Radioactive Waste Management

NDA Report no. DSSC/313/01

Geological Disposal

Generic Operational Safety Assessment
Volume 3 - Accident Safety Assessment

December 2016

Radioactive Waste Management

NDA Report no. DSSC/313/01

Geological Disposal

Generic Operational Safety Assessment
Volume 3 - Accident Safety Assessment

December 2016

Conditions of Publication

ISBN 978-1-84029-547-4

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

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.

Hazard identification and fault schedule development

A systematic hazard identification study has been undertaken. The study is based on the current Basis of Assessment (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
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/off-site))	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

Number	HAZAN	Comment	Type of Assessment
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.

Exclusions

The following fault sequence groups have not been assessed in the 2016 generic Operational Safety Case (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.

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 IEF. 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.

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 Initiating Event Frequency (IEF) 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.

Results of Design Basis Accident Analysis

The initial DBAA has identified and assessed a total of ten bounding faults which comprise two class B, seven 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.

Feasibility of meeting Design Basis Accident Analysis 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.

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.

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
- collapse, 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.

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 to implement (with today's technology) and that the GDF will be safe to operate as a result. 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.

List of Contents

1 Introduction

1.1 The generic Disposal System Safety Case

RWM has been established as the delivery organisation responsible for the implementation of a safe, sustainable and publicly acceptable programme for geological disposal of the UK's higher activity radioactive waste. Information on the approach of the UK Government and devolved administrations of Wales and Northern Ireland[1] 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].

A 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 a GDF could be located, the Government is developing an 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 a 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 radioactive 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 do not 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] Hereafter, 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.

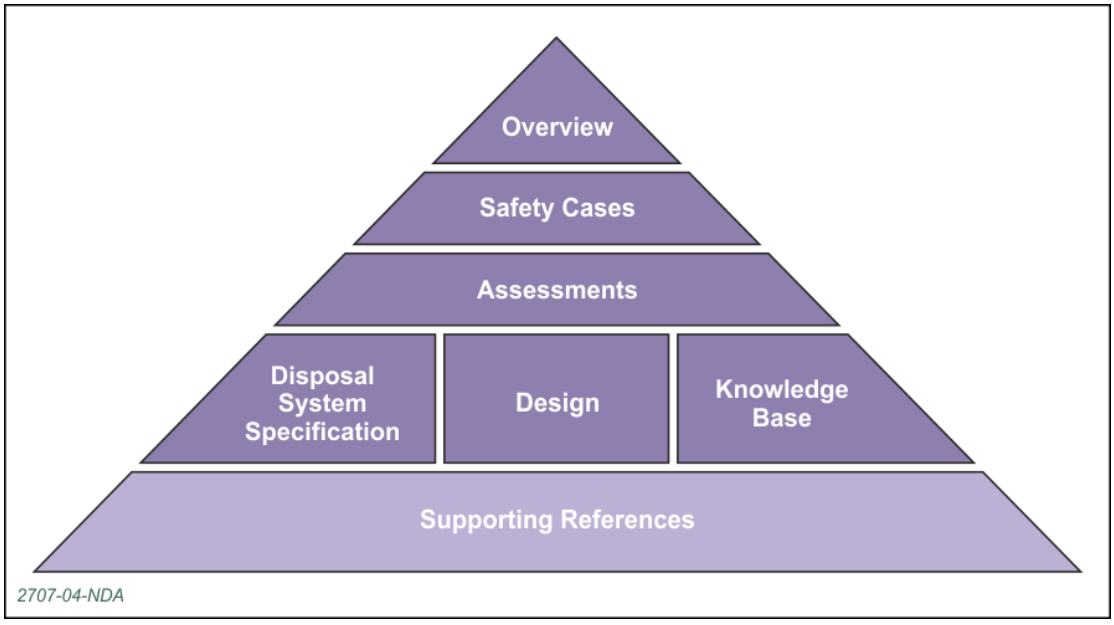
High level information on the inventory for disposal, the illustrative disposal concepts and other aspects of the disposal system is collated in a technical background document (the Technical Background) [3] that supports this generic Disposal System Safety Case.

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 Assessment: Volume 3 – Accident Safety Assessment

This document is the Accident Safety Assessment and is one of 4 volumes that, together with a summary report, make up the Operational Safety Case.

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

This document presents the illustrative accident safety assessment for the GDF. This report covers radiological faults only. Criticality faults are addressed in the Volume 4: Criticality Safety Assessment.

Volume 2: Normal Operations Safety Assessment identifies the most significant radiological hazard potential locations within the GDF where exposures to direct radiation will require management. Calculated doses are used in order to signpost the assessment in terms of distinguishing the highest potential hazard areas which will provide the focus for the development of suitable design solutions to ensure that RWM dose criteria will be met. Dependent on the magnitude of potential exposure, suitable solutions will range from robust engineered features to administrative controls. This ensures that the needs of normal operations and additional controls identified to prevent faults are correlated in the design requirements. The loss of function of these systems or other errors is the subject of the accident safety assessment.

There is also an interface with Volume 1: Construction and Non-Radiological Safety Assessment. Construction activities with the potential to impact on waste emplacement operations are assessed as internal hazards in the accident safety assessment.

1.3 Objective

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 this accident safety assessment at this stage of the 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 volume includes the forward action plans (FAPs) to demonstrate the feasibility of implementing illustrative safety measures within the developing design.

The detailed methodology and results of the accident safety assessment are reported in the Basis of Operational Assessment (BOA) [4] report and the hazard assessment document (HAZDOC) with its supporting hazard analysis (HAZAN) documents [5]. Subsequent design development will follow the RWM design and safety integration (DASI) process. The DASI process is of a level of detail commensurate with the current phase of the GDF programme and consistent with industry standards. All safety assessments will be undertaken in accordance with the methodologies set out in the RWM Nuclear Operational Safety Manual (NOSM) [6].

This document, the generic Operational Safety Assessment (Volume 3), provides a summary of the assessment approach and the main conclusions.

1.4 Scope

The scope of this volume covers all fault scenarios with potential for significant risk of harm to workers or members of the public. The scope of the accident assessment at this stage is limited to consideration of issues related to:

- waste package and wasteform behaviour and contents
- the functional requirements and potential for errors during receipt, handling and emplacement operations
- internal or external factors directly or indirectly affecting safe operation

Operations for backfilling, decommissioning, sealing and closure (which do not involve the handling of waste packages) have not been specifically considered as the level of design available does not permit any meaningful assessment of fault conditions. The operational safety impacts of different backfilling and decommissioning strategies are currently being considered in the context of design optimisation.

A systematic hazard identification study has been undertaken. The study is based on the current BOA which presents the GDF concepts as a Process Flow Description (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.

The safety analysis is undertaken within the HAZDOC report, and considers radiological consequences to workers and members of the public from direct external dose and inhalation/ingestion of radioactive material. Section 2.7 presents an overview of those fault sequences.

The report does not include consideration of construction and non-radiological (conventional) hazards; with the exception of internal hazards; normal operations and criticality hazards, which are addressed in the generic OSC volumes 1, 2 and 4 respectively.

Table 1 summarises the limitations of the safety assessment presented within this report.

Table 1 Omissions and Limitations

Type	Generic OSC Status	Justification
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) • waste package transfer facility (WPTF) unloading of package from transfer facility (rail or road) • surface preparation of package for below ground transfer via a drift or shaft	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). There are therefore no design basis events with radiological consequences arising from faults involving packages in transport configuration. The operations to be undertaken at the surface are tried and tested activities undertaken extensively on UK nuclear licensed sites. These sites apply established codes and standards to the buildings and equipment with them, which ensure that the risk of accidents is minimised.
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.
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.
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.

Type	Generic OSC Status	Justification
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.
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.
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.
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.

Type	Generic OSC Status	Justification
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.
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.

1.5 Document Structure

This report is structured as follows:

- Section 2 presents the safety objectives, changes from the 2010 generic OSC and methodology from hazard identification to initial Design Basis Accident Analysis (DBAA), including those faults subject to DBAA
- Section 3 presents the fault classification for each of the faults subject to DBAA. This includes the development of requirements to be placed on the design and assessment of feasibility and sensitivity analysis of the fault set
- Section 4 describes the future work identified for the accident safety assessment that is either ongoing or planned to address issues raised by this report
- Section 5 summarises the assessments undertaken, the results and conclusions with respect to the generic OSC

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

2 Safety Assessment Approach

2.1 Introduction

This section presents an overview of the approach taken in the assessment of radiological hazards in the generic DSSC. The objective of the accident safety assessment is to demonstrate safety 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.

This high level 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 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.

2.2 Safety objectives

The accident safety assessment provides the arguments and evidence to support the claim that:

- the proposed facility can be designed and operated within a well-defined, credible safe operating envelope
- the means of meeting the safety requirements through engineered or operational systems is both credible and feasible

At this stage of the GDF programme, the safety justification is focussed on demonstrating the feasibility of the GDF concept which will be used to inform more detailed design and assessment studies. The subsidiary claims to be demonstrated through suitable arguments and evidence are:

- a systematic hazard identification process has been and will be applied to the GDF
- hazards have been screened, grouped and bounded in order to derive a representative set of faults which have the same functional requirement on the design, regardless of location

- an initial DBAA has been performed based on conservative unmitigated radiological consequences and initiating event frequencies for the representative set of faults
- faults have been classified and the equivalent outputs (safety functional requirements and safety measures) identified
- it is feasible and credible that the representative set of design basis faults will be adequately protected in the developing design 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
- there is an understanding of the uncertainties and variability issues which can impact on the results of the safety analysis
- 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
- 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
- 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
- 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 safety objectives relate to national requirements (as defined by the Office for Nuclear Regulation) and international frameworks (as defined by the International Atomic Energy Agency and the International Commission on Radiological Protection). These are reflected in the NOSM, which sets out the targets, constraints and limits relevant to radiological safety derived from the Radiological Protection Criteria Manual [7] (see Table 2).

The expectations derived from these safety objectives are that the assessment shall:

- identify and analyse all initiating faults having the potential to lead to any person receiving a significant dose of radiation[2], or to a significant quantity of radioactive material escaping from its designated place of residence or confinement
- where possible, draw conclusions regarding the suitability and sufficiency of engineered safety measures provided within the generic stage and to indicate, where necessary, shortfalls requiring attention before candidate site-specific safety cases can be prepared
- where the generic stage does not support a quantitative assessment, undertake a high-level assessment of the key hazards and identify likely hazard management strategies

The initial screening criteria for effective dose received by any person exposed to a design basis fault sequence are the Basic Safety Objectives set out in Table 2 below.

[2] Faults that cannot cause doses of 0.1 mSv to workers, or 0.01 mSv to a hypothetical person outside the site, are regarded as part of normal operation and may be excluded from the fault analysis. These are the levels above which individual doses should be regarded as 'significant'. A 'significant quantity' of radioactive material is one which, if released, could give rise to a significant dose.

Table 2 Radiological Protection Criteria for Design Basis Analysis

	Basic Safety Limits		Basic Safety Objectives
	Initiating Fault Frequency (per year)	Effective Dose (mSv)	Effective Dose (mSv)
Off-Site	>1E-03	1	0.01
	1E-03 to 1E-04	10	
	1E-04 to 1E-05	100	
On-Site	>1E-03	20	0.1
	1E-03 to 1E-04	200	
	1E-04 to 1E-05	500	

The detailed assessment of design basis accidents requires the calculation of mitigated doses to demonstrate the magnitude of the claim being placed on systems in a design. This provides a measure of the adequacy and ability of the safety measures claimed within the DBAA to prevent, protect or mitigate the impact of accidents.

This study and assessment has included the identification of candidate safety measures which, if implemented, would be basis of the claim for compliance with the DBAA criteria. To demonstrate that it is feasible that the criteria can be satisfied, the DBAA undertaken in the 2016 generic OSC is focussed on certain stages of the DBAA, namely:

- initial calculation of fault classes
- identification of safety functions and conceptual safety functional requirements and
- specification of candidate safety measures based on the NOSM hierarchy

Following the derivation of conceptual safety functional requirements, optioneering identifies the safety measures to be claimed in the design. The priority is to eliminate the hazard as the first preference followed by measures which prevent the fault occurring. Preventative measures that reduce the initiating event frequency (IEF) have preference over those that reduce the consequence after the accident. It is not meaningful or appropriate at this stage to present mitigated doses from design basis faults, as the implication would be that the hierarchy had already been applied.

2.3 Changes from the 2010 generic OSC

There are a number of changes in approach from the 2010 generic OSC, details of which are presented within the BOA report. Those changes, which have directly affected this volume and resulted in a difference in the input, approach and conclusions of the safety assessment, are detailed below.

Any changes to the inventory of radioactive material being received, transported and emplaced at the GDF result in a change to the potential consequences received by workers and members of the public during fault conditions. The 2013 Derived Inventory [8] has underpinning assumptions that reflect the best available information at the time of publication. This information and data can change for a number of reasons, for example, new data become available from an update to the UK radioactive waste inventory or from other sources. As a result, the wastes that are included in the 2013 Derived Inventory differ from those that are included in the 2010 equivalent. The key assumptions underpinning both the 2010 and 2013 Derived Inventories are presented in the BOA report; examples include waste package types not included in the 2010 generic OSC, such as robust shielded waste

containers, 500 litre and 1 cubic metre concrete drums, plus the exclusion of the Scottish wastes.

Since the publication of the 2010 generic OSC, RWM has produced a NOSM which sets out the nuclear safety assessment process and safety case documentation for the GDF. The NOSM ensures RWM is compliant with legislation, regulatory expectations and current best practice in the UK nuclear industry for nuclear safety assessment. The nuclear safety assessment and safety case produced for the 2016 generic OSC for the GDF has followed the requirements of the NOSM and associated procedures and instructions. For the current generic stage, it informs:

- identification of options for evaluation through the design process
- the development of hazard management strategies which the design will be required to implement
- design principles which provide the basis from which the requirements of the hazard management strategy can be translated into safety measures against which design can be assessed for suitability

The introduction of the NOSM, and associated procedures and instructions, has a significant impact on the safety case approach and structure for this 2016 version of the generic OSC, for example:

- a systematic hazard identification using the GDF functional PFD
- safety functions (conceptual) now identified based on analysis of both normal operations and fault analysis

2.4 Methodology

The illustrative assessment considered waste categories which are subsets of the generic waste groups set out in Section 1.1. This approach has been taken because the analysis is waste category specific and hence needs to be structured in this way to align with the PFD. Furthermore, it gives a useful discrimination and structure between the radiological hazards, the wastes and the process combinations. For clarity, the relationship between the waste categories is set out in Table 3.

