Preliminary Hazard Identification for the Mark II Conceptual Design

NWMO-TR-2016-02 **January 2016**

Heini Reijonen and Taina Karvonen

Saanio & Riekkola Oy

José Luis Cormenzana

Empresarios Agrupados Internacional, S.A.

nwmo
NUCLEAR WASTE MANAGEMENT ORGANIZATION
SOCIÉTÉ DE GESTION DES DÉCHETS NUCLÉAIRES

Nuclear Waste Management Organization
22 St. Clair Avenue East, 6th Floor
Toronto, Ontario
M4T 2S3
Canada

Tel: 416-934-9814
Web: www.nwmo.ca

Preliminary Hazard Identification for the Mark II Conceptual Design

NWMO-TR-2016-02

January 2016

Heini Reijonen and Taina Karvonen
Saanio & Riekkola Oy

José Luis Cormenzana
Empresarios Agrupados Internacional, S.A.

Document History

Title:	Preliminary Hazard Identification for the Mark II Conceptual Design		
Report Number:	NWMO-TR-2016-02		
Revision:	R000	Date:	January 2016
[1]Saanio & Riekkola Oy [2]Empresarios Agrupados Internacional, S.A.			
Authored by:	Heini Reijonen[1], Taina Karvonen[1] and José Luis Cormenzana[2]		
Verified by:	Pirjo Hellä[1] and Antti Ikonen[1]		
Approved by:	Timo Saanio[1]		
Nuclear Waste Management Organization			
Reviewed by:	Helen Leung and Neale Hunt		
Accepted by:	Paul Gierszewski		

ABSTRACT

Title: **Preliminary Hazard Identification for the Mark II Conceptual Design**
Report No.: **NWMO-TR-2016-02**
Author(s): Heini Reijonen [1], Taina Karvonen [1] and José Luis Cormenzana [2]
Company: [1] Saanio & Riekkola Oy
[2] Empresarios Agrupados Internacional, S.A.
Date: January 2016

Abstract
Operational safety is an important aspect of concept development. This report describes the methodology used and results obtained from a preliminary hazard identification assessment performed for Adaptive Phased Management (APM)'s Mark II conceptual design. Failure Modes and Effects Analysis has been used to identify potentially hazardous events and accident scenarios that could result in an increase in radiological consequence during the operating period. Internal and external initiating events were considered.

The identified failure modes were grouped into the following categories based on the anticipated initiating event frequencies:

- Anticipated Operational Occurrences (AOOs): Events with frequencies $> 10^{-2}$ a^{-1};
- Design Basis Accidents (DBAs): Events with frequencies $> 10^{-5}$ a^{-1} but $< 10^{-2}$ a^{-1};
- Beyond Design Basis Accidents (BDBAs): Events with frequencies $< 10^{-5}$ a^{-1} but $> 10^{-7}$ a^{-1}; and
- Non-credible Events: Event with frequencies $< 10^{-7}$ a^{-1}.

The estimation of initiating event frequencies is preliminary at this early design stage.

Based on this preliminary work, twenty-three AOOs, six DBAs, and four BDBAs have been identified, with most of these events resulting in extended outage periods at the Used Fuel Packaging Plant. Due to the high frequency of operations, the dropping of a module by the overhead transfer crane/gantry and the potential damage of fuel bundles during fuel transfer operations are identified in the AOO category.

The DBA category includes the failure and fall of an elevator during a used fuel transport package (UFTP) operation, the failure of the scissor lift resulting in the fall of a module/fuel bundles, a UFTP transport vehicle fire, a used fuel container (UFC) placement vehicle fire, the dropping of a UFTP containing an undetected flaw, and the dropping of an UFC containing an undetected flaw.

Shaft cage fall with an UFC, flooding of the repository facility, a major earthquake leading to repository cave-in, and repository collapse on the UFCs are all placed in the BDBA category.

The presence or absence of ventilation system filters is also considered in combination with specific accident scenarios.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Page

LIST OF ABBREVIATIONS

AGV	Automatic Guided Vehicle
ALARA	As Low As Reasonably Achievable
AOO	Anticipated Operational Occurrence
APM	Adaptive Phased Management
BDBA	Beyond Design Basis Accident
CANDU	CANada Deuterium Uranium
CNSC	Canadian Nuclear Safety Commission
DBA	Design Basis Accident
DGR	Deep Geological Repository
DOE	Department of Energy (U.S.)
EBS	Engineered Barrier System
FMEA	Failure Modes and Effects Analysis
HA	Hazard Assessment
HAZOP	Hazard and Operability Study
HEPA	High Efficiency Particulate Air
HLAW	Hybrid Laser Arc Welding
HLW	High Level Waste
ILW	Intermediate level Waste
LILW	Low and Intermediate Level Waste
LLW	Low Level Waste
LWR	Light Water Reactor
MLD	Master Logic Diagram
NBCC	National Building Code of Canada
NDA	Nuclear Decommissioning Authority (U.K.)

