide confidence that RWM safety criteria will be met
- at the present time, internal hazards have been assessed qualitatively because safety measures, their locations and requirements have not been identified in sufficient detail to undertake a detailed assessment. Although no site has been identified for the GDF, there are general features regarding internal hazards that are relevant to the generic stage
- working in a deep underground environment with the hazards associated with nuclear and radiological materials
- the structural stability and associated reliability claims of the tunnels and vaults deep underground, all of which will require more detailed assessment and design development
- further work will be required for external hazards when specific candidate sites are selected

In conclusion, the illustrative accident safety assessment provides confidence that the GDF can be constructed and operated safely and that radiological risk to the workforce and members of the public will be tolerable and ALARP.

5.4 Volume 4: Criticality Safety Assessment

5.4.1 Safety justification

The safety claims, arguments and evidence related to criticality safety are summarised in Table 8.

Table 8 Criticality Safety Claims, Arguments and Evidence

Reference	Safety Claim	Argument	Evidence
Principal Claim			
OSC.SC4	All reasonably practicable steps will have been taken to implement design provisions whose function is to prevent or mitigate the consequences of nuclear accidents (ie unplanned criticality).	Criticality safety is assured through the highly conservative package limits with large safety margins. The double contingency approach applies to accident conditions; for a criticality event to occur, two unlikely and independent failures would have to occur concurrently.	The assessment has shown that, for the bounding faults assessed in the operational phase, two unlikely, independent, concurrent changes in the conditions essential to criticality safety must occur for a criticality event to happen. There is a single exception case for a specific spent fuel waste stream for which a design package is yet to be designed and the design will need to confirm that the package will be deterministically safe.
Supporting Claims			
OSC.SC4.1	The GDF will be designed and operated safely with regard to criticality hazards. The key criticality safety issues associated with specific fault sequences have been identified and plans for resolution are in place.	Only double failure of contingencies could result in criticality. The likelihood of such scenarios is very low. The nature of the waste material is inherently unfavourable to criticality and the failure of controls on waste packages would not result in a critical configuration, either in individual packages or in combination.	Design basis fault analysis has shown that if multiple ILW packages are breached, packages would have to release all fissile material into an optimum geometry with optimum moderation and reflection for a criticality event to occur. The facility will be designed to ensure that such events are not possible. HLW contains insufficient fissile material to present a criticality risk. In addition, the nature of the vitrified waste form is well mixed and passively safe. The Disposability Assessment process applies highly conservative, worst case package limits. All conceivable fault conditions involving a single package are within these limits.

Reference	Safety Claim	Argument	Evidence
OSC.SC4.2	It will not be possible for normal operations to give rise to a criticality incident provided there is compliance with the conditions in the relevant disposability assessment.	Compliance with the limits and conditions associated with waste packages provides assurance that a criticality incident cannot occur during normal operations. Furthermore, there are large safety margins between package limits and criticality safety limits. For an 'out of specification' package to cause a criticality during normal operations, it would need to be sub-critical in the waste packagers' facility, yet have potential for sufficient increase to become critical due to GDF operations.	Waste packagers are responsible for the criticality safety assessment associated with the packaging and storage of their wastes including providing assurance that the limits and conditions (including fissile limits, moderators, etc) imposed on the waste packages cannot be breached. Compliance with the limits and conditions will therefore ensure that a criticality event within the GDF is not possible. Large safety margins make a criticality event during normal operation highly unlikely. The event that a package changes from sub-critical to critical is very unlikely because of the relative immobility of waste inside most packages and the robustness of the packages themselves.
OSC.SC4.3	A criticality warning system will not be required in the GDF.	Criticality accidents with the potential to give rise to significant doses to the operators or members of the public will be sufficiently low in likelihood that a criticality warning system will not be required. At the generic stage, this argument is preliminary only and will require full re-assessment when there is more design definition available.	The nature of the waste material is inherently unfavourable to criticality and the failure of controls on waste packages would not be reasonably expected to result in a critical configuration. The nature of normal operations in the GDF would not reasonably be expected to result in a change of configuration from sub-critical to critical. This initial assessment will be revisited as the design develops.

Reference	Safety Claim	Argument	Evidence
OSC.SC4.4	Prior to seeking approval to operate, it will have been demonstrated that it will be possible to implement a robust design that classifies rockfalls and structural failures as beyond design basis faults.	Compliance with industry codes and standards for tunnels and vaults will provide engineering basis for ensuring that suitable and sufficient measures are included such that structural failures are of sufficiently low probability to be deemed beyond the design basis.	Design will demonstrate that appropriate civil support structures will deliver reliability commensurate with the claim which will be substantiated as meeting the requirement.