Table 3 Waste Groups and Categories

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

The safety analysis of accident conditions includes:

- HAZID using the Hazard and Operability (HAZOP) technique and production of the full hazard log with auditable link from the initiating events in the HAZOP records to the faults
- screening and grouping of hazards and recording in the preliminary fault schedule
- selection of the representative design basis fault set which have the same functional requirement on the design regardless of location for quantitative assessment
- designation of fault class through DBAA for those faults subject to numerical assessment as reported in the HAZDOC and HAZANs 1 to 4
- qualitative assessment for those faults not screened and not subject to numerical assessment as reported in the HAZDOC and HAZANs 5 and 6

- qualitative assessment for criticality faults as reported in the HAZDOC and HAZAN 7

A summary of these steps is described in the following sub-sections and illustrated in Figure 2. The approach is consistent with the NOSM and associated procedures and instructions.

The assignment of fault sequence groups to quantitative and qualitative assessment is set out in Table 4.

Table 4 Fault Analysis assessment by Fault Type

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
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 Section 2.7.1)
5	External hazards	Faults initiated by external hazards (not under the control of the operator (air/ground/off-site)	Qualitative as the assessment requires site-specific data and information
6	Internal hazards	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 is 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.

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.

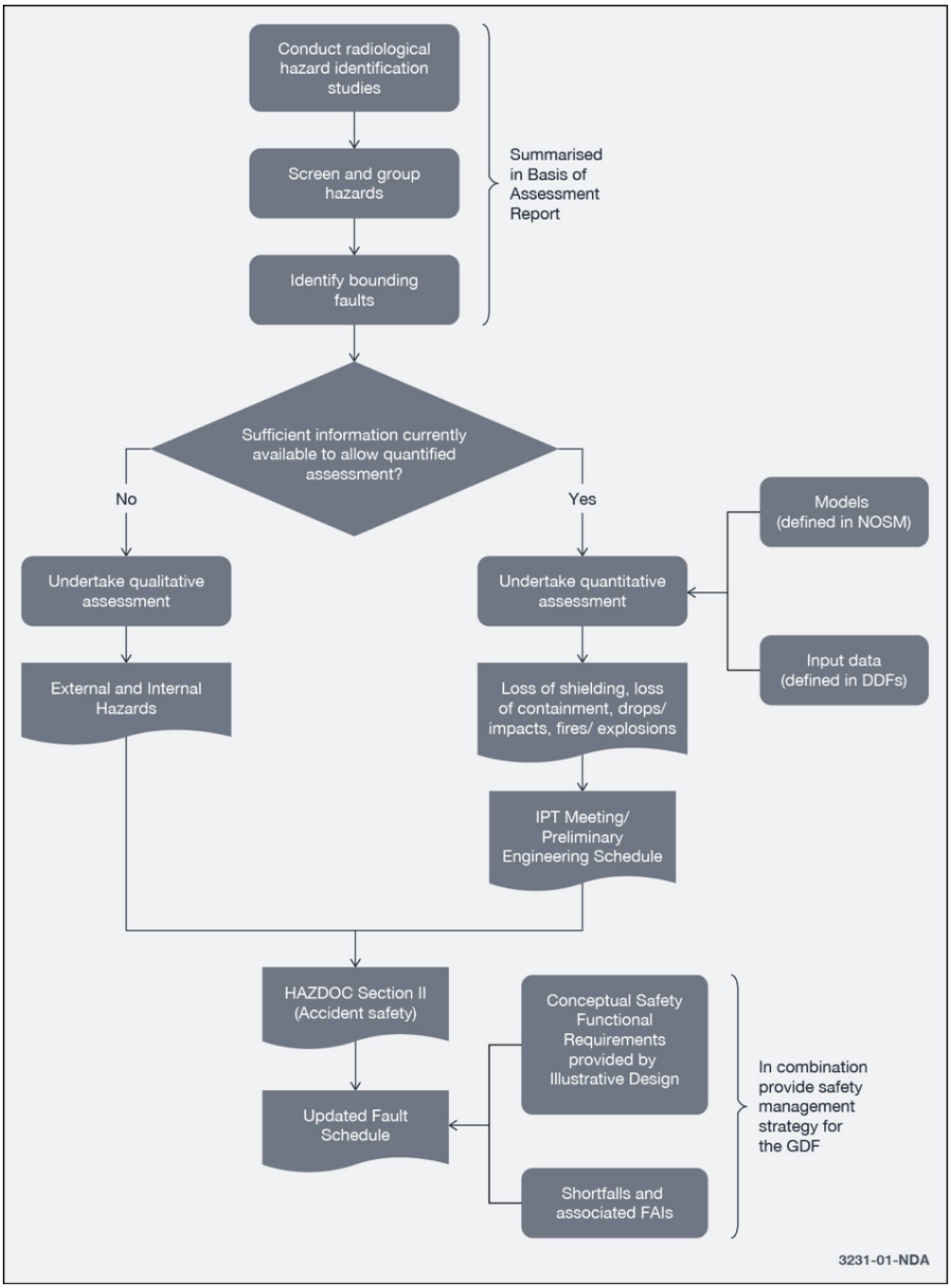
This approach is consistent with the scope and quality of information available at this stage of the GDF programme. For example, if fault consequences can be determined with generic data to allow order of magnitude interpretation of results, then DBAA has been undertaken. This allows task duration and distance data to be estimated in a meaningful way and the quality of any conclusions to be understood.

The full assessment will use data derived from actual layouts and well defined tasks sets. This additional safety analysis, as specified within the NOSM includes, but is not limited to:

- development of radiological consequences and the IEF assessments using data specific to the fault scenario, taking account of additional exposure pathways such as contaminated wounds
- further development of the DBAA including determination of suitable and sufficient numbers of safety measures to meet the DBAA safety criteria
- probabilistic safety assessment
- detailed comparison against RWM safety criteria, together with the ALARP justification
- substantiation of safety claims including definition and substantiation of the safe operating envelope

The results of the fault analysis will be used to develop hazard management strategies which in turn will inform design principles for use in design development activities.

Figure 2 Overview of Radiological Fault Analysis Process



2.5 Radiological hazard identification studies

HAZID studies were used to identify hazards associated with normal operations and potential fault conditions and the outputs are summarised below:

- HAZOP 0 study sessions – these were undertaken to identify the inherent hazards and operability issues and developed in the full hazard log
- HAZOP 1 study sessions – these were undertaken to produce a set of initiating events for each process type prompted by keywords
- External hazards identification study sessions – these were undertaken to identify external hazards and credible combinations of external hazards

The use of the PFD as the basis for hazard identification exercises ensured the process was systematic and focused on identifying functional failures that would result in outcomes with radiological consequences to workers or members of the public. This ensures that the HAZID is independent of rock type. The PFD ensures full coverage of the functional processes at task level for emplacement of all waste package types in the UK 2013 Derived Inventory. Other features of the PFD of relevance to the assessment are:

- It incorporates both drift and shaft as modes of transfer of waste packages underground to enable hazard identification of both modes.
- Waste packages are assumed to arrive in one of three transport unit configurations, namely a transport overpack (IP-2) generally for the shielded ILW/LLW categories, standard waste transport containers (SWTC) for the unshielded ILW category and disposal container transport containers (DCTC) for the HLW/spent fuel type.
- It maps through changes of configuration from transport packages to disposal unit and the relationship to high-hazard areas of the GDF. This ensures the failure of systems that will ensure safe normal operations is considered as part of the accident assessment and both can be traced back to the PFD.
- It is consistent with the high level breakdown of the waste emplacement process and provides a structural framework to assess and control future design development.
- It provides a clear and non-technical framework for dialogue within the project and supporting functions.

2.6 Initial hazard screening

The output from the HAZID studies generated over 9000 individual records. To manage the production of the preliminary fault schedule from such a large number of records, a strategy was adopted that:

- presented a clear auditable link from the initiating events in the HAZOP records to the faults
- enabled a clear and structured presentation of the types and numbers of faults expected across the GDF

A top down approach was performed to identify a set of generic Fault Schedule Groups (FSGs). At the generic FSG level, the fault description does not contain any reference to where in the GDF a fault might have occurred or to what waste type it is applicable. This process is summarised in Figure 3.

For consistency and clarity, the generic FSGs were defined with the following structure:

<hazard> due to <fault type>

Or:

<event> resulting in <fault type>

The generic FSGs listed in the preliminary fault schedule are presented in Table 5.

Table 5 Faults in the preliminary fault schedule

gFSG ID	gFSG Description
1.A	Elevated dose rates due to (package) not being removed from transport container
1.B	Elevated dose rates due to (package) not being removed from transport equipment

gFSG ID	gFSG Description
1.C	Elevated dose rates due to (package) not being removed from holding facility
1.D	Elevated dose rates in operational area due to entry when (package) in an unshielded configuration
1.E	Elevated dose rates in operational area due to entry when facility in an unshielded configuration
1.G	Elevated dose rates due to leak of contaminated liquids
2.A	Elevated levels of RA in air present due to disturbance of accumulation of loose RA internally in transport container
2.B	Elevated levels of RA in air present due to disturbance of accumulation of loose RA externally on transport container
2.C	Elevated levels of RA in air present due to disturbance of accumulation of loose RA contamination internally in transport vehicles
2.D	Elevated levels of RA in air present due to disturbance of accumulation of loose RA contamination externally on transport vehicles
2.E	Elevated levels of RA in air present during maintenance of in-vault equipment
2.F	Elevated levels of RA in air present due to disturbance of accumulated contamination in area
2.G	Elevated levels of RA in air present due to leak and evaporation from contaminated liquids
3.A	Elevated dose rates in operational area due to failure of transport unit shielding following impact
3.B	Elevated dose rates in operational area due to failure of disposal unit shielding following impact
3.C	Elevated dose rates in operational area due to failure of facility shielding following impact
3.D	Elevated neutron dose rates due to failure of transport unit or holding facility shielding following impact
3.E	Gross release of RA to air in operational area due to full failure of transport unit containment following impact
3.F	Gross release of RA to air in operational area due to failure of disposal unit containment following impact
4.A	Elevated dose rates due to loss of shielding/gross release of RA to air due to loss of containment due to thermal loading during fire on surface transport vehicle
4.B	Elevated dose rates due to loss of shielding/gross release of RA to air due to loss of containment due to thermal loading during fire on drift vehicle
4.C	Elevated dose rates due to loss of shielding/gross release of RA to air due to loss of containment due to thermal loading during fire on sub-surface vehicle
4.D	Elevated dose rates due to loss of shielding/gross release of RA to air due to loss of containment due to build-up of flammable liquids or gases during facility fire
4.E	Elevated dose rates due to loss of shielding/gross release of RA to air due to loss

gFSG ID	gFSG Description
	of containment due to thermal loading during fire on lifting equipment
4.G	Elevated dose rates in operational area due to fire resulting in thermal damage to neutron shielding
5.A	(EVENT) resulting in damage of surface facility
5.B	(EVENT) resulting in damage of surface to sub-surface connection facility
5.C	(EVENT) resulting in damage sub-surface facility
5.D	(EVENT) resulting in fire in surface facility
5.G	(EVENT) resulting in collapse of lifting equipment in surface facility
5.H	(EVENT) resulting in collapse of lifting equipment in surface to sub-surface connection facility
5.I	(EVENT) resulting in collapse of lifting equipment in sub-surface facility
6.A	(EVENT) resulting in damage of surface facility
6.B	(EVENT) resulting in damage of surface to sub-surface connection facility
6.C	(EVENT) resulting in damage sub-surface facility
6.L	(EVENT) resulting in flooding in sub-surface facility
7.A	Criticality event induced by change of geometry due to impact
7.B	Criticality event induced by addition of moderator
8.A	Nuclear fire/thermal release induced by rupture of spent fuel canister following impact (heating during post-accident nuclear processes)

Figure 3 Fault Sequence Development Process

Within this structure, FSGs were developed for each waste type (if relevant) and the necessary type of assessment stated (qualitative or quantitative). FSGs were grouped together in HAZANs, as shown in Table 4 with additional detail provided in Appendix A . These FSGs are considered to be representative of all similar faults: for similar faults the same safety function would result, albeit potentially with a less onerous design requirement depending on the fault location.

A screening assessment was then undertaken on the FSGs to decide which faults to take forward for further assessment. The criteria applied at this stage of the GDF programme are:

- category ‘1’ ‘screened in faults’: faults that are judged to be design basis faults and sufficient information is available to enable an assessment to be performed
- category ‘0’ ‘screened out faults’: the unacceptable faults that should be possible to preclude by design
- category ‘Q’ faults pending resolution of queries: faults that require site-specific data or resolution of a FAP before they can be screened out from further assessment, for example:
  - unusual external hazards related to below ground behaviours are not screened out at this stage as substantiation of claims is required to screen them out
  - low consequence faults; these will be assessed once more design information becomes available

Application of this screening process ensures that faults are not carried forward unnecessarily to consequence assessments if insufficient design information is available. The full assessment will confirm faults assigned a ‘Q’ status have been reassigned to:

- ‘1’ once the iteration with design progresses and if further assessment is required or

- ‘0’ status if it can be demonstrated through the design solution that the fault can be ‘engineered out’ and that the claim is substantiated

The following sub-sections describe the methodology applied in the assessment and more detail given in the HAZDOC.

2.6.1 Identification of bounding design basis faults

Appendix A lists the design basis faults as assessed in the HAZDOC and HAZANs, together with identification of those faults which have not been taken forward for numerical assessment. 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. Section 3 presents the assessment of these faults.

2.6.2 Design basis accident analysis

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 functions that must be delivered by the design and the 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 IEF. The unmitigated dose is used as the basis of this assessment. The term ‘unmitigated’ refers to the radiological consequences of a fault with all safety measures removed other than those that demonstrably retain their safety function post-accident. 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.

Any assessment is dependent on information such as the radiological inventory, the assessment methodology and other input parameters. The inputs to the numerical assessment are defined and discussed in the HAZDOC.

Radiological consequence assessment

Based on the 2013 Derived Inventory, more than 500 separate waste streams in a variety of configurations will be received at the GDF. The radionuclide fingerprint for the waste streams currently considers 112 radionuclides.

An exercise was conducted to define a bounding source term for each of the three specified GDF waste routes in the PFD (namely SILW, UILW and HLW/spent fuel) for use in bounding fault consequence assessment. The purpose was not to identify the absolute worst case, but instead to develop a ‘construct’ to bound all combinations such that the safety assessment no longer relies on specific data for a single package. The bounding source term is derived from the combination of the worst case or maximum throughput and the maximum inventory by PFD waste route. This approach provides a level of flexibility to accommodate changes in the inventory for disposal because the assessment is not built upon a single waste stream and its associated data.

This approach accounts for uncertainty and variability in the waste stream inventories and shipment schedule. For example, the bounding source term for SILW is based on a waste stream with a throughput of 20 disposal units per year whereas the full waste category throughput of 2300 per year has been applied. Although the case may not be bounding in inventory, it is bounding in terms of IEF and hence risk both from normal operations and accidents. It should be noted that this approach ensured that outliers were not selected. A waste stream with a single package inventory is not considered a sensible basis for deriving the bounding source term.