5.4.2 Safety assessment

The principal safety claim (SC) to be demonstrated for the criticality safety assessment is that:

OSC.SC4: All reasonably practicable steps will have been taken to implement design provisions whose function is to prevent or mitigate the consequences of nuclear accidents (ie unplanned criticality).

A criticality accident is an unplanned and uncontrolled chain reaction that results in a sudden release of energy and radiation. It can only occur when fissile material is present. A criticality accident can cause structural damage to the waste matrix and the immediate package. As a result, doses of radiation in the immediate vicinity can be harmful if no safety measures are provided to alert workers to the onset of an event and/or reduce the dose to safe levels. As the GDF will contain wastes with fissile material, the safety assessment must demonstrate that the magnitude and likelihood of a criticality accident is less than the regulatory and RWM safety criteria.

At this stage of the GDF programme the focus is on identifying key issues that need to be addressed in developing a criticality safety case. This approach is appropriate where the aim is to demonstrate that the management of significant hazards is possible. The level of assessment is appropriate for the current design development stage of the GDF; it is a feasibility study. The assessment summarises key aspects of criticality safety and presents specific arguments for fault conditions and criticality warning systems. No numerical assessments have been carried out due to the current illustrative nature of the design.

The criticality safety assessment includes emerging capability to identify waste streams that could credibly exceed their safe fissile mass limit. High uncertainty in the package contents is one factor in particular in this assessment. The capability will be developed further, and such packages assessed in greater depth, to ensure that any areas of uncertainty that would affect compliance with the safe fissile mass limits are understood and documented. The safety assessment also considers the Disposability Assessment process, the potential impact of ‘out of specification’ material and the credible faults identified in the preliminary fault schedule.

The assessment covers normal operations and design basis fault conditions. For normal operations, compliance by waste packagers with fissile limits will ensure that a criticality accident within the GDF is highly unlikely. The safety margins within fissile material limits will ensure that ‘out of specification’ waste packages do not pose a risk.

The design basis faults have been reviewed and the conclusions of the assessment are presented below.

Beyond design basis accidents (BDBA) such as rockfall are included in the preliminary fault schedule. Hazard management strategies discussed in Volume 1, will ensure that the facility is 'passively safe' in terms of disposal activities. This will include installation of robust rock support systems during construction. The safety argument is supported by all the factors included in setting fissile limits such that the risk is very low in all circumstances.

Low Heat Generating Waste

For ILW, the fissile concentration in most of the conditioned waste is typically well below the level where criticality risk is a concern. Uncertainty and variability in the wasteform is accounted for when safety limits are set, by making conservative assumptions. The Disposability Assessment process provides the mechanism for checking that appropriate criticality controls are proposed and applied. Waste producers are required to develop criticality compliance assurance documentation that demonstrates how their procedures ensure the safe fissile masses will not be exceeded (now or in the future). Auditing of the waste producers' systems and procedures for the control of the fissile material content of waste packages is an integral part of demonstrating that the risk will be low.

Criticality in a single waste package is not possible during the operational period of the GDF due to the following factors:

- limits set on fissile package contents
- waste contains fissile nuclides distributed at low concentration with other non-fissile materials, so there would be very little neutron interaction between packages
- fissile limits are set assuming that the packages will be stored in arrays in the worst configuration. This means that any actual emplacement of the waste in large arrays within the GDF will not lead to a criticality

Dropping a waste package from a height much greater than its withstand capability could lead to failure of the package and a change of geometry, including redistribution of the contents. This will lead to a decrease in reactivity. Even if there was accumulation of fissile material in a single location this will still not exceed the criticality safety criterion.

The assessment has shown that the following sequence of events would result in the greatest criticality risk:

1. Failure to package waste in accordance with waste acceptance criteria, and
2. Failure to identify the deviation from waste acceptance criteria, and
3. Shipment of the 'out of specification' package, and
4. Emplacement with other 'out of specification' packages, and/or
5. Addition of moderator

More generally, two unlikely, independent, concurrent changes in the conditions essential to criticality safety are required for a criticality risk to occur (the 'double contingency' principle) and hence the likelihood is very low. Following the production of the procedures and processes at the waste producers' plants and at the GDF, the criticality safety arguments will be fully developed and a safety justification produced.

High Heat Generating Waste

HLW contains insufficient fissile material to present a criticality safety concern as the fission products have been separated from re-usable fissile material. In addition to the well mixed and passive nature of the vitrified wasteform, the concentration of fissile material per package is very low.

For spent fuel, the fissile concentration in the wasteform will be significantly higher than that found in ILW. However, there are other features of the wasteform and package design which contribute significantly to criticality safety:

- the wasteform will normally contain significant amounts of neutron absorbers and diluents in the form of U-238 and fission products
- packaging, storage and transport of spent fuel are mature technologies supported by safety assessment methodologies based on many decades of industrial experience at reactor sites and reprocessing centres
- the wasteform is well defined with less variability and uncertainty than ILW
- packaging arrangements could include, for example, the presence of fixed neutron absorbers in the container and internal furniture to maintain sub-critical configurations during GDF operation
- the robust wasteform and waste package prevent rearrangement of fissile material into an unsafe arrangement

For separated plutonium residues and highly enriched uranium, the wasteform will be engineered to provide a well-defined and stable material and where necessary, will include neutron absorbing material. The processed waste within the disposal container will be designed to be passively safe under any credible accident conditions that may occur during on-site storage, transport or emplacement at the GDF. The potential for post-event distribution and accumulation of spent fuel, for example on filters and sumps, has not been assessed at this stage.

For the majority of spent fuel, a major disruptive event leading to a change in geometry and the addition of water is required for a criticality accident. For fresh or low burn-up fuels, a criticality accident would require failure of the disposal container combined with loss of a system preventing flooding. Both of these examples meet the double contingency principle, ie, the independent and unlikely events of rockfall and an inrush of water would both have to occur concurrently for a criticality event to take place.

Dounreay Prototype Fast Reactor fuel is a potential exception as it has higher enrichment and therefore the potential to create a criticality without addition of a moderator. This fuel will require specific consideration as the waste package design is developed. It should be noted that the amount of fuel in a package will be limited to meet other requirements, for example to limit heat output and ensure post-closure safety.

5.4.3 Criticality warning systems

The illustrative criticality safety assessment has included an initial review of the requirements for the provision of a criticality warning system in line with regulatory guidance and the NOSM. The initial assessment concluded that a criticality warning system including a criticality incident detection and alarm system will not be required in the GDF. The nature of the packaged waste material is inherently unfavourable for criticality and a control failure on waste packaging will not result in a critical configuration. Normal operations in the GDF will not result in a change of configuration from sub-critical to critical, mainly due to the immobility of waste inside most packages and the robustness of the packages themselves. This conclusion will be kept under review as the design develops.

5.4.4 Concluding remarks

The extent to which the principal safety claim (OSC.SC4) has been demonstrated is summarised below.

The illustrative criticality safety assessment presents evidence related to the process that has been followed, the scope of the assessment, nature of hazards identified requiring design provisions, regulatory expectation related to their control, and hazard management strategies that will need to be adopted to prevent or minimise the consequences of criticality accidents.

The nature of the waste material is inherently unfavourable to criticality and the failure of controls on waste packaging would not result in a critical configuration, either in individual packages or in combination. Normal operations at the GDF would not result in a change of configuration from sub-critical to critical.

Fissile mass limits for waste packages and the criticality assessments that underpin the derivation of any limits are based on conservative assumptions. As a result, there is a significant safety margin between the fissile mass limits and the minimum critical masses required for a criticality. Normal GDF operations cannot give rise to a criticality incident provided the safety margin is maintained to ensure that there are no cliff edge effects.

Design basis fault scenarios have been reviewed and the double contingency approach applies; for a criticality event to occur, two unlikely and independent failures would have to occur concurrently. The likelihood of this is very low. The assessment also indicates that a criticality warning system is unlikely to be required on this basis. Following the detailed definition of the procedures and processes at the waste packagers' plants and at the GDF, the criticality safety arguments will be fully developed and a full assessment undertaken.

RWM recognises its responsibility to reduce the likelihood of criticality at the GDF to meet relevant criteria and standards and to reduce the likelihood of criticality accidents to a level that is tolerable and ALARP. No significant obstacles to making future claims for compliance with targets for tolerability of risk or the ALARP principle have been identified. Areas that require further work to fully underpin the principal claim are related to design development, including the design of waste packages and detailed package-specific criticality safety assessment and the resolution of the forward action plans.

5.5 Multiple or paired consequences from accidents

It is recognised that there is the potential for multiple or paired consequences to operators and members of the public to arise from some fault conditions. For example, the radiological safety assessment could determine that the radiological consequences from a particular process or fault are low and therefore screen the relevant hazards from further assessment, whereas the risk posed by the conventional hazard is high. Alternatively, safety measures implemented to control the risks from conventional hazards could make the radiological consequences worse (or vice versa).