The sources of the inventory data for the bounding source terms used in the consequence calculations are detailed in Table 6.

Table 6 Sources of inventory data for the Bounding Source Terms

Faults (FS ID)	HAZAN	Type of Dose	Waste category	Bounding Source Term (2013 Derived Inventory)
1.A.6.2.1, 1.B.6.3.1, 1.D.6.2.1, 1.E.6.3.1, 1.E.6.2.1 & 1.E.5.3.1 3.A.4.1.1, 3.A.4.2.1, 3.A.4.3.1, 3.B.6.1.1 & 3.C.6.3.1	1: Loss of shielding 3: Dropped load (loss of shielding)	Direct dose to workers	UILW (LHGW)	2D26
			SILW (LHGW)	9D50
			HLW/spent fuel (HHGW)	MEP100
3.E.4.1.1, 3.E.4.2.1, 3.E.4.3.1, 3.F.6.1.1 & 3.F.6.2.1	3: Dropped load (loss of containment)	Inhalation dose to workers	UILW (LHGW)	2D03
			SILW (LHGW)	9D22
			HLW/spent fuel (HHGW)	MOX100

Consequence models/methodologies

The numerical safety analysis requires the use of consequence models to determine the unmitigated consequences for the faults selected for quantitative assessment. The dominant radionuclides are expected to be high energy gamma emitting radionuclides (for example Cs-137) for direct radiation exposures and alpha emitting radionuclides (for example transuranics, including plutonium isotopes) for inhalation exposures.

Computational models have been applied at a level consistent with the quality of information available. For example, precise modelling of dispersion is not appropriate when the dominant uncertainty is in the inventory.

Application of the consequence models has enabled early insight into whether risk reduction targets can be met for the worst case consequences. This approach gives high confidence that claims of feasibility can be supported now. The DASI process will aim to ‘design out’ faults and, as the precision of the data and assessment increases, the risk reduction targets will become clearer and more precisely reflect actual needs.

The safety analysis has not assessed mitigated fault consequences, ie taking into account engineered safety measures, as this requires design detail or intent to be specified. Substantiation arguments are not proposed or relevant at the pre-Preliminary Safety Report however commentary on the feasibility of the identified risk reduction measures is provided.

The consequence models relevant to the scope of the assessment calculate the following:

- exposure to direct radiation, dependent on the distance of the exposed individual from the source
- exposure of workers to internal radiation (by inhalation), where the release is assumed to be into a volume defined by the hemisphere in which the worker stands. For larger separations, dilution is assumed to be constrained by the volume of the room (or location if below ground) occupied by the worker
- exposure of members of the public to internal radiation, where the dose is dependent on the amount of radioactive material released and the dose release ratio

Model input parameters

The input parameters that most influence the inhalation dose assessment are the release fraction and the containment factor. These are applied to model the release of radioactive material into the release envelope where it can be inhaled. Selection of conservative values and assumptions allows for:

- optimisation of the design that will reduce the level of challenge to a package
- sufficient margin in the design capability to accommodate variation in performance within the population of package types

This approach ensures that the design requirement does not become more onerous in future and develop into a feasibility issue. This group of parameters can vary significantly, resulting in order of magnitude effects, as discussed in the sensitivity analysis in Section 3.2.2. Developing an improved methodology for the design and its relationship to the fault assessment will ensure any pessimism can be reduced before setting design requirements. This task will be the subject of future work through FAP.2016.VOL3.17. The priority is for elimination or prevention of faults, for example, by eliminating the potential for challenge to the waste package by limiting lift heights to below the withstand capability of the package.

Four other variables are of interest to the calculation of radiological consequences:

- distance from the point of release to the location of the exposed individual; applies to both workers (direct and inhalation doses) and the public (direct and inhalation doses)
- duration of the exposure; this applies to both workers (direct and inhalation doses) and the public (direct doses) while for the workers, this was either the task duration (revealed fault, of the order of minutes) or half a shift (unrevealed fault, four hours)
- volume into which the radiological release, assumed to be instantaneous, is homogenously dispersed; this applies to the exposure of workers to airborne contamination which can be inhaled
- distances for workers were task dependent. The distance to the public was estimated as a generic value and is embedded within the dose release ratios for off-site releases in the absence of a site-specific design

All the sources of data are defined in the BOA report and derived from approved and validated data held by RWM.

Initiating event frequencies

The assignment of fault class is dependent on both the unmitigated consequence and the fault IEF. The safety case has been developed without design-specific data related to details

of the operational activities or systems other than those defined at a high level in the illustrative designs. At this stage of the GDF programme, the IEF has been derived by multiplying the probability of failure on demand (pfd), either a mechanical failure or human error probability, by the throughput of waste packages. These design assumptions and discussed in more detail in the BOA. This allows the assessment to be based on setting a ceiling to benchmark against and to focus attention on the design and inventory data impacts in the generic OSC.

The pfd values used are typical of general industrial operations, processes and equipment. This is appropriate given the absence of supporting data and substantiation that would be expected at the detailed design stage. This means that the assigned fault class, based on the relevant bounding source term and facility throughput, is demonstrably the worst case and will not be increased by the accommodation of higher-precision pfd values. As the design develops, waste stream specific throughputs will be compiled in a population to demonstrate that the safe operating envelope remains valid.

A sensitivity assessment has been undertaken within Section 3.2.2 to evaluate the impact of less conservative IEF estimates that would be used when appropriate substantiation of the claims and capabilities of plant and equipment can be demonstrated.

2.6.3 Illustrative assessment of safety measure requirements

The detailed assessments (HAZAN and HAZDOC) 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 detailed in the NOSM 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 risk reduction measures were reviewed to determine which are feasible to implement and to identify further work relating to design development to better understand the fault initiators and progression. This information is presented in Appendix B and gives high confidence that a robust safety argument can be developed to satisfy the requirements of DBAA in the full safety case.

2.7 Overview of fault sequence groups assessed

As defined in the BOA report, the waste packages received from the waste producer are assumed to meet the waste acceptance criteria. Nonetheless checks will be made when the waste package is received. For a worker or member of the public to receive a radiological dose, the waste package containment and, in some cases, transport containers, would have to be compromised by a fault. The faults of interest relate to a dropped load or impact, fire,

external event or operator error. A direct (shine) or indirect exposure pathway (inhalation or ingestion) to a worker or member of the public could arise if there is a loss of the waste package containment and/or shielding.

The HAZAN groups are presented in Table 4. A further description of the fault groups is provided within the following section including a justification for excluding some faults from detailed assessment. The criticality faults detailed in the preliminary fault schedule are discussed in Volume 4 of the generic OSC.

2.7.1 Faults not assessed within the 2016 generic OSC

The following fault sequence groups have not been assessed in the 2016 generic OSC and the justification for their omission at this stage of the GDF programme is summarised below.

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. An event of this type requires rupture of a spent fuel canister and loss of the multiple water barrier which also provide containment. The exclusion of these faults requires resolution of other FAPs related to dropped loads and stability of the structures below ground.

Contaminated wounds

Assessments of radiological consequences arising from injection and/or contaminated wound pathways have not been undertaken. 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.

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. This assumption is supported by operational experience at a number of nuclear sites where monitoring during LOOP events has shown no significant increase in airborne contamination levels. A FAP has been raised (FAP.2016.VOL3.10) to undertake a study to identify which areas of the GDF design are vulnerable to LOOP. Other issues related to conventional safety (ie flooding and air quality) are discussed in Volume 1.

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. A FAP has been raised (FAP.2016.VOL3.11) to undertake a study to define requirements and develop the ventilation system design to a level which permits loss of ventilation faults to be assessed. 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. No safety analysis has been undertaken at the generic OSC stage. This claim will be substantiated as the safety case and design develops (FAP.2016.VOL3.09) and will be considered in relation to design requirements related to retrievability.

Loss of containment (spread of contamination)

Transport packages have strict limits on removable contamination levels on their surfaces in order to comply with the Transport Regulations. This is limited by the waste package specification and release rates set to comply with A_2 values (whichever is the most onerous). As a result, there may be low levels of contamination present on or within transport containers received at the GDF. The design intent is that the GDF will be operated as a 'clean' facility with all necessary controls as required by IRR99 to ensure that risks to workers are ALARP from normal operations.

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 of compliance with the ALARP principle.

Fire

Potential fire hazards associated with the GDF have been identified through the hazard identification studies and recorded in the preliminary fault schedule. The scope of work has been limited to estimation of the combination of release fractions and containment factors required to screen faults as being below the design basis thresholds.

The application of a safety integrated design process in support of developing the full assessment will ensure that the hazard management strategy focuses on elimination and preventing spread. This will be required to ensure compliance with conventional safety requirements. 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. For example, the developing design will need to consider features such as:

- the exclusion of energetic systems and energy sources from the sub-surface environment (where practicable)
- minimisation of hydrocarbon and other flammable material inventories such that there are no major fuel sources
- changes to the backfilling strategy to eliminate the potential for emplaced waste packages to be exposed to a fire
- application of relevant good practice such as the Mines Regulations to minimise the potential for underground fires and their spread

As the majority of the GDF is underground, the fire hazard may result in specific additional requirements related to conventional rather than radiological safety. In such cases the more stringent requirements will need to be adopted. A hazard management strategy for fire hazards will include the following core elements:

- provide a means of preventing initiation of fire
- provide a means of preventing fire capable of challenging the thermal withstand of a package

- provide a means of preventing or minimising worker exposure to radioactivity in the event of fire
- provide a means of preventing the spread of fire and its effects, including smoke

These will be developed as the safety case and design mature and will be adopted within design principles in the GDF requirement set.

FAP.2016.VOL3.01 has been identified to manage future work associated with the fire hazard. The purpose of the FAP is to ensure that appropriate design optimisation is undertaken so that fire faults are not unnecessarily included in the design basis. This includes the specific case of the fire withstand of a HLW/spent fuel disposal container which is to be confirmed to avoid over-specification of safety measures arising from an excessively conservative calculation of harm potential from loss of neutron shielding.

2.7.2 Faults assessed within the 2016 generic OSC

The following fault sequence groups have been assessed within the 2016 generic OSC, either quantitatively through the DBAA or qualitatively, where appropriate.

Loss of shielding

This fault sequence group is associated with process errors and non-impact related events resulting in shielding failures and an worker being exposed to an unshielded waste package in error. This could be due to an incorrect operational sequence being followed such as the return of a 'loaded' SWTC to the collection area or personnel accessing the inlet cell when an unshielded waste package is located within the cell.

Dropped load/impact

Waste packages need to be lifted and moved during GDF operations. As a result, there is a potential for the waste packages to be dropped or to be subjected to an impact. This could be due to, for example:

- failure of lifting or stacking arrangements
- impacts resulting from failures in the transfer process from the surface to the sub-surface environment, ie accidents in the shaft or drift
- impact from transport vehicles
- impact with other waste packages

Internal hazards

Internal hazards are defined in the NOSM as 'those hazards to plant and structures that originate within the site boundary and over which the facility operator has control over the initiating event in some form'. It is implicit within the definition that the internal hazard must compromise a safety function provided by a structure, system or component (SSC) supporting an engineered safety measure.

These hazards could impact the waste packages directly, such as fire, explosions or flooding, or they could induce secondary events, such as a loss of services or ventilation leading to a spread of contamination or other domino effects, such as build-up of flammable gases resulting in fires.

External hazards

External hazards are defined as those challenges to integrity or function which are outside the control of the operator of the facility. These hazards can be from naturally occurring events, for example, a seismic event, flooding or extreme weather, or from man-made events, such as an incident at another site/facility adjacent to the GDF or aircraft impact.

These hazards have the potential to damage the GDF buildings, structures, plant or equipment (surface and sub-surface). There is also the potential for these hazards to result in a fire, directly or through domino effects. Ultimately, they could lead to a loss of the waste package containment and a release of radioactive material and/or exposure.

2.8 Safety analysis approach to support a feasibility study

The faults associated with loss of shielding and dropped loads and impacts have been assessed quantitatively, subject to the limitations stated in Section 2.7. For the fire hazards, the only activity undertaken at this stage of this GDF programme was the demonstration that the release fractions would need to be diminishingly small to justify screening from further assessment. This will be taken forward as an input to inform development of a hazard management strategy and the associated design principles.

The assessment of internal hazards (HAZAN 6) requires a greater level of design definition than is currently available before potential impacts can be related to loss of any specific safety system component. For this reason, the approach has been to identify which internal hazards have the potential to affect the key safety functions. The conclusions from this review will be used to inform the hazard management strategy and design development process.

The assessment of external hazards (HAZAN 5) requires some knowledge of the site or potential sites in order to perform a quantitative assessment. At this generic stage of the project, no sites have been identified. As a result, external hazards have been the subject of a qualitative rather than quantitative assessment as the site-specific data required to perform a detailed safety analysis are not available at the generic stage.

The results of the accident safety analysis are reported in Section 3.

3 Results of Safety Analysis

3.1 Quantified assessment

The fault sequence groups subjected to quantitative DBAA have been assessed at a level appropriate to the current stage of the GDF programme. The results are summarised in Table 7 below.

Table 7 Fault Analysis Results (DBAA with Fault Class assignment)

Fault Sequence Group Number	Fault Sequence Group	Indicative DBAA Fault Class	Indicative Risk Reduction Target
3.F.6.2.1	Inadvertent exposure to elevated levels of radioactive material in air due to loss of disposal unit containment following stack collapse within UILW vault	B	3.2E-06
3.F.6.1.1	Inadvertent exposure to elevated levels of radioactive material in air due to loss of disposal unit containment following stack collapse within SILW/LLW vault	B	3.2E-05
1.D.6.2.1	Inadvertent exposure to elevated dose rates due to accessing SWTC (UILW) inlet cell facility when unshielded package present	C	3.2E-04
1.E.6.2.1	Inadvertent exposure to elevated dose rates due to SWTC unloading operations commencing with staff adjacent with UILW inlet cell door open	C	3.2E-04
3.B.6.1.1	Inadvertent exposure to elevated dose rates due to damage to disposal unit shielding following impact in SILW vault	C	3.2E-03
1.A.6.2.1	Inadvertent exposure to elevated dose rates from package within SWTC returned to collection area in error	C	3.2E-03
1.E.6.3.1	Inadvertent exposure to elevated dose rates in DCTC receipt area due to HLW/spent fuel deposition operations commencing with shield door open	C	3.2E-03
3.C.6.3.1	Inadvertent exposure to elevated dose rates due to loss of shielding following vehicle impact with HLW/spent fuel holding system	C	3.2E-03
1.E.5.3.1	Inadvertent exposure to elevated dose rates due to DCTC unloading operations commencing with DCTC receipt area shield door open	C	3.2E-03

Fault Sequence Group Number	Fault Sequence Group	Indicative DBAA Fault Class	Indicative Risk Reduction Target
1.B.6.3.1	Inadvertent exposure to elevated dose rates from disposal unit present in error during maintenance of HLW/spent fuel deposition machine	D	3.2E-01

To ensure an appropriate level of conservatism in the fault classification, all faults that lie close to the transition between fault classes have been assigned the higher class.

For the assessed faults, the fault classification is based on the unmitigated worker dose. In all cases, the unmitigated doses to the public are below the design basis thresholds. The assessment therefore concludes that there are no design basis accidents in that grouping which will require severe accident analysis due to the potential off-site dose to a member of the public.

A group of faults related to the use of a shaft or drift for surface to sub-surface transfers has not been subject to full quantitative assessment of DBAA. These fault sequence groups are listed in Table 8 below. A qualitative safety argument is presented in Section 3.2.1.

Table 8 Fault Analysis Results (DBAA without Fault Class assignment)

Fault Sequence Group Number	Fault Sequence Group
3.A.4.1.1 (LS) & 3.E.4.1.1 (LC)	Impact with Shielded Intermediate Level Waste (SILW) /Low Level Waste (LLW) transport unit in shaft leading to: • total loss of shielding (LS) and inadvertent exposure to elevated dose rates • total loss of containment (LC) and elevated levels of radioactive material in air
3.A.4.2.1 (LS) & 3.E.4.2.1 (LC)	Impact with Standard Waste Transport Container containing Unshielded ILW (UILW) transport unit in shaft leading to: • total loss of shielding and inadvertent exposure to elevated dose rates • total loss of containment and elevated levels of radioactive material in air
3.A.4.3.1 (LS) & 3.E.4.3.1 (LC)	Impact with Disposal Container Transport Container (high heat generating waste) transport unit in shaft leading to: • total loss of shielding and inadvertent exposure to elevated dose rates • total loss of containment and elevated levels of radioactive material in air
3.A.4.1.2 (LS), 3.A.4.2.2 (LS), 3.A.4.3.2 (LS), 3.E.4.1.2 (LC), 3.E.4.2.2 (LC) & 3.E.4.3.2 (LC)	Inadvertent exposure to elevated dose rates due to damage to disposal unit shielding and inadvertent exposure to elevated levels of radioactive material in air due to loss of disposal unit containment following impact during surface to sub-surface transfer in the drift

3.2 Loss of shielding

For those faults which result in a worker being exposed to an unshielded waste package in error, the safety analysis has identified the CSFRs. The means of meeting these requirements may be included in the current GDF concept or can be identified from comparable operations at other nuclear sites and are readily adaptable. This approach ensures that there is a high degree of confidence in claims of feasibility being made now.

For example, if unshielded waste packages are to be removed from the SWTCs to enable emplacement, this introduces the potential to expose workers if they enter the area whilst operations are being undertaken. Therefore, the design needs to consider, through suitable optioneering, the application of the NOSM hierarchy of controls (eliminate, prevent, protect, mitigate) to derive the optimum design solution. Illustrative examples of risk reduction measures based on the hierarchy are provided in Appendix B and include:

- elimination of the fault by building up the disposal unit within a shielded structure (such as a concrete block) at the surface or
- providing a means of protecting workers from direct radiation from exposed waste packages (such as remote handling through a shielded cell with suitable shield doors and access control through interlocks) or
- preventing operations taking place when the facility is in an unshielded (open) configuration

For those activities and areas associated with HLW/spent fuel, the CSFRs would be similar to those identified for SWTCs, but the conceptual safety measure performance requirement would be an order of magnitude lower due to the in external dose rates.

The safety measure performance requirement is lower for HLW/spent fuel because of the inherent shielding within the waste container which limits the surface dose rates. This means that the inherent shielding and containment of the package has a high safety class (probably class 1) and will be subject to robust substantiation to support the claim by the waste producer.

For the assessed design basis loss of shielding faults (which are all class C or D), the risk reduction targets could be achieved by implementing functional requirements and through the design development process. Possible design solutions included in Appendix B are typical of engineered safety measures already provided in UK nuclear licensed facilities (such as area gamma monitors/alarms and interlocks) and are therefore considered feasible.

3.2.1 Dropped loads and impacts

As discussed in Section 3.1, faults associated with transferring waste packages down the emplacement shaft or drift have not been subject to DBAA at this stage of the GDF programme. These faults are based on the dropping or loss of control during lowering of waste packages (SILW, UILW and HHGW) down the shaft or a loss of control of during transfer down the drift, resulting in damage to the waste package and loss of shielding and of containment. For the loss of containment pathway, there is considerable uncertainty associated with the behaviour of the waste package and disposal unit in the event of impact and this requires resolution in order to assign an overall fault class from all pathways.

For the shaft, risk reduction measures include features such as:

- preventative risk reduction measures:
  - high integrity and reliability lifting equipment and load path
  - changes to the shaft design to limit drop heights including combined drift and shaft access
  - engineering features to prevent damage to the package

- protective safety measures:
  - load follower or arrestor devices
  - engineering features to limit damage to the package
  - shielding and containment barriers at the top and bottom of the shaft coupled with exclusion of personnel
- mitigating safety measures:
  - impact absorbing devices or materials
  - radiation monitoring equipment

All illustrative measures will form part of the considerations in future design development and optioneering and are presented in more detail in Appendix B.

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). These are designed, constructed and operated to the highest safety standards, and include fail-safe systems. At the operating facility for the disposal of transuranic waste within evaporite deposits at the Waste Isolation Pilot Plant (WIPP) in the USA, waste is transported via shafts. In addition, it was proposed to utilise shaft transport at a repository in the Gorleben salt dome in Germany. The shaft systems 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, because nuclear lifts are normally kept to a minimal height and undertaken within the withstand capability of the package.

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 IEF 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.

For impact hazards in the drift, the most challenging fault is considered to be a runaway locomotive (noting wheeled vehicles are planned for use in other international geological disposal concept designs) and a loss of containment due to an impact within the drift. As with the shaft, a variety of risk reduction measures are planned for use in other GDF projects. Risk reduction measures in Appendix B include the following:

- preventative safety measures:
  - the use of rack and pinion rail systems
  - dedicated independent braking provisions
- protective safety measures:
  - train protection and warning systems
  - worker exclusion through engineered access controls
  - shield and containment barriers
  - speed limiters and buffers
- mitigative safety measures:
  - radiation monitoring equipment

Faults that have been subject to a wider scope of DBAA include two dropped load/impact faults related to stack collapse in the vault. The NOSM specifies the safety measure requirements for class B faults as:

- two diverse, similar reliability, segregated engineered safety measures
- detailed common cause failure analysis to demonstrate negligible probability of failure on demand compared to independent failure probability
- no vulnerability to single failure criterion

FAP.2016.VOL3.07 has been identified to further design development and assessment. For the vault, the development and optimisation of the design and operating philosophy will include consideration of a range of risk reduction measures. Illustrative safety measures identified are given in Appendix B and include the following:

- elimination of the fault by removal of the need to stack waste packages at height:
  - modifying the vault emplacement strategy to stack in layers and backfilling by layer
- preventative safety measures:
  - high integrity and reliability lifting equipment and load path
  - engagement guides or racks to align and retain stacked waste packages
  - engineering features to prevent damage to the package
  - handling and emplacement in protective pre-formed concrete boxes
- protective safety measures:
  - remote handling and emplacement
  - shielding and containment barriers coupled with exclusion of personnel
- mitigating safety measures:
  - radiation monitoring equipment
  - ventilation

As a general principle, in terms of minimising the risks associated with dropped loads, the preferred approach is to:

- eliminate the need for lifting packages
- if this is not possible, use of suitable preventative measures to render such an event very unlikely, including ensuring that a fall or impact beyond the withstand capability of the package is impossible
- protection of workers by excluding them from the area with suitable barriers and access controls
- mitigation measures such as ventilation

FAP.2016.VOL3.08 has been raised to optimise the lifting and emplacement strategy. In addition, the potential for package to package impacts resulting in damage and a radiological hazard requires further investigation in terms of segregation and sentencing (FAP.2016.VOL3.14).

The remainder of the faults are all class C or D. The NOSM specifies the safety measure requirements for class C faults as two engineered safety measures that are:

- redundant
- of similar reliability
- segregated

- with common cause failure potential demonstrably low (including dependencies due to operator actions).

For class D faults, the requirement is for a single engineered or procedural safety measure. Safety measures for class D faults are not covered in Appendix B .

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. This is presented in more detail in Appendix B .

3.2.2 Sensitivity analysis

Sensitivity analysis of the results of the accident safety assessment determines whether there are any contributors for which uncertainties or variabilities may lead to a change in fault class. For this stage of the GDF programme any sensitivity analysis is illustrative only.

The sensitivity analysis has focused on topics of relevance to work being undertaken now, in particular, disposability assessments and provision of waste packaging advice. Input parameters considered fall into 3 categories: those related to the waste package, the IEF, and other parameters such as those relating to worker exposure.

The impact of changes to these values on the provisional assessment and classification of faults could potentially be:

- under-classification of faults and hence insufficient engineered safeguards are assigned or the risk reduction targets are set too low
- over-classification of faults and hence the safety demands placed on the design are too onerous

3.2.2.1 Waste package contents

Variations in the waste package contents that could result in a change of fault class include:

- variability arising from a waste category that is not homogeneous or from an inconsistent or low reliability packaging process with a homogenous waste category (overbatching)
- uncertainty arising from the inability to accurately determine the contents, for example, the inherent physical limitations of measurement systems

Some very conservative assumptions are made in the assessment of faults that lead to a loss of containment, including:

- The form of the waste within the package – for example, many waste streams will be immobilised in grout or the radioactive content will be associated with structural or other components either as surface contamination or as material diffused into the component surfaces. This means that a much smaller proportion of the package contents is likely to contribute to the fault in the form of dispersible material than is currently assumed.
- The current assessments assume release fractions applicable to the free fall of material, whereas the radioactive material in a waste package is not in a state which permits free fall therefore introducing an additional level of pessimism.
- The current assessments take no credit for the fact that the waste package itself will retain a level of containment following an accident. However, typically containment factors of between 10 and 100 can be claimed where the post-accident performance can be substantiated.

3.2.2.2 Initiating Event Frequency

The input parameters used to define the IEFs are based on very conservative estimates of:

- human error probability (1E-02 per demand/task)
- mechanical failure (probability of failure on demand of 1E-03 per demand/task)
- throughput of either 2300 packages per year for SILW and UILW or 200 packages per year for HLW/spent fuel packages

Throughput is derived from a system requirement to meet the demands of the transport schedule limit. This is an upper value and as such any variation will only reduce the IEF.

Both the human error probability and pfd for systems have been selected to be conservative; as such any variations would be expected to be beneficial and would therefore reduce the IEF. This is particularly of interest for SILW and UILW related faults.

The IEF would need to be reduced by two orders of magnitude in order to affect the fault class assignment. This would require claims of human error probabilities at the human performance limiting value of 1E-04 per demand/task or mechanical failures at 1E-05 per demand equivalent to Safety Integrity Levels 3 or 4. Such claims of individual or cumulative improvements cannot be substantiated at this stage.

3.2.2.3 Other parameters used in fault modelling

Conservative estimates have been made for the values of worker exposure time and separation distance between the source and the worker. There is a direct relationship between these parameters and the calculated consequences. However, any variation in the parameters is likely to be only a single order of magnitude at the most. For example, an assumption of a 1 hour task duration would require a real task duration of 10 hours to increase the estimated dose by an order of magnitude. Hence the assignment of fault class is not particularly sensitive to these parameters.

3.3 Considerations for optioneering

The class B faults relate to stack collapse events in the vaults. It is currently assumed that SILW vaults are man-access for emplacement. Removing this requirement, in advance of exploring other means of eliminating the fault, and isolating the worker from the hazard by adopting remote operation is on its own a credible means of reducing the consequences below the design basis fault region. FAP.2016.VOL3.16 has been raised to ensure the DASI process is implemented in full at the appropriate stage and includes consideration of all means of reducing risks.

3.4 Feasibility of potential risk reduction measures

Credible options for risk reduction have been identified and are reported in Appendix B to support claims of feasibility. They are presented in terms of engineered safety measures already implemented and detailed in the design reports [9] or in use for comparable operations at currently operating facilities. A summary of the conclusions of this review is presented in Table 9.

Table 9 Initial Demonstration of Feasibility of Safety Measure Provision

Fault Sequence Group Number	Fault Sequence Group	Initial Fault Class & Risk Reduction Target	Number of Safety Measures Required	Options Presented in Appendix B
3.F.6.2.1	Inadvertent exposure to elevated levels of radioactive material in air due to loss of disposal unit containment following stack collapse within UILW vault	B 3.2E-06	2 engineered, diverse, meets single failure criterion	Yes - 2 engineered measures
3.F.6.1.1	Inadvertent exposure to elevated levels of radioactive material in air due to loss of disposal unit containment following stack collapse within SILW/LLW vault	B 3.2E-05	2 engineered, diverse, meets single failure criterion	Yes - 2 engineered measures
1.D.6.2.1	Inadvertent exposure to elevated dose rates due to accessing SWTC (UILW) inlet cell facility when unshielded package present	C 3.2E-04	2 engineered with redundancy and segregation	Yes - 2 independent engineered measures
1.E.6.2.1	Inadvertent exposure to elevated dose rates due to SWTC unloading operations commencing with staff adjacent with UILW inlet cell door open	C 3.2E-04	2 engineered with redundancy and segregation	Yes - 2 independent engineered measures
3.B.6.1.1	Inadvertent exposure to elevated dose rates due to damage to disposal unit shielding following impact in SILW vault	C 3.2E-03	2 engineered with redundancy and segregation	Yes - 2 independent engineered measures
1.A.6.2.1	Inadvertent exposure to elevated dose rates from package within SWTC returned to collection area in error	C 3.2E-03	2 engineered with redundancy and segregation	Yes - 1 engineered measure supported by administrative controls

Fault Sequence Group Number	Fault Sequence Group	Initial Fault Class & Risk Reduction Target	Number of Safety Measures Required	Options Presented in Appendix B
1.E.6.3.1	Inadvertent exposure to elevated dose rates in DCTC receipt area due to HLW/spent fuel deposition operations commencing with shield door open	C 3.2E-03	2 engineered with redundancy and segregation	Yes - 2 independent engineered measures
3.C.6.3.1	Inadvertent exposure to elevated gamma dose rates due to loss of shielding following vehicle impact with HLW/spent fuel holding system	C 3.2E-03	2 engineered with redundancy and segregation	Yes - 2 independent engineered measures
1.E.5.3.1	Inadvertent exposure to elevated dose rates due to DCTC unloading operations commencing with DCTC receipt area shield door open	C 3.2E-03	2 engineered with redundancy and segregation	Yes - 2 independent engineered measures
1.B.6.3.1	Inadvertent exposure to elevated dose rates from disposal unit present in error during maintenance of HLW/spent fuel deposition machine	D 3.2E-01	1 engineered or procedural	Yes - 1 engineered measure supported by administrative controls

3.5 Qualitative assessment

3.5.1 External hazards

The methodology applied in the assessment of external hazards is appropriate for a generic assessment when the location of the GDF site is unknown. The approach and methodology adopted is summarised in Figure 4 and includes the following:

- define a list of external hazards appropriate to a generic OSC, classified by hazard group according to whether the event has its source:
  - in the atmosphere or space (‘air-based’)
  - in the aquatic environment (‘water-based’) or
  - In the terrestrial environment (‘ground-based’)
- screen the list of external hazards based on consideration of criteria including:
  - relevance to the UK
  - relevance to the GDF and its operations and
  - IEF (exclude where less than 1.0E-07 per annum)

- establish a set of relevant external hazards appropriate to a generic OSC within the screening criteria and, for each of the baseline set of external hazards, identify whether it is applicable to:
  - the surface facilities design
  - the surface to sub-surface facilities design
  - the sub-surface facilities design or
  - the movement of the waste packages through the GDF systems
- for each of the baseline set of external hazards, determine the design basis events only for those naturally occurring external hazards for which a generic, non-site-specific approach can be applied
  - for these naturally occurring external hazards, establish regional design basis events (frequency of 1.0E-04 per annum) magnitude or hazard intensities and
  - where practicable, consider potential 'cliff-edge' effects by establishing the magnitude or hazard intensities at an occurrence frequency an order of magnitude lower (ie 1.0E-05 per annum)
- for each of the naturally occurring baseline set of external hazards, consider the potential impact of climate change and credible hazard combinations

The design basis event magnitude, or hazard intensity, of the external hazard in question is the intensity level that GDF structures and safety-related plant and equipment will be designed to withstand. 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.