As an example, in the event of a fire underground, the radiological hazard is relatively low in comparison to the conventional hazard. Accidents involving fires deep underground have the potential to lead to fatalities and serious injuries due to the fire itself, smoke inhalation and structural failures which could be far greater than any radiological consequences. Therefore for fires, the focus should equally be on the conventional hazard management strategy as well as the radiological hazard. Thus, the design approach will be to prevent loss of life by preventing fires occurring in the first place. This requirement will also meet the radiological safety requirement.

Another example is flooding in an underground environment. Any radiological consequences would only be realised after a significant delay (once waste packages started to fail). However, the potential for operator fatalities from drowning or detrimental effects associated with plant and equipment in the water and the secondary consequences ('domino effects') is much greater. Clearly hazard management strategy should prioritise protection of life from the dominant hazard. This approach will invariably address both the conventional and radiological hazard, ensuring a holistic approach.

A third example is the hazard associated with the handling of heavy loads and the related emplacement issues. Where heavy loads, such as waste packages, are lifted and lowered into position in a specific location such as an emplacement vault, there is a concurrent radiological hazard associated with the dropping of a package and a conventional hazard that could lead to fatalities and serious injuries regardless of the radiological impact. For both conventional and radiological hazard management, heavy lifts at height and storage in unsupported stacks should be minimised and, where possible, operators excluded from the area. Implementation of this concept impacts on the category of safety functions and the safety measure classifications associated with lifting and emplacement equipment and will impact on the emplacement and backfill strategy. A FAP has been raised to address this issue (FAP.2016.MR.04).

Design development in accordance with the RWM DASI process will ensure that a balanced design and safety assessment is implemented to manage the 'paired' risk.

5.6 Relevant industry experience

At this stage of the GDF programme the level of design definition limits both the scope and the detail of the assessment. However, it should be recognised that the handling and storage of radioactive waste is a well understood and highly practised activity, both within the UK nuclear industry and world-wide. For example, the use of fully shielded, remote handling facilities as a solution is common throughout the nuclear industry and there currently exist similar facilities for the handling and storage of HHGW and LLGW at many sites within the UK. Given that the operations proposed for the GDF are likely to be very similar to those undertaken at nuclear sites handling and storing radioactive waste, including the use of similar safety measures, the historical doses received by operators at these site are directly relevant to the feasibility demonstration. For example, data are collected and reported by all UK nuclear site licensees on the average annual doses to operators from a number of facilities including those which process, handle and store radioactive waste. In all cases, average doses are below 2.5 mSv/year for radiation workers; this demonstrates the effectiveness of both engineering provisions and managerial controls in the management of radiological exposures. As the developing GDF design will focus on the use of proven solutions, it is reasonable to expect that annual doses can be managed to such levels.

As a result, this relevant nuclear industry experience gives a high level of confidence that suitable design solutions exist and can be developed such that the GDF can be operated safely. The design will need to consider the specific requirements of operating a nuclear facility in the sub-surface environment, which may present certain challenges that are relatively unique but are not expected to require novel technological solutions. In addition to UK experience in the management of radioactive waste, due account will be taken of on-going and developing international programmes, which will aid in demonstration of the feasibility of design solutions identified for the GDF. RWM is highly committed to participation in international collaboration and development programmes such as:

- the International Association for Environmentally Safe Disposal of Radioactive Materials
- the 'Club of Agencies' - a group of European radioactive waste management organisations, set up to exchange information on all aspects of radioactive waste management
- the European Commission Implementing Geological Disposal - Technology Platform
- bi-lateral agreements
- technology transfer projects such as with SKB (Sweden) and Andra (France)
- the Nuclear Energy Agency – Radioactive Waste Management Committee
- the International Atomic Energy Agency

In addition, as the GDF design develops, due account will be taken of licensing, construction and operating experience in the following directly relevant disposal projects:

- the Posiva spent fuel disposal facility project in Finland which has been granted a construction licence by the Finnish nuclear regulator and within which spent fuel disposal is expected to commence in the next decade
- the spent fuel repository project at Forsmark (Sweden), for which regulatory approval to construct has been granted but is awaiting approval from the environmental courts - work on the construction is expected to start in the early 2020s with operations scheduled to commence in the 2030s
- the Bure Meuse/Haute-Marne Underground Research Laboratory (France) which commenced underground research in the 1990s as a precursor to granting a construction licence for the GDF for LLW, ILW, HLW and spent fuel in 2018 with emplacement operations planned to commence in 2025
- the US Waste Isolation Pilot Plant project which was developed for transuranic materials arising from the US military programme which had operated for over 10 years until an underground fire and a waste package fault resulted in closure of the facility by the US Nuclear Regulatory Commission – WIPP resumed waste emplacement operations in January 2017

In addition, due account will be taken of the experience of other countries currently embarking on a national radioactive waste disposal programme which includes Argentina, Canada, Czech Republic, Switzerland, Germany, Japan, Belgium, Netherlands, South Korea and Spain.