The focus at this stage is natural external hazards since they are largely independent of the site. In addition, some generic man-made hazards are considered. It is acknowledged that a more comprehensive assessment cannot be made until the site-specific design has been produced. Man-made external hazards do not have a frequency-magnitude relationship in the same sense that natural events do. Instead, the design basis requirements will be based on the credible hazards in a specific location. For example, the frequency and magnitude of an impact from road traffic or an accident in an adjacent industrial facility will clearly be dependent on the specific location and size of these hazards.

Even for more widespread hazards such as aircraft impact, the probability of an accidental crash impacting a GDF will be highly dependent on the amount of air traffic and proximity to airports of the selected sites. Over long timescales it is reasonable to assume that there is potential for change in land use and the introduction or removal of man-made hazards during the planned period of GDF operation (100+ years). Therefore, at this stage, this will remain in the design basis fault set, as recommended in international best practice and required under UK regulations as part of the nuclear site licensing process.

The baseline set of external hazards considered at this stage of the GDF programme 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 safety assessment does not yet include any assessment of malicious acts. The current regulatory expectation is for malicious acts to be treated as external hazards. Challenges from such acts may well outweigh those from accidents in the development of an acceptable

design. The assessment of malicious acts will be reported in separate documents not included in the published suite due to restrictions within extant UK security regulations.

The baseline set of external hazards applicable to the GDF in the UK has been collated and, where possible, illustrative design basis event magnitudes defined. In addition, combinations which occur simultaneously or nearly simultaneously have been identified (correlated hazards). Examples include extreme high winds and extreme heavy rain or storm surge from the coincidence of high tide, abnormally low atmospheric pressure and high winds. The external hazards (including correlated hazards) provide a basis that will be taken into account as the siting process and GDF design develops.

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 as shown in Figure 5. This division is based on those hazards for which the available data show regional variation. For some natural external hazards; namely snowfall, lightning and seismicity; there is a large amount of historical data available and there are broad patterns of variation across the UK. These data and broad patterns of variation provide the basis for division of England and Wales into the six regions.

Table 10 shows the variation of design basis event magnitude, for natural external hazards, across the geographical regions. 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. The single parameter with a significant variation is extreme low temperature which, based on historical records, has a maximum difference of approximately 25 °C between inland and coastal sites.

In the case of human-made external hazards, air traffic density provides a regional discriminant for the aircraft crash hazard. The regional variation of aircraft crash rates and relationship to air traffic density and/or location of major UK airports has been assessed. This does not include determination of a specific design basis event at a local level as the exact proximity to airports/airfields, which is a major factor for the design basis event calculation, will not be known until later in the site selection process.

Figure 4 Process for Derivation of Design Basis External Events

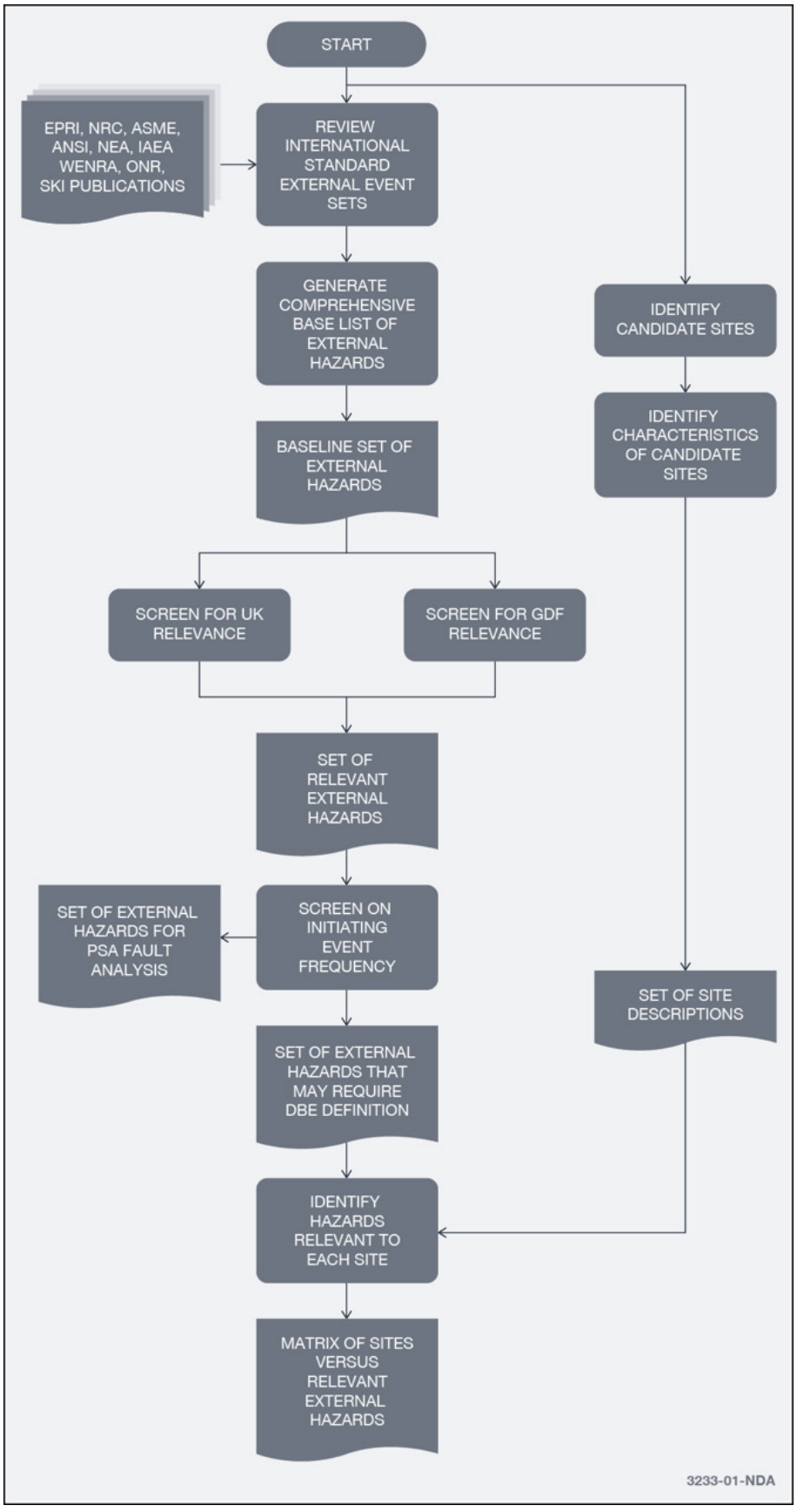


Table 10 UK Magnitude Values for 1E-04 pa Return Frequency

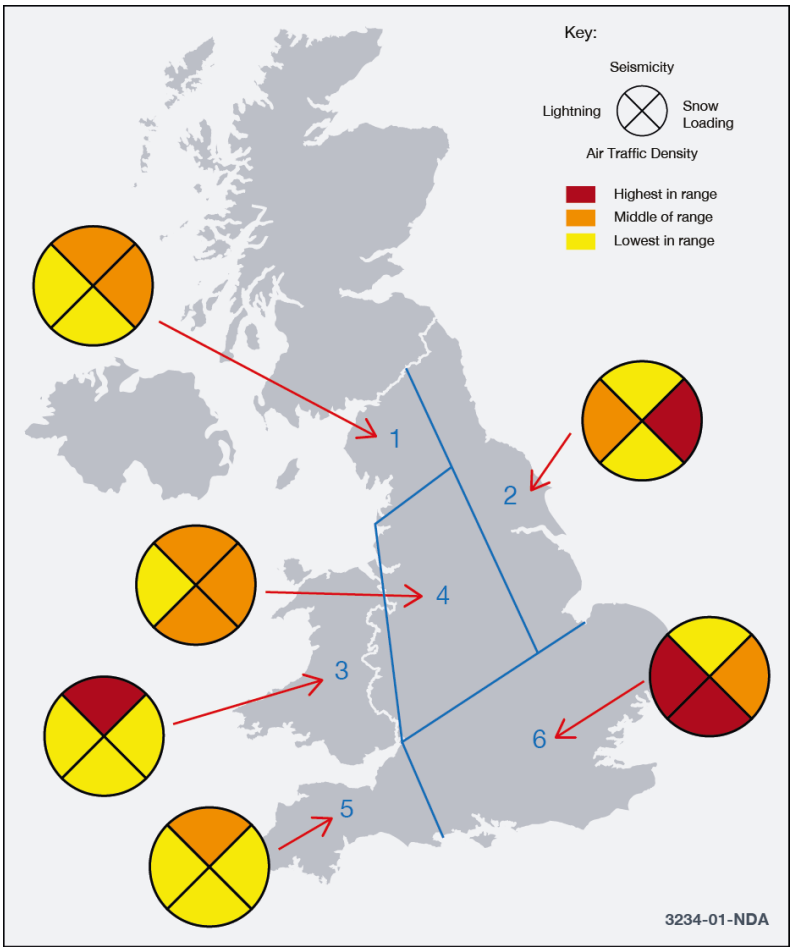
Category	Sub Category	Max	Median	Min
Wind	Maximum Hourly Wind Speed ($m\ s^{-1}$)	34.7	32.6	30.6
	Effective Wind Speed ($m\ s^{-1}$)	60.1	56.9	54.5
Temperature (Coastal)	High Temp (°C)	42.8	40.2	38.9
	Low Temp (°C)	-16.5	-18.3	-22.0
Temperature (Inland)	High Temp (°C)	45.4	42.2	41.5
	Low Temp (°C)	-29.3	-32.9	-32.9
Snow	Snow Loading on Ground ($kN.m^{-2}$)	1.4	1.4	1.1
Lightning	Lightning Flash Density (pa)	1.8E-03	1.6E-03	9.0E-04
Seismicity	Seismic pga (g)	0.26	0.24	0.18

Figure 5 shows the design basis event magnitude in each region for those external hazards on which the regional division is based. The magnitude for each hazard in each region is indicated by a colour. For a given hazard in the UK:

- The region corresponding to the largest magnitude is red;
- The region corresponding to the smallest magnitude is yellow, as are any other regions with approximately the same magnitude as the smallest;
- The remaining regions in the middle of the range are orange.

Figure 5 shows that while there is a regional variation, in no cases is this variation significant enough to warrant either significant design change or exclusion of any region. None of these external hazards would present a challenge to the feasibility of implementing a GDF anywhere in the UK, provided the appropriate hazard management strategies are in place.

Figure 5 Overview of Relative Regional Variability of Key External Hazards



Future changes in the UK climate, driven by global warming, solar cycles or other climatic phenomena, will influence the frequency and/or magnitude of many of the natural hazards considered relevant to the GDF. There are very large uncertainties involved in modelling the future impacts of the release injection of 'greenhouse gases' into the atmosphere resulting from significant uncertainties in the prediction of global generation rates for these gases. Climate change projections carried out by the UK Meteorological Office have been examined. The review concluded that the effects are bounded by the hazard intensity for an order of magnitude increase in the timescales considered for the design basis event (1 in 10,000 year return as opposed to 1 in 1,000).

The assessment of external hazards has also considered the potential for combination with other hazards:

- two hazards are more onerous than in isolation; and
- the hazards can be correlated (ie more likely to occur together than just by chance)

From the baseline set, credible external hazard couples have been identified which may need to be considered as the design of the GDF develops. External hazard couples have been defined as either 'weak', 'medium' or 'strong' coupled for future consideration in the developing design. As illustrative examples, the strongly coupled or correlated hazards are shown in Table 11.

Table 11 External Hazards with 'Strong' Coupling

ID	Natural or Man-made Events	ID	Coupled Natural or Man-made Events
A4.2	Extreme rainfall	A1.3	Hurricane
A4.3	Extreme hail	A1.3	Hurricane
A4.2	Extreme rainfall	A1.4	Cyclone
A4.3	Extreme hail	A1.4	Cyclone
W3.12	Storm surge	A4.2	Extreme rainfall
W3.15	Waterspouts	A4.3	Extreme hail

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. The assessment will be extended to cover Northern Ireland as the siting process progresses.

It is recognised that the external hazards assessments will need to consider impacts in the sub-surface areas, beyond design basis events and domino effects. This full assessment will be undertaken when site-specific information is available.

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 adoption of suitable design principles. This will, in turn, drive the need for design development from which design solutions to manage external hazards will be developed.

Further items of work specified for the site-specific stage are:

- the list of generic design basis events defined for external hazards affecting the GDF will need to be systematically reviewed and extended once a site has been selected
- the safety functional requirements will have to be considered against the site-specific design once candidate sites have been selected and the associated external hazards have been assessed in detail
- once the GDF design reaches the site-specific stage, the magnitude and frequency of coupled external hazards should be determined and consideration should be given to the identified potential for 'causal' or 'sequential' relationships between external hazards

3.5.2 Internal hazards

Internal hazards are defined in the NOSM as 'those hazards to plant and structures that originate within the site boundary and over which the facility operator has control over the initiating event in some form'.

The assessment of internal hazards (HAZAN 6) requires a greater level of design definition than is currently available before potential internal hazards can be linked to any specific safety system component. For this reason, the approach has been to identify which internal hazards have the potential to affect the key safety functions. The conclusions from this will be used to inform the hazard management strategy and design development process.

A summary of the nature of the assessment is presented below:

- a sequential approach has been taken in considering internal hazards relevant to the GDF
- review of the internal hazards resulting from the hazard identification process conducted for the generic OSC
- potential causes, potential consequences and hazard management strategies are identified for each of the internal hazards identified in the preliminary fault schedule
- consideration of the likely GDF safety functional requirements (at a high level) to determine their possible vulnerability to internal hazards

The internal hazards identified at this stage of the GDF programme are as follows:

- internal fires and explosions, resulting in damage to infrastructure, structures or loss of services
- internal flooding due to failures such as:
  - fire-fighting system activation
  - water (or other fluid) vessel or pipework failure
  - flooding from the surface or an aquifer leading to in-rush, resulting in loss of services such as electrical supplies or ventilation
- dropped loads and other impacts resulting in damage to infrastructure, structures or loss of services
- energetic releases such as failure of pressurised systems or missile generation from degeneration of machinery and equipment
- gas generation
- exothermic chemical reactions
- structural faults and failures introduced by construction-related errors
- interactions and interfaces from parallel working with simultaneous construction, emplacement or decommissioning

As the GDF is at the generic stage, the assessment focuses on identifying the internal hazards that are both likely and, in the absence of optimisation, potentially significant if not addressed. Based on the generic list from the NOSM, 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.

Recognising that internal hazards might lead to the loss of a structure, system or component providing a safety function, the likely GDF safety functional requirements have been reviewed to determine the nature of the vulnerability and potential effect on safety.

Table 12 Vulnerability of Potential Safety Functional Requirements to Internal Hazards

Potential GDF Safety Functional Requirement	Potential Vulnerability to Internal Hazards
Provide a means to stop/ prevent worker access to areas of elevated potential radiation levels	Likely to be provided by a variety of structures (for example, shield doors), systems (such as interlocks) and components. Detailed assessment required once the means and location of the SSCs have been identified because the means to stop/prevent worker access is potentially affected by the majority of types of internal hazard, including fires, flooding (for example, leading to loss of power), impacts and dropped loads.
Provide a means to prevent operations commencing when a package is present	Likely to be provided by a variety of systems (such as interlocks) and components. Detailed assessment required once the means and location of the SSCs have been identified because the means to prevent operations commencing is potentially affected by internal hazards such as fires, flooding (for example, leading to loss of power), impacts and dropped loads.
Provide a means to prevent the exposure of people to direct radiation	Likely to be provided by robust structures. Detailed assessment required once the shielding design has been completed, recognising that the structures may be adversely affected by internal hazards such as impacts and dropped loads.
Provide a means for remote handling of packages	Likely to be provided by cranes. Detailed assessment required once the means and location of the SSCs have been identified. The crane, and the structures that support the crane, have the potential to be adversely affected by the majority of types of internal hazard, including fires, flooding (for example, leading to loss of power, loss of structural stability), impacts and dropped loads.
Provide the means to confirm the presence of a loaded package	Likely to be provided by an engineered system comprising components. Detailed assessment required once the means and location of the SSCs have been identified because the means to confirm the presence of a loaded package is potentially adversely affected by the majority of types of internal hazard, including fires, flooding (for example, leading to loss of power), impacts and dropped loads.

Potential GDF Safety Functional Requirement	Potential Vulnerability to Internal Hazards
Provide a means to prevent a drop of a load onto safety systems	The use of cranes and other lifting devices within the GDF means that the potential for a dropped load will be an important safety consideration. The means to prevent drops beyond the withstand capability of waste packages or to prevent the possibility of stack collapse could be met by revisions to the emplacement strategy (FAP.2016.VOL3.08). In addition, the potential for dropped loads directly onto safety systems needs consideration.
Provide a means to prevent an uncontrolled vehicle drive-away	Likely to be provided by a variety of systems (for example, interlocks) and components. Detailed assessment required once the means and location of the SSCs have been identified because the means to prevent drive-away are potentially affected by internal hazards such as fires, flooding (for example, leading to loss of power) impacts and dropped loads.
Provide a means of preventing structural collapses in the underground vaults and tunnels	The underground structures will be supported by specific engineered safety measures. However, structural movements or collapses caused either by construction or installation errors (an internal hazard) or soil or ground changes or instabilities (an external hazard) will need to be assessed as part of the developing design. FAP.2016.VOL3.05 has been raised to address the need for input information to this analysis while for the external hazard initiated case FAP.2016.VOL3.15 has been raised.

4 Implementation

The accident safety assessment has identified, at a generic level, issues that require further design development and additional assessment. The issues recorded here are consistent with the level of design detail available at this stage. Many are typical of issues that will be considered during development of major infrastructure or large construction projects. Others are more specific to GDFs and the functions required to access and work in an underground facility, and have a strong correlation to issues that are routinely managed in sub-surface mining operations.

Further work will be required in terms of optioneering and design development in order to develop solutions which will ensure that RWM safety criteria are met. This will include but is not limited to:

- Validation of base assumptions before further design work is undertaken
- Identification of all areas requiring robust design provision
- Identification of all areas requiring process or task optimisation
- Definition and adoption of design requirements to satisfy criteria

The most significant FAPs relevant to the accident safety assessment are presented in Table 13.

Table 13 Forward Action Plan

FAP ID	FAP Description
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.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 DCTC 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 ID	FAP Description
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 LOOP 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.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

5 Conclusions

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

The 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 hazard control
- hazard management strategies that will need to be adopted to prevent or mitigate the consequences of radiation accidents.

The assessment at this stage of the GDF programme provides a means of signposting the significant issues which will be the priority for design development.

A systematic hazard identification, screening and fault grouping process has been completed for the functional processes and associated activities as defined in the PFD. This represents a significant improvement in the approach adopted to support the GDF programme. The representative set 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 or are relevant to the disposability advice being given now.

Following the identification of the representative fault set, fault sequence groups were identified for qualitative or quantitative assessment. DBAA was performed on those fault sequence groups identified for quantitative assessment and conceptual safety functions and safety functional requirements identified for the design basis faults. Illustrative safety measures have been identified which demonstrate that credible options are available to meet the risk reduction targets arising from the DBAA.

For the faults subject to qualitative analysis (internal and external hazards), it is demonstrated that the potential hazards are understood and appropriate hazard management strategies are defined and can be implemented. It is recognised that further work is required for internal hazards when the engineered safety measures and their structures, systems and components are determined.

An assessment of the design basis fault sequence groups has determined that there are no faults resulting in off-site doses to the public in excess of design basis thresholds.

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 to implement (with today's technology) and that the GDF will be safe to operate as a result. 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 issues 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 is 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. Areas that require further work to fully underpin the principal safety claim are largely related to design development and the resolution of the forward action plans.

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, *2016 Disposal System Safety Case (DSSC): Basis of Operational Assessment*, 2016.

5 Risktec, *HAZDOC Section II: Accident Safety*, RWM-04-R-09, Issue 3.0, 2016 (unpublished).

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

7 Radioactive Waste Management, *Radiological Protection Criteria Manual*, RWM02, Rev 2, 2015 (unpublished).

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

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

Glossary

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

Appendix A – Schedule of Faults Within HAZANs

OSC FSG ID	OSC FSG Name	Type of Safety Assessment Undertaken
HAZAN 1: Loss of Shielding		
1.A.6.2.1	Inadvertent exposure to elevated dose rates from package within SWTC returned to collection area in error	Numerical – initial DBAA
1.B.6.3.1	Inadvertent exposure to elevated dose rates from disposal unit present in error during maintenance of HLW/spent fuel deposition machine	
1.C.6.3.1	Inadvertent exposure to elevated dose rates from disposal unit present in error during maintenance of HLW/spent fuel holding facility	None – bounded by 1.B.6.3.1
1.D.6.2.1	Inadvertent exposure to elevated dose rates due to accessing SWTC (UILW) inlet cell facility when unshielded package present	Numerical – initial DBAA
1.E.6.3.1	Inadvertent exposure to elevated dose rates in DCTC receipt area due to HLW/spent fuel deposition operations commencing with shield door open	
1.E.6.2.1	Inadvertent exposure to elevated dose rates due to SWTC unloading operations commencing with staff adjacent with UILW inlet cell door open	
1.E.5.3.1	Inadvertent exposure to elevated dose rates due to DCTC unloading operations commencing with DCTC receipt area shield door open	
1.G.6.2.1	Inadvertent exposure to elevated dose rates due to leak of contaminated liquids in UILW vault	None
HAZAN 2: Spread of Contamination		
2.A.2.2.1	Inadvertent exposure to elevated RA in air due to disturbance of internal contamination in SWTC during maintenance operations.	None
2.B.6.2.1	Inadvertent exposure to elevated RA in air due to disturbance of contamination on vehicle/package on exit from UILW inlet cell	
2.C.6.1.1	Inadvertent exposure to elevated RA in air during maintenance SILW emplacement vehicle due to presence of internal contamination	
2.D.6.1.1	Inadvertent exposure to elevated RA in air due to disturbance of contamination on SILW emplacement vehicle on exit from SILW/LLW vault	

OSC FSG ID	OSC FSG Name	Type of Safety Assessment Undertaken
2.E.6.2.1	Inadvertent exposure to elevated RA in air due to disturbance of contamination on UILW vault lifting equipment during maintenance operations	
2.F.5.2.1	Inadvertent exposure to elevated RA in air due to disturbance of contamination during maintenance operations within UILW inlet cell	
2.F.6.1.1	Inadvertent exposure to elevated RA in air due to disturbance of accumulated contamination during emplacement operations in SILW/LLW vault	
HAZAN 3: Dropped Load (Loss of Shielding)		
3.A.4.1.1	Inadvertent exposure to elevated dose rates due to total loss of shielding following impact with SILW/LLW transport unit in shaft	Indicative consequence assessment - qualitative
3.A.4.2.1	Inadvertent exposure to elevated dose rates due to total loss of shielding following impact with SWTC (UILW) transport unit in shaft	
3.A.4.3.1	Inadvertent exposure to elevated dose rates due to total loss of shielding following impact with DCTC (HLW/spent fuel) transport unit in shaft	
3.B.6.1.1	Inadvertent exposure to elevated dose rates due to damage to disposal unit shielding following impact in SILW vault	Numerical – initial DBAA
3.C.6.3.1	Inadvertent exposure to elevated gamma dose rates due to loss of shielding following vehicle impact with HLW/spent fuel holding system	
3.D.6.3.1	Inadvertent exposure to elevated neutron dose rates due to loss of shielding following vehicle impact with HLW/spent fuel holding system	None
3.A.4.1.2, 3.A.4.2.2, 3.A.4.3.2	Inadvertent exposure to elevated dose rates due to damage to disposal unit shielding following impact during surface to sub-surface transfer in the drift	Indicative consequence assessment - qualitative
HAZAN 3: Dropped Load (Loss of Containment)		
3.E.4.1.1	Inadvertent exposure to elevated levels of RA in air due to total loss of containment following drop of SILW/LLW transport unit in shaft	Indicative consequence assessment - qualitative
3.E.4.2.1	Inadvertent exposure to elevated levels of RA in air due to total loss of containment following drop of SWTC (UILW) transport unit in shaft	
3.E.4.3.1	Inadvertent exposure to elevated levels of RA in air due to total loss of containment following drop of DCTC (HLW/spent fuel) transport unit in shaft	

OSC FSG ID	OSC FSG Name	Type of Safety Assessment Undertaken
3.F.6.1.1	Inadvertent exposure to elevated levels of RA in air due to loss of disposal unit containment following stack collapse within SILW/LLW vault	Numerical – initial DBAA
3.F.6.2.1	Inadvertent exposure to elevated levels of RA in air due to loss of disposal unit containment following stack collapse within UILW vault	Numerical – initial DBAA
3.E.4.1.2, 3.E.4.2.2, 3.E.4.3.2	Inadvertent exposure to elevated levels of RA in air due to loss of disposal unit containment following impact during surface to sub-surface transfer in the drift	Indicative consequence assessment - qualitative
HAZAN 4: Fire		
4.C.6.1.1	Inadvertent exposure to elevated levels of RA in air as a result of loss of containment due to emplacement vehicle fire impinging on SILW/LLW disposal unit within SILW/LLW vault	None
4.E.6.2.1	Inadvertent exposure to elevated levels of RA in air as a result of loss of containment due to lifting equipment fire impinging on UILW disposal units within UILW vault	
4.G.5.3.1	Inadvertent exposure to elevated dose rates due to loss of neutron shielding following a vehicle fire impinging on a DCTC within the HLW/SF Disposal Preparation Area	
4.G.6.3.1	Inadvertent exposure to elevated dose rates due to loss of neutron shielding following a deposition system (vehicle) fire in the HLW/SF Disposal Area	
HAZAN 5: External Hazards		
5.A.1.0.1	External (natural) event resulting in direct damage to vehicle at rail buffer park	Qualitative assessment
5.A.2.0.1	External (natural) event loading on WPTF resulting in structural failure	
5.A.2.0.2	External (man-made) event loading on WPTF resulting in structural failure	
5.A.3.0.1	External (natural) event loading on drift top building resulting in structural failure	
5.A.3.0.2	External (man-made) event loading on drift top building resulting in structural failure	
5.A.3.0.3	External (natural) event loading on shaft top building resulting in structural failure	
5.A.3.0.4	External (man-made) event loading on shaft top building resulting in structural failure	
5.B.4.0.1	Seismic event resulting in drift distortion or collapse	

OSC FSG ID	OSC FSG Name	Type of Safety Assessment Undertaken
5.B.4.0.2	Seismic event resulting in shaft distortion or collapse	
5.B.4.0.3	Seismic event resulting in derailment in drift	
5.C.5.0.1	Seismic event resulting in collapse of sub-surface tunnels during package transfers	
5.C.5.0.2	Seismic event resulting in distortion of remotely operated sub-surface railways	
5.C.5.0.3	Seismic event resulting in distortion of remotely operated sub-surface roadways	
5.C.5.3.1	Seismic event resulting in collapse of DCTC receipt and preparation area	
5.D.1.0.1	External (man-made) event resulting in fire at rail buffer park	
5.D.1.0.2	External (man-made) event resulting in fire at road buffer park	
5.D.2.0.1	External (man-made) event resulting in fire at WPTF	
5.D.3.0.1	External (man-made) event resulting in fire at drift top building	
5.D.3.0.2	External (man-made) event resulting in fire at shaft top building	
5.G.2.0.1	Seismic event resulting in dropped load during package lift in WPTF	
5.G.2.0.2	Seismic event resulting in structural failure and collapse of lifting equipment in WPTF	
5.H.4.0.1	Seismic event resulting in collapse of shaft lifting equipment during package movements	
5.I.5.3.1	Seismic event resulting in collapse of lifting equipment in disposal preparation area	
HAZAN 6: Internal Hazards		
6.A.2.0.1	On-site (internal man-made) explosion resulting in damage to rail buffer park infrastructure (caused by detonation of explosives during transit on surface).	Qualitative assessment
6.A.2.0.2	On-site (internal man-made) explosion resulting in damage to road buffer park infrastructure (caused by detonation of explosives during transit on surface).	
6.A.2.0.3	On-site (internal man-made) explosion resulting in damage to WPTF building structure and breach or collapse (caused by detonation of explosives during transit on surface).	