6 Implementation

In addition to providing confidence in the feasibility of the GDF, the generic OSC is used to:

- support packaging advice, discussed in Section 6.1 below
- set Forward Action Plans, discussed in Section 6.2 below
- develop design requirements, discussed in Section 3.4.1

These are discussed below.

6.1 Packaging advice

The generic OSC generates requirements, needs and information that are then implemented in the packaging advice given to waste producers. The following steps are undertaken for new waste packaging submissions:

- determine whether the submission presents any new hazards not previously considered in the generic OSC
- where new hazards are identified, assess regulatory requirements, develop hazard management strategies and define design principles
- determine whether the new packaging submission is within the current design capability through consideration of the harm potential on- and off-site
    - where there is a higher harm potential relative to the current baseline, this may represent a new bounding source term
- review the fault classes to determine whether there is a substantive change to the design requirements
    - if the fault class moves to class A, this represents a potential feasibility issue that requires resolution either through substantial improvement to the package or the philosophy of the GDF design and operation
- undertake a review of the fault class to ensure that the design demands are effectively implemented
    - where the fault class increases from class D to C or B, additional safety measures will be required in the design
- substantiate the safety claims to confirm that the required design features are feasible to implement
    - where a qualitative argument can be made that supports the safety claims made in the generic Operational Safety Assessment, the package is acceptable to the GDF

6.2 Forward actions

The safety assessment has identified a number of areas which will be the focus of detailed optioneering and design development activities to support a full definitive assessment. The FAPs presented here (Table 9) relate to:

- key process assumptions
- design detail
- assessment methodology
- uncertainties or variabilities in any of the above.

In addition to the FAPs listed in, each of the supporting volumes of the generic OSC contains a schedule of FAPs relevant to that topic area. A schedule of these FAPs is included as Appendix A.

FAPs identified in Volumes 1 to 3 (ie the construction and non-radiological assessment, the normal operations assessment and the accident assessment) relate to establishing design requirements and assumptions, developing hazard management strategies and setting detailed design principles. Volume 4 (criticality assessment) identifies FAPs relating to fissile limits and compliance.

Table 9 Forward Action Plans Specific to Main Report

FAP ID	FAP Description
FAP.2016.MR.01	Undertake an optimisation study of the emplacement areas, develop corresponding plant layout drawings and review the fault schedule. The aim of this is to minimise the risk of an incomplete fault set and incorrect specification of safety measures.
FAP.2016.MR.02	Develop and implement a construction and non-radiological safety assessment process. The aim of this is to ensure that conventional hazards are subject to an appropriate and proportionate level of analysis which ensures a design that gives due consideration to conventional, radiological and environmental hazards.
FAP.2016.MR.03	Develop a preliminary maintenance strategy. The aim is to ensure EIMT requirements, including access and egress to equipment, are sufficiently understood and accounted for in the design and safety assessment.
FAP.2016.MR.04	Review the lifting & emplacement strategy. The aim is to minimise the risk of damaging the package during lifting, stacking & emplacement.
FAP.2016.MR.05	Ensure arrangements can be put in place to minimise the risk of waste packages being received at the GDF that do not meet waste acceptance criteria.
FAP.2016.MR.06	Extend the PFD to cover the full GDF lifecycle, and develop it to clarify the waste emplacement routes. The aim is to ensure a definitive PFD is available for the developing design to ensure the hazard and fault set are correctly aligned to GDF processes.
FAP.2016.MR.07	Undertake optioneering and optimisation studies of the plant layout and construction plan. The aim is to minimise the risk of events occurring during underground construction giving rise to hazards relating to waste emplacement activities, and vice versa.
FAP.2016.MR.08	Undertake a study to determine the conditions that could give rise to a criticality event within an HLW disposal unit. The aim is to improve understanding of credible criticality faults for HLW/spent fuel disposal units.
FAP.2016.MR.09	Review the effectiveness of the NOSM, having learnt from the experience of producing the generic OSC, and implement a plan to update the NOSM as necessary.