OSC FSG ID	OSC FSG Name	Type of Safety Assessment Undertaken
6.A.3.0.1	On-site (internal man-made) explosion resulting in damage to drift top building structure and breach or collapse (caused by detonation of explosives during transit on surface).	
6.A.3.0.2	On site (internal man-made) explosion resulting in damage to shaft top building structure and breach or collapse (caused by detonation of explosives during transit on surface).	
6.B.4.0.1	On site (internal man-made) explosion or fire within drift resulting in damage to structure and collapse	
6.C.5.3.1	On site (internal man-made) explosion or fire within HLW/SF Disposal Preparation Area resulting in damage to structure and collapse	
6.C.5.3.2	On site (internal man-made) explosion or fire within HLW/SF Disposal Preparation Area resulting in loss or isolation from ventilation extract	
6.C.6.1.1	On site (internal man-made) explosion or fire within SILW vault resulting in damage to structure and collapse	
6.C.6.1.2	On site (internal man-made) explosion or fire within SILW vault resulting in loss or isolation from ventilation extract	
6.C.6.2.1	On site (internal man-made) explosion or fire within UILW vault resulting in damage to structure and collapse	
6.C.6.2.2	On site (internal man-made) explosion or fire within UILW vault resulting in loss or isolation from ventilation extract	
6.C.6.3.1	On site (internal man-made) explosion or fire within HLW/SF Deposition Area resulting in damage to structure and collapse	
6.C.6.3.2	On site (internal man-made) explosion or fire within HLW/SF Deposition Area resulting in loss or isolation from ventilation extract	
6.L.6.1.1	Flooding within SILW vault resulting in loss of electrical supplies and loss or isolation from ventilation extract	
6.L.6.2.1	Flooding within UILW vault resulting in loss of electrical supplies and loss or isolation from ventilation extract	
6.L.6.3.1	Flooding within HLW/SF deposition area resulting in loss of electrical supplies and loss or isolation from ventilation extract	

Appendix B – Summary of Safety Analysis and Identification of Illustrative Risk Reduction Measures

Fault ID	1.A.6.2.1
Fault Description	Inadvertent exposure to elevated dose rates from package within SWTC returned to collection area in error
Initial Fault Class	C
Indicative Risk Reduction Target	3.2E-03
Conceptual Safety Function	Prevent/mitigate dose due to external radiation resulting from exposure to an unshielded waste package

Conceptual Safety Functional Requirement (CSFR)	Risk Reduction Hierarchy	Example Risk Reduction Measures (RRM)	Is the RRM Feasible?	Notes
Change the configuration of the returns process to remove the requirement for SWTCs to be returned.	Eliminate	No returns of SWTC, ie dispose of SWTCs in the vaults.	No	Not acceptable from an operational perspective as the waste consignor requires the SWTC to be returned. This option was considered at the inlet cell optioneering study and ruled out due to the expense associated disposing of SWTCs and not reusing them. The additional excavation would also result in additional costs and the GDF would potentially have to operate for a longer duration. In addition, emplacement of the waste package in a SWTC means that the SWTC becomes a SSC providing a nuclear safety function which would need to be substantiated.

Conceptual Safety Functional Requirement (CSFR)	Risk Reduction Hierarchy	Example Risk Reduction Measures (RRM)	Is the RRM Feasible?	Notes
Provide a means of preventing removal of a SWTC with a disposal unit still present.	Prevent	Removing the requirement to return the SWTC with lid refitted means that several means of inspection prior to dispatch could be used such as: • weighing the mass of the SWTC (for example with a load cell) • laser scanning to identify if a DU is present within the SWTC • radiation monitoring with an interlock system (see notes) • visual inspection via CCTV prior to dispatch	Yes	The specified engineered measures will be supported by an operator visually checking via CCTV that the DU has been removed from the SWTC. There could be an operational requirement to override the engineered safety measure (under strict managerial controls) if there is an out of specification DU within the shielded facility.
Provide a means of confirming that a disposal unit is present in the SWTC within the shielded facility.	Protect	Radiation monitoring of SWTC.	Yes	This could be difficult to achieve due to the background dose within the shielded facility and the low level of radioactive contamination present on the detectors.
Provide a means of detecting and alarming operators of elevated radiation levels within collection area.	Mitigate	Radiation monitoring and alarms assuming collection area is radiation controlled.	Yes	Duty system for normal operations but with additional high alarm settings.

Conceptual Safety Functional Requirement (CSFR)	Risk Reduction Hierarchy	Example Risk Reduction Measures (RRM)	Is the RRM Feasible?	Notes
Provide a means of tracking SWTCs & disposal units and their movement within the GDF.	Mitigate	Waste package configuration management system – providing a means of identifying the location of the DU within the GDF.	Yes	Waste package tracking in facilities is feasible and will be a requirement for certain waste packages. Nuclear material safeguards assurance system will be independent of this system.

Fault ID	1.D.6.2.1 1.E.6.2.1
Fault Description	Inadvertent exposure to elevated dose rates due to accessing SWTC (UILW) inlet cell facility when unshielded package present Inadvertent exposure to elevated dose rates due to SWTC unloading operations commencing with operators adjacent with UILW inlet cell door open
Initial Fault Class	C
Indicative Risk Reduction Target	3.2.E-04
Conceptual Safety Function	Protect operators from receiving a dose due to external radiation from exposure to an unshielded waste package

Conceptual Safety Functional Requirement (CSFR)	Risk Reduction Hierarchy	Example Risk Reduction Measures (RRM)	Is the RRM Feasible?	Notes
Remove the requirement to handle waste packages in an unshielded configuration below ground.	Eliminate	Process for removal of waste package from transport container provides an arrangement for direct interface of shielding systems.	Yes	Removal of waste package from transport container by attaching a contiguous shielding arrangement with gamma gate providing a fully shielded intermediate configuration of same performance as SWTC, to support subsequent transfer to a transit and handling flask (concrete box for handling) which removes need to handle unshielded unit at any time below ground, permits emplacement directly, provides shielding (aids recovery scenarios) and additional protection against dropped loads as well as partial backfilling. This would require a modification to the operating philosophy.

Conceptual Safety Functional Requirement (CSFR)	Risk Reduction Hierarchy	Example Risk Reduction Measures (RRM)	Is the RRM Feasible?	Notes
Provide a means of preventing access to the inlet cell when an unshielded package is present.	Prevent	Controlled access: interlock between shield doors and in-cell monitoring equipment such as radiation monitoring, load cell. Provide a visual indication such as CCTV and shielded viewing windows.	Yes	Current inlet cell concept design includes interlocking of shield door.
Provide a means of protecting the operators from external dose when inlet cell is in unshielded configuration.	Protect	Controlled access: radiation monitoring. Additional shield doors (double shield door arrangement). Shield labyrinth arrangement prior to shield door(s).	Yes	
Provide a means of mitigating the dose to operators from direct radiation from UILW operations with shield door open.	Mitigate	Radiation monitoring equipment and alarm to alert operators to increased radiation levels in the event of a fault condition with evacuation in event of high alarm.	Yes	This RRM is located outside of the inlet cell and therefore provides mitigation only. This system will act as a duty system with various alarm levels for normal operations as well as faults.

Fault ID	1.E.6.3.1
Fault Description	Inadvertent exposure to elevated dose rates in DCTC receipt area due to HLW/spent fuel deposition operations commencing with shield door open
Initial Fault Class	C
Indicative Risk Reduction Target	3.2E-03
Conceptual Safety Function	Prevent dose due to external radiation resulting from exposure to an unshielded waste package

Conceptual Safety Functional Requirement (CSFR)	Risk Reduction Hierarchy	Example Risk Reduction Measures (RRM)	Is the RRM Feasible?	Notes
Remove the requirement to operate disposal areas with disposal units in an unshielded configuration.	Eliminate	Sarcophagus pre-filled with bentonite with concrete overpack.	Yes	Provides shielding, fire and buffer performance requirements. Functionally similar in concept to HLW/spent fuel super containers.
Provide a means of preventing opening of the shield door with a HLW/spent fuel disposal unit present.	Prevent	Controlled access: interlock between shield doors and in-cell monitoring equipment such as radiation monitoring, load cell.	Yes	Current concept is HLW/spent fuel transfer hall, the DCTC is docked with the emplacement machine and the waste package is transferred as a fully remote operation.

Conceptual Safety Functional Requirement (CSFR)	Risk Reduction Hierarchy	Example Risk Reduction Measures (RRM)	Is the RRM Feasible?	Notes
Provide a means of protecting operators from direct radiation from HLW/spent fuel deposition operations with shield door open	Protect	Controlled access: interlock between shield doors and radiation monitoring. Additional shield doors (double shield door arrangement). Shield labyrinth arrangement prior to shield door. Provide a visual indication such as CCTV and shielded viewing window.	Yes	See controlled access: radiation monitoring.
Provide a means of protecting operators from direct radiation from unshielded package in facility/operator access to HLW/spent fuel deposition operations	Protect	Remote handling of DCTC, for example, shielded facility with shield doors as duty system. Controlled access: radiation monitoring	Yes	Providing an indication of increased radiation levels and signal to the shield door interlock to remain closed.
Provide a means of mitigating the dose to operators from direct radiation from HLW/spent fuel deposition operations with shield door open	Mitigate	Radiation monitoring equipment and alarm to alert operators to increased radiation levels in the event of a fault condition with evacuation in event of high alarm	Yes	This RRM is located outside of the transfer hall and therefore provides mitigation only. This system will act as a duty system with various alarm levels for normal operations as well as faults.

Fault ID	1.E.5.3.1
Fault Description	Inadvertent exposure to elevated dose rates due to DCTC unloading operations commencing with DCTC receipt area shield door open
Initial Fault Class	C
Indicative Risk Reduction Target	3.2E-03
Conceptual Safety Function	Prevent dose due to external radiation resulting from exposure to an unshielded waste package

Conceptual Safety Functional Requirement (CSFR)	Risk Reduction Hierarchy	Example Risk Reduction Measures (RRM)	Is the RRM Feasible?	Notes
Provide a means of preventing DCTC unloading operations taking place when receipt area facility is in unshielded configuration.	Prevent	Controlled access: interlock between shield doors and in-cell monitoring equipment such as radiation monitoring, load cell. Provide a visual indication such as CCTV and shielded viewing area for operations being undertaken within receipt area.	Yes	See controlled access: radiation monitoring. Current concept is HLW/spent fuel transfer hall, the DCTC is docked with the emplacement machine and the waste package is transferred as a fully remote operation.
Provide a means of protecting the operators from external dose during DCTC unloading operations taking place when receipt area facility is in unshielded configuration.	Protect	Controlled access: radiation monitoring Additional shield doors (double shield door arrangement). Shield labyrinth arrangement prior to shield door or double interlocked shield doors.	Yes	Providing an indication of increased radiation levels and signal to the shield door interlock to remain closed.

Conceptual Safety Functional Requirement (CSFR)	Risk Reduction Hierarchy	Example Risk Reduction Measures (RRM)	Is the RRM Feasible?	Notes
Provide a means of mitigating the dose to operators from direct radiation from DCTC unloading operations when receipt area facility is in unshielded configuration.	Mitigate	Radiation monitoring equipment and alarm to alert operators to increased radiation levels in the event of a fault condition with evacuation in event of high alarm.	Yes	This RRM is located outside of the receipt area and therefore provides mitigation only. This system will act as a duty system with various alarm levels for normal operations as well as faults.

Fault ID	3.A.4.1.1(SILW/LLW) 3.A.4.2.1 (SWTC-UILW) 3.A.4.3.1 (DCTC-HLW/spent fuel)
Fault Description	Inadvertent exposure to elevated dose rates due to total loss of shielding following impact with transport unit in the shaft
Initial Fault Class	N/A
Indicative Risk Reduction Target	N/A - although it is recognised that the indicative assessment calculates significant consequences and associated targets
Conceptual Safety Function	Prevent dose due to external radiation resulting from exposure to an unshielded waste package (illustrative only)

Conceptual Safety Functional Requirement (CSFR)	Risk Reduction Hierarchy	Example Risk Reduction Measures (RRM)	Is the RRM Feasible?	Notes
Eliminate the potential for an uncontrolled lowering of a waste package down a shaft.	Eliminate	Use of an alternative means of transporting the waste package from the surface to the sub-surface.	No	Not currently feasible as RWM wishes to retain shaft option.
Provide a means of preventing loss of load path integrity leading to comprised waste package shielding integrity.	Prevent	High reliability lifting arrangement and equipment preventing drop of a waste package.	Single system unlikely (taking account of all diverse and redundant measures within it) to meet all safety requirements - to be confirmed through FAP	Note, a high integrity nuclear lifting arrangement with specific safety measures to prevent a drop is likely provide a maximum probability of failure on demand of 1E-06.

Conceptual Safety Functional Requirement (CSFR)	Risk Reduction Hierarchy	Example Risk Reduction Measures (RRM)	Is the RRM Feasible?	Notes
Provide a means of preventing loss of waste package shielding integrity in the event of a drop or impact.	Prevent	Independent segregated operable load path capable of supporting the load such as an independent load follower or similar device. Minimise impact to less than the withstand capability of the waste package and transport unit such as staggered shaft (passive). Means of minimising impact damage to waste package and transport such as over-pack which prevents damage and/or contains the radiological inventory of the waste package. Means of dissipating energy to prevent structural failure of waste package – local measures such as cage with crush zones or shaft measures with crush zones or controlled means of deceleration.	To be confirmed through FAP	Means of minimising acceleration need to be explored such as air brakes or systems which maximise air resistance. Guided platforms provide an alternative means of arresting movement to braking systems via the wire rope load path. It is recognised that some waste packages will be transported to the sub-surface in transport containers made from high integrity materials that provide containment of radioactive materials and shielding even under surface transport accident conditions (severe impact and fire). However, the depth of the GDF shaft is at least 600m which is significantly greater that the IAEA regulatory requirements for the type B packages impact test which is a free drop of 9m.

Conceptual Safety Functional Requirement (CSFR)	Risk Reduction Hierarchy	Example Risk Reduction Measures (RRM)	Is the RRM Feasible?	Notes
Provide a means of preventing loss of waste package shielding integrity in the event of a drop or impact.	Prevent	Waste package and transport unit capable of withstanding accident worst case impact force without a release of radioactive material.	To be confirmed through FAP	Does not prevent the initiating event from occurring and is likely to result in significant damage to the shaft in the event that it does occur; note that there could be significant energy potential, for impact accident involving a waste package (65 tonnes gross).
Provide a means to protect operators from direct radiation exposure from failure of waste package shielding following a drop or impact.	Protect	Shield door(s) located at the base and top of the shaft to protect operators or members of the public in the event of a drop and loss of waste package shield integrity.	To be confirmed through FAP	Combined with operational requirement below (exclusion of personnel).
Provide a means to mitigate direct radiation exposure from failure of waste package shielding following a drop or impact.	Mitigate	Means of minimising impact damage to waste package and transport. Examples include ‘soft target’ such as shaft bottom arrestors. Exclusion of personnel from operational areas, for example, lowering of waste packages remotely. Radiation monitoring equipment and alarm to alert operators to increased radiation levels in the event of a fault condition and aid evacuation.	To be confirmed through FAP	-

Fault ID	3.E.4.1.1 (SILW/LLW) 3.E.4.2.1 (SWTC-UILW) 3.E.4.3.1 (DCTC-HLW/spent fuel)
Fault Description	Inadvertent exposure to elevated levels of radioactive material in air due to total loss of containment following drop of transport unit in shaft
Initial Fault Class	N/A - although it is recognised that the indicative assessment calculates significant consequences and associated targets
Indicative Risk Reduction Target	N/A - although it is recognised that the indicative assessment calculates significant consequences and associated targets
Conceptual Safety Function	Prevent/mitigate the release of radioactive material from a failed waste package

Conceptual Safety Functional Requirement (CSFR)	Risk Reduction Hierarchy	Example Risk Reduction Measures (RRM)	Is the RRM Feasible?	Notes
Eliminate the potential for an uncontrolled lowering of a waste package down a shaft.	Eliminate	Use of an alternative means of transporting the waste package from the surface to the sub-surface.	No	Not currently feasible as RWM wishes to retain shaft option.
Provide a means of preventing loss of load path integrity leading to comprised waste package containment integrity.	Prevent	High reliability lifting arrangement and equipment preventing drop of a waste package.	Single system unlikely (taking account of all diverse and redundant measures within it) to meet all safety requirements - to be confirmed through FAP	Note, a high integrity nuclear lifting arrangement with specific safety measures to prevent a drop is likely provide a maximum probability of failure on demand of 1E-06.

Conceptual Safety Functional Requirement (CSFR)	Risk Reduction Hierarchy	Example Risk Reduction Measures (RRM)	Is the RRM Feasible?	Notes
Provide a means of preventing loss of waste package containment integrity in the event of a drop or impact.	Prevent	Independent segregated operable load path capable of supporting the load such as an independent load follower or similar device. Minimise impact to less than the withstand capability of the waste package and transport unit such as staggered shaft (passive). Means of minimising impact damage to waste package and transport such as over-pack which prevents damage and/or contains the radiological inventory of the waste package. Means of dissipating energy to prevent structural failure of waste package – local measures such as cage with crush zones or shaft measures with crush zones or controlled means of deceleration.	To be confirmed through FAP	Means of minimising acceleration need to be explored such as air brakes or systems which maximise air resistance. Guided platforms provide an alternative means of arresting movement to braking systems via the wire rope load path. It is recognised that some waste packages will be transported to the sub-surface in transport containers made from high integrity materials that provide containment of radioactive materials and shielding even under surface transport accident conditions (severe impact and fire). However, the depth of the GDF shaft is at least 600m which is significantly greater that the IAEA regulatory requirements for the type B packages impact test which is a free drop of 9m.

Conceptual Safety Functional Requirement (CSFR)	Risk Reduction Hierarchy	Example Risk Reduction Measures (RRM)	Is the RRM Feasible?	Notes
Provide a means of preventing loss of waste package containment integrity in the event of a drop or impact.	Prevent	Waste package and transport unit capable of withstanding accident worst case impact force without a release of radioactive material.	To be confirmed through FAP	Does not prevent the initiating event from occurring and is likely to result in significant damage to the shaft in the event that it does occur. Note that there could be significant energy potential, for impact accident involving a waste package (65 tonnes gross).
Provide a means to protect operators from inhalation exposure from failure of waste package containment following a drop or impact.	Protect	Containment door(s) located at the base and top of the shaft to protect operators or members of the public in the event of a drop and loss of waste package integrity.	To be confirmed through FAP	Combined with operational requirement below (exclusion of personnel).
Provide a means to mitigate inhalation exposure from failure of waste package containment following a drop or impact.	Mitigate	Means of minimising impact damage to waste package and transport. Examples include 'soft target' such as shaft bottom arrestors. Exclusion of personnel from operational areas, for example, lowering of waste packages remotely. Radiation monitoring equipment and alarm to alert operators to increased radiation levels in the event of a fault condition and aid evacuation. Provision of ventilation systems.	To be confirmed through FAP	-

Fault ID	3.C.6.3.1
Fault Description	Inadvertent exposure to elevated gamma dose rates due to loss of shielding following vehicle impact with HLW/spent fuel holding system
Initial Fault Class	C
Indicative Risk Reduction Target	3.2E-03
Conceptual Safety Function	Prevent dose due to external radiation resulting from exposure to an unshielded waste package

Conceptual Safety Functional Requirement (CSFR)	Risk Reduction Hierarchy	Example Risk Reduction Measures (RRM)	Is the RRM Feasible?	Notes
Prevent potential for plant, machinery or vehicles entry into areas where vulnerable waste packages may be located.	Eliminate	Requires suitable engineered segregation systems to eliminate potential for any impacts.	To be confirmed through FAP	Linked to plant layout needs.
Prevent exposure due to external radiation resulting from waste package in unshielded configuration.	Prevent	Holding facility recessed in floor.	Yes	The RRM is in the illustrative concepts and with further analysis may prove to eliminate the fault by design.
Provide a means of mitigating the dose to operators from direct radiation from when waste package is in unshielded configuration.	Mitigate	Radiation monitoring equipment and alarm to alert operators to increased radiation levels in the event of a fault condition with evacuation in event of high alarm.	Yes	This system will act as a duty system with various alarm levels for normal operations as well as faults.

Fault ID	3.B.6.1.1
Fault Description	Inadvertent exposure to elevated dose rates due to damage to disposal unit shielding following impact in SILW vault
Initial Fault Class	C
Indicative Risk Reduction Target	3.20E-03
Conceptual Safety Function	Prevent dose due to external radiation resulting from exposure to an unshielded waste package

Conceptual Safety Functional Requirement (CSFR)	Risk Reduction Hierarchy	Example Risk Reduction Measures (RRM)	Is the RRM Feasible?	Notes
Provide a means of preventing the integrity of the disposal unit shielding from being compromised in the event of a drop or impact.	Prevent	Provide an external concrete structure or cover around the package for transfer and emplacement.	Yes	Provides waste package with a robust external barrier which permits emplacement directly, provides additional protection against dropped loads (damage to package), fire protections as well as possibly partial backfill component with high quality control.
Provide a means of preventing the integrity of the disposal unit shielding from being compromised in the event of a drop or impact.	Prevent	Amend emplacement strategy, for example, grouting material or by filling vault a level at a time, etc Disposal unit capable of withstanding maximum accident drop height/impact force. Limit lift height and impact force for waste packages to within its withstand capability.	To be confirmed through FAP	Lateral emplacement followed by backfilling by layer could remove need to lift or stack packages. Design reports currently show a range of stack heights between 2 and 6 waste packages height depending on waste type as stacking is matched to waste package withstand criteria in waste package specification.

Conceptual Safety Functional Requirement (CSFR)	Risk Reduction Hierarchy	Example Risk Reduction Measures (RRM)	Is the RRM Feasible?	Notes
Provide a means of protecting operators from direct radiation from disposal unit in vault.	Protect	Shield door(s) located at the vault entrance. Remote handling and emplacement.	Yes	-
Provide a means to mitigate direct radiation exposure from failure of disposal unit shielding.	Mitigate	Radiation monitoring and alarms assuming collection area is radiation controlled.	Yes	-

Fault ID	3.F.6.1.1
Fault Description	Inadvertent exposure to elevated levels of radioactive material in air due to loss of disposal unit containment following stack collapse within SILW/LLW vault
Initial Fault Class	B
Indicative Risk Reduction Target	3.2E-05
Conceptual Safety Function	Prevent/mitigate the release of radioactive material from a failed disposal unit

Conceptual Safety Functional Requirement (CSFR)	Risk Reduction Hierarchy	Example Risk Reduction Measures (RRM)	Is the RRM Feasible?	Notes
Eliminate the potential for stack collapse below ground.	Eliminate	Amend emplacement strategy, for example, filling by level at a time then backfilling and filling at next level, etc	Yes	Stacking of packages by layer means that all nuclear lifts would be only a few centimetres thereby preventing dropped loads capable of exceeding the withstand capacity of the package and then backfilling as soon as a layer is complete means that the next layer can be filled without the need to stack.
Provide a means of preventing the integrity of the disposal unit from being compromised in the event of a drop or impact.	Prevent	Disposal unit capable of withstanding maximum accident drop height/impact force.	To be confirmed through FAP	Credible max drop height 11m (SILW / LLW vault highest strength rock).

Conceptual Safety Functional Requirement (CSFR)	Risk Reduction Hierarchy	Example Risk Reduction Measures (RRM)	Is the RRM Feasible?	Notes
Provide a means of preventing loss of load path integrity leading to a drop of a disposal unit onto the stack causing collapse.	Prevent	High reliability lifting arrangement and equipment preventing drop of a disposal unit. Provision of positive engagement/guides or racks to ensure correct emplacement and provide further structural stability.	Single system unlikely (taking account of all diverse and redundant measures within it) to meet all safety requirements - to be confirmed through FAP	Note, a high integrity nuclear lifting arrangement with specific safety measures to prevent a drop is likely provide a maximum probability of failure on demand of 1E-06.
Provide a means of protecting operators from the impact of containment failure of a disposal unit in vault.	Protect	Remotely operated emplacement operations (operators excluded). Containment doors on access point to vault. CCTV cameras to aid emplacement activities.	Yes	-
Provide a means of mitigating inhalation exposures of operators following failure of disposal unit containment.	Mitigate	Radiation monitoring equipment and activity-in-air alarms to alert operators to increased radiation levels in the event of a fault condition. Provision of ventilation systems.	Yes	-

Fault ID	3.F.6.2.1
Fault Description	Inadvertent exposure to elevated levels of radioactive material in air due to loss of disposal unit containment following stack collapse within UILW vault
Initial Fault Class	B
Indicative Risk Reduction Target	3.2E-06
Conceptual Safety Function	Prevent/mitigate the release of radioactive material from a failed disposal unit

Conceptual Safety Functional Requirement (CSFR)	Risk Reduction Hierarchy	Example Risk Reduction Measures (RRM)	Is the RRM Feasible?	Notes
Eliminate the potential for stack collapse below ground.	Eliminate	Amend emplacement strategy, for example, filling by level at a time then backfilling and filling at next level, etc	Yes	Stacking of packages by layer means that all nuclear lifts would be only a few cm thereby preventing dropped loads capable of exceeding the withstand capacity of the package and then backfilling as soon as a layer is complete means that the next layer can be filled without the need to stack.
Eliminate the potential for stack collapse below ground.	Prevent	Removal of waste package from transport container at surface and providing an external concrete structure around the package for transfer underground and emplacement.	Yes	Provides waste package with a robust external barrier (concrete) which removes need to handle unprotected unit at any time below ground, permits emplacement directly, provides shielding and additional protection against dropped loads as well as partial backfilling.

Conceptual Safety Functional Requirement (CSFR)	Risk Reduction Hierarchy	Example Risk Reduction Measures (RRM)	Is the RRM Feasible?	Notes
Provide a means of preventing the integrity of the disposal unit from being compromised in the event of a drop or impact.	Prevent	Disposal unit capable of withstanding maximum accident drop height/impact force.	To be confirmed through FAP	Credible max drop height 8.7m (SILW / LLW vault highest strength rock).
Provide a means of preventing loss of load path integrity leading to a drop of a disposal unit onto the stack causing collapse.	Prevent	High reliability lifting arrangement and equipment preventing drop of a disposal unit. Provision of positive engagement/guides or racks to ensure correct emplacement and provide further structural stability.	Single system unlikely (taking account of all diverse and redundant measures within it) to meet all safety requirements - to be confirmed through FAP	Note, a high integrity nuclear lifting arrangement with specific safety measures to prevent a drop is likely provide a maximum probability of failure on demand of 1E-06.
Provide a means of protecting operators from the impact of containment failure of a disposal unit in vault.	Protect	Remotely operated emplacement operations (operators excluded). Containment doors on access point to vault. CCTV cameras to aid emplacement activities.	Yes	-
Provide a means of mitigating inhalation exposures of operators following failure of disposal unit containment.	Mitigate	Radiation monitoring equipment and activity-in-air alarms to alert operators to increased radiation levels in the event of a fault condition. Provision of ventilation systems.	Yes	-

Fault ID	3.A.4.1.2, 3.A.4.2.2, 3.A.4.3.2 3.E.4.1.2, 3.E.4.2.2, 3.E.4.3.2
Fault Description	Inadvertent exposure to elevated dose rates due to damage to disposal unit shielding during surface to sub-surface transfer in the drift Inadvertent exposure to elevated levels of radioactive material in air due to loss of disposal unit containment following impact during surface to sub-surface transfer in the drift
Initial Fault Class	N/A - although it is recognised that the indicative assessment calculates significant consequences and associated targets
Indicative Risk Reduction Target	N/A - although it is recognised that the indicative assessment calculates significant consequences and associated targets
Conceptual Safety Function	Prevent/mitigate the release of radioactive material from a failed package Prevent/mitigate dose due to external radiation resulting from exposure to an unshielded package

Conceptual Safety Functional Requirement (CSFR)	Risk Reduction Hierarchy	Example Risk Reduction Measures (RRM)	Is the RRM Feasible?	Notes
Eliminate potential for impact to the waste package from runaway locomotive in the drift.	Eliminate	Use another means such as shaft to transfer waste packages and disposal units underground.	No	This is not feasible based on the illustrative design and the operation of the shaft has risks which would not eliminate faults completely.
Provides a means of preventing an impact to the waste package from runaway locomotive in the drift.	Prevent	Multiple, diverse and independent rack and pinions. Multiple, diverse and independent braking system.	Yes	Current concept includes multiple fail safe braking systems with drift system having one track and single locomotive transfer unit in operation.

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