The manner in which implementation of the FAPs will be managed and controlled has yet to be agreed. The FAP schedule will be linked to the Science and Technology Plan which will be the vehicle for implementation and close-out of the FAPs. Progress on the implementation of the FAPs will be monitored, reported and reviewed by the design and safety assessors through RWM's DASI process. All future work associated with the development of the OSC will be managed as part of RWM's 'Technical Programme' which is a key element of the overall GDF Programme.

7 Conclusions

This assessment work undertaken in producing the generic OSC Main Report has:

- applied methodologies specified within the NOSM to the assessment of normal operations, radiological accidents and criticality safety assessments in line with regulatory expectations and current practice in the UK nuclear industry
- performed an assessment of normal operations, determining the illustrative radiological dose to operators and comparing with legal requirements and RWM safety criteria
- undertaken a systematic hazard identification process, followed by:
    - a screening and grouping exercise to form a representative set of the most challenging faults for assessment
    - an illustrative qualitative and quantitative assessment of hazards to provide the basis for hazard management strategies and associated design principles, as the basis for the development of the design
    - identification of conceptual safety functions and safety functional requirements for the assessed faults, together with identification of safety measures in accordance with the NOSM risk reduction hierarchy in order to demonstrate the feasibility of meeting risk reduction targets
    - identification of design requirements and shortfalls; this included a series of design and safety integrated project team meetings for bounding fault assessments subjected to initial design basis accident analysis

The generic OSC concludes that the GDF will be safe to construct and operate. The main findings that support this claim are:

- credible hazard management strategies can be developed to ensure that risks to workers and members of the public will be tolerable and ALARP
- the means of meeting these needs are not novel; they are based on technology available now that delivers tried and tested above ground solutions in a below ground environment
- the means of ensuring packages meet GDF requirements is already in place and operating through the Disposability Assessment process

Areas of future work to support design development and the preparation of the full and definitive assessment are defined in the FAPs. The general themes, which act as signposts for future design development, relate to establishing design requirements and assumptions, developing hazard management strategies and setting detailed design principles. The criticality assessment identified FAPs relating to fissile limits and compliance with those limits.

Specific findings for each area of the assessment are:

Construction and non-radiological assessment:

- Hazard management strategies will need to be developed and design principles defined, and these will be implemented by means of the design and safety integration approach. It is expected that the identified hazards will not warrant further consideration as design basis accidents in the operational phase.
- Sufficient confidence has been gained that the most significant conventional and non-radiological hazards have been identified, and that it will be possible to put in place sufficient and adequate controls and arrangements for the management of these

hazards. As such no challenges to the feasibility of constructing and operation the GDF are expected.

Normal operations safety assessment:

- Optioneering and design development will be required to optimise normal operational procedures. This will required improvements in the data and assumptions used in the assessment.
- The assessment has provided a high level of confidence that a means of meeting the safety demands placed on the GDF are feasible (with today's technology) and that the GDF will be safe to operate.

Accident safety assessment:

- Optioneering and design development will be required to provide confidence that RWM accident safety criteria will be met. The design development will include the adaptation of existing technology to GDF underground facilities.
- The most challenging internal hazards identified are internal fires and explosions leading to damage to infrastructure, structures, waste packages or loss of services; internal flooding resulting in loss of services and rockfalls as a result of construction activities. The hazard management strategies will set out the safety requirements to be implemented in the design, such as exclusion, segregation and minimisation to ensure that potential impacts are removed entirely or, in the event that they cannot be eliminated, are negligible.

Criticality safety assessment:

- The GDF will be designed and operated safely with regard to criticality hazards and plans for resolution of identified issues are in place. The nature of the waste material is inherently unfavourable to criticality and the failure of controls on waste packages would not result in a critical configuration, either in individual packages or in combination.
- Further work has been identified to confirm that procedures, processes and controls are sufficiently comprehensive and robust, and that base assumptions related to package criticality limits can be verified from measurements or records.

The operations proposed within the GDF are, in general, activities that are tried and tested over many decades of nuclear operations world-wide. There are radioactive waste packaging, handling and storage facilities located on most of the UK's nuclear sites, including some with operating experience dating back to the start of the nuclear industry in the late 1940s. The proposed operations within the GDF are, in general, activities that are tried and tested over many decades of nuclear operations world-wide. In addition, there is considerable experience of underground working including tunnelling and mining which can be incorporated within the GDF project. As such, the current GDF concept does not propose any new or novel activities and therefore is considered not to present any challenges to the feasibility of operations; RWM understands what needs to be done to develop the design to ensure that the GDF can and will be operated safely.

In addition to UK experience in the management of radioactive waste, due account will be taken of on-going and developing international programmes, which will aid in demonstration of the feasibility of design solutions identified for the GDF, including:

- current disposal projects in Posiva (Finland), Forsmark (Sweden), Bure (France) and the Waste Isolation Pilot Plant in the USA
- planned projects in other countries currently embarking on a national radioactive waste disposal programme including Argentina, Canada, Czech Republic, Switzerland, Germany, Japan, Belgium, Netherlands, South Korea and Spain

This experience gives a level of confidence that suitable design solutions can be developed such that the GDF can be operated safely with doses and risks which can be demonstrated to be tolerable and ALARP.

In conclusion, based on relevant good practice and UK nuclear site licence operational experience, no significant obstacles have been identified where claims of future compliance against targets, tolerability of risks and ALARP are being made. The resolution of these issues will be the subject of formal design development and safety assessment and the resolution of the FAPs. It is acknowledged that the design will need to be further developed in order to reduce the risk to ALARP levels. This will be further considered as part of the design development in accordance with the RWM DASI process, as detailed in the NOSM and the RWM design process, which is in accordance with current nuclear industry standards and relevant good practice.

References

1 Radioactive Waste Management, *Geological Disposal: Overview of the Generic Disposal System Safety Case,* DSSC/101/01, 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, 2014.

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

4 Radioactive Waste Management, *Geological Disposal: Volume 1: Construction and Non-Radiological Safety Assessment*, DSSC/311/01, 2016.

5 Radioactive Waste Management, *Geological Disposal: Volume 2: Normal Operations Safety Assessment*, DSSC/312/01, 2016.

6 Radioactive Waste Management, *Geological Disposal: Volume 3: Accident Safety Assessment*, DSSC/313/01, 2016.

7 Radioactive Waste Management, *Geological Disposal: Volume 4: Criticality Safety Assessment*, DSSC/314/01, 2016.

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

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

10 Radioactive Waste Management, *Geological Disposal: Generic Facility Designs*, DSSC/412/01, 2016.

11 Radioactive Waste Management, *Geological Disposal: Generic Transport Systems Designs,* DSSC/411/01, 2016.

12 IAEA, *Fundamental Safety Principles*, Safety Fundamentals SF-1, 2006.

13 Office for Nuclear Regulation, *Fundamental Principles*, NS-TAST-GD-004 Revision 5, 2016

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

15 Radioactive Waste Management, *Geological Disposal: Generic Transport Safety Case - Main Report*, 2016.

16 Radioactive Waste Management, *Geological Disposal: Generic Environmental Safety Case - Main Report*, DSSC/203/01, 2016.

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

18 Office for Nuclear Regulation, *The Purpose, Scope and Content of Safety Cases*, NS-TAST-GD-051 Revision 3, 2013.

19 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, October 2009.

20 Radioactive Waste Management, *Geological Disposal: Safety Case Production and Management Report*, DSSC/431/01, 2016.

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

22 Radioactive Waste Management, *GDF Design Principles*, LL11530271, 2014.

23 IAEA, *Disposal of Radioactive Waste*, Specific Safety Requirement SSR-5, 2011.

24 Environment Agency, Northern Ireland Environment Agency, *Geological Disposal Facilities on Land for Solid Radioactive Waste: Guidance on Requirements for Authorisation*, February 2009.

25 Nirex, Nuclear Design Safety Principles, 1998.

26 Health and Safety Executive, *Risk Assessment – A Brief Guide to Controlling Risks in the Workplace*, INDG163, Rev 4, ISBN 978 0 7176 6463 4, 2014.

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

28 Radioactive Waste Management, *Disposal System Safety Case (DSSC): Basis of Operational Assessment*, 2016 (unpublished).

Glossary

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

Appendix A Forward Action Plan Listing (Volumes 1 to 4)

FAP ID	FAP Description
FAP.2016.VOL1.01	Undertake a study to optimise the design to ensure that the risk to operators and other on-site workers as a result of vehicle accidents are minimised including the provision of safe access and egress routes.
FAP.2016.VOL1.02	Undertake a study to determine what engineering or administrative measures are required to ensure a safe operating envelope to minimise the risk from hazards related to moving plant.
FAP.2016.VOL1.03	Undertake a study to determine design requirement related to air quality in the subsurface environment to minimise the risk of airborne hazards to operators.
FAP.2016.VOL1.04	Undertake a study to determine the requirements for waste package specifications to include thresholds for flammable or explosive gas build up to minimise the risk of potential injury following deflagration or conflagration of an explosive atmosphere.
FAP.2016.VOL1.05	Undertake a study to ensure a safe blast radius is defined to minimise the risk of potential for explosions impinging on packages.
FAP.2016.VOL1.06	Undertake a study to determine appropriate locations for transformers present in the drift to minimise the risk of potential explosion of transformers impinging on vehicles in drift.
FAP.2016.VOL2.01	Undertake further assessment to identify areas of concern for a normal operation dose assessment to minimise the risk of a poorly defined set of requirements related to normal operations.
FAP.2016.VOL2.02	Undertake a study to determine the radiation and contamination zoning requirements and the controls necessary to minimise exposures and prevent unauthorised contamination transfer.
FAP.2016.VOL2.03	Undertake a study to review the impact of the location of the buffer areas on the surface to minimise elevated dose rates for operators and the public in surface buffer areas.
FAP.2016.VOL2.04	Undertake a study to determine which buildings and areas require buffer zones to minimise the risk of non-compliance with the Environmental Permitting Regulations 2010 (fugitive releases from buildings)
FAP.2016.VOL3.01	Develop a fire hazard management strategy and undertake a preliminary fire safety assessment for the GDF (including waste packages) and design studies to minimise the risk of poorly defined design or safety measure requirements for fire faults.
FAP.2016.VOL3.02	Undertake studies for surface and sub-surface facilities to ensure that risks arising from credible external events are understood and an appropriate hazard management strategy for the design is made and implemented to minimise the risk of building structural failure under external hazards.

FAP ID	FAP Description
FAP.2016.VOL3.03	Undertake a design evaluation, including option studies, in order to identify a potential design solution for the use of a shaft for waste transfers to the sub-surface environment in order to prevent an inappropriate design being carried forward.
FAP.2016.VOL3.04	Undertake studies to determine disposal container transport container related failure modes and the resulting fault scenarios to minimise the risk of credible faults being dismissed in error.
FAP.2016.VOL3.05	Undertake a study to determine the design basis rate of natural rock movement and the effect on sub-surface structures to minimise the risk of damage and degradation leading to lifting and emplacement faults or flooding within sub-surface structures.
FAP.2016.VOL3.06	Undertake a study to determine what systems are necessary for personnel accountancy to minimise the risk of operators remaining undetected in potentially hazardous situations (normal operations/emergencies).
FAP.2016.VOL3.07	Review the design to minimise the risk of misalignment of packages in the vault and stack collapse.
FAP.2016.VOL3.08	Develop the lifting strategy and undertake design studies to minimise the risk of dropped loads or load path obstructions during lifting operations for different package and equipment types.
FAP.2016.VOL3.09	Undertake studies to evaluate in-package processes with the potential to challenge package integrity in order to minimise the risk of loss of package containment and release of radioactive material.
FAP.2016.VOL3.10	Undertake a study to identify which areas of the GDF design are vulnerable to long-term loss of off-site power to minimise the risk of failure to assess secondary faults (domino effects) arising.
FAP.2016.VOL3.11	Undertake a study to define requirements and develop the ventilation system design to a level which permits hazard and failure identification studies to be undertaken in order to provide a definitive fault set related to ventilation system failures.
FAP.2016.VOL3.12	Undertake a study to optimise the provision of safe access and egress routes for GDF operators, including refuges in order to minimise the risk to operators in the event of an accident in the sub-surface environment.
FAP.2016.VOL3.13	Undertake a study to determine which engineering systems are required to ensure compliance with any effluent authorisation to minimise the risk of unauthorised discharges.
FAP.2016.VOL3.14	Undertake a study to determine the nuclear safety requirements for a logistical system for segregation and sentencing of waste packages to minimise the risk of hazards associated with waste packages being in the wrong location.
FAP.2016.VOL3.15	Undertake a study to demonstrate seismic withstand to understand the risk of distortion or collapse of the drift or underground tunnels.
FAP.2016.VOL3.16	Develop and implement the integrated design and safety process to minimise the risk of potential inconsistencies between the developing design and safety requirements leading to an inadequate safety assessment.

FAP ID	FAP Description
FAP.2016.VOL3.17	Undertake a study to review factors related to package performance during accidents which could result in over-conservative accident safety assessments and incorrect specification of identified safety measures.
FAP.2016.VOL4.01	Undertake a study to determine the likelihood of receipt of ’out-of-specification’ packages and the safety margins to prevent the potential for a criticality accident.
FAP.2016.VOL4.02	Undertake a study to determine the thresholds at which criticality needs to be considered within a UILW disposal unit to minimise the risk of a criticality accident.

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