NEW	Nuclear Energy Worker
NWMO	Nuclear Waste Management Organization
OHN	Ontario Hydro Nuclear
OPG	Ontario Power Generation
OTC	Overhead Transfer Crane
PGRC	Phased Geological Repository Concept
PHA	Preliminary Hazard Assessment
PRA	Probabilistic Risk Assessment
PSA	Probabilistic Safety Assessment
RPN	Risk Probability Number
SKB	Svensk Kärnbränslehantering AB (Sweden)
TRU	Trans Uranic waste
UFC	Used Fuel Container
UFPP	Used Fuel Packaging Plant
UFTP	Used Fuel Transport Package
WIPP	Waste Isolation Pilot Plant (U.S.)

1. INTRODUCTION

1.1 BACKGROUND AND SCOPE

The Nuclear Waste Management Organization (NWMO) is implementing Adaptive Phased Management (APM), a program that has as its endpoint the centralized containment and isolation of Canada's used nuclear fuel in a deep geological repository (DGR). The APM repository design development and optimization program is currently advancing the reference design for a generic geology (crystalline or sedimentary rock).

This report documents a preliminary hazard identification performed for the Mark II conceptual design. The hazard identification considers both above ground and below ground operations. Internal and external initiating events are considered, and the resulting accident scenarios are sorted according to their anticipated frequencies of occurrence.

Conventional safety, transportation safety and malevolent actions, such as terrorism or acts of war, are outside the scope of this work.

1.2 REGULATORY CONTEXT

For the purpose of this study, regulatory guidance specified in Canadian Nuclear Safety Commission (CNSC) RD-310 (CNSC 2008) is adopted. In particular, Section 5.2.3 of RD-310 establishes frequencies for event classification in nuclear power stations as follows:

- Anticipated Operational Occurrences (AOOs): Events with frequencies > 10^{-2} a^{-1};
- Design Basis Accidents (DBAs): Events with frequencies > 10^{-5} a^{-1} but < 10^{-2} a^{-1}; and
- Beyond Design Basis Accidents (BDBAs): Events with frequencies < 10^{-5} a^{-1}.

In addition, a lower limit is set to be 10^{-7} a^{-1}, after which accidents are considered non-credible in this study.

2. METHODOLOGY IDENTIFICATION

2.1 LITERATURE REVIEW SUMMARY

To assist in the identification of events and applicable methodologies, a literature review has been conducted to identify the types of operational occurrences and accidents considered by organizations similar to the NWMO. The review considers the following reports, some of which also include radioactive waste types other than used nuclear fuel:

- OPG DGR for Low and Intermediate Level Waste (Chapter 7 of OPG 2011);
- Ontario Hydro Nuclear preclosure assessment of a conceptual system (OHN 1994);
- U.K. Nuclear Decommissioning Authority (NDA) generic operational safety assessment (NDA 2010, Areva 2012);
- U.S. Yucca Mountain Project (U.S. DOE 2009);
- U.S. Waste Isolation Pilot Plant (WIPP 2013, rev 4);
- Finnish used fuel disposal project by Posiva (Posiva 2013, Rossi and Suolanen 2013, Kukkola 2009, Rossi et al. 2009, Holmberg et al. 2012); and
- SKB, Sweden, SR-Operation (SKB 2010).

The results of the review are summarized in Table 1.

Table 1: Summary Table of the Relevance of the Reviewed Material

Reference	Relevant for Methodology Development	Includes Dose Results for Used Nuclear Fuel	Notes
OPG (2011)	Yes	No	Results are for low and intermediate level waste
OHN (1994)	Yes	Yes, used fuel analysed	- CANDU fuel - Relevant for crystalline environment (plutonic rock) - The design is outdated compared to the current one
NDA (2010)	Yes	Yes	Results are presented together for high level waste and used fuel
U.S. DOE (2009)	Yes	Yes	Used fuel and high level waste are analysed
U.S. WIPP (2013)	Yes	No	Results are for transuranic waste
Posiva (2013)	No; approach relies on national requirements.	Yes, used fuel analysed	Light water reactor fuel instead of CANDU fuel
SKB (2010)	No; several topics and stages are included that are excluded from NWMO's current work.	Yes, used fuel analysed	Light water reactor used fuel instead of CANDU

Most of the studies use a similar approach in the hazard identification process. In general, the methodologies reviewed are based on systematic handling of the hazardous events (and event chains) and are applicable for NWMO's preliminary hazard identification, despite the different waste types considered. For the APM project, there is primarily one waste type to consider; therefore, the waste categorisation process is simpler than in repositories that host various types of waste with variable radioactivity levels, such as Low Level Waste (LLW), Intermediate Level Waste (ILW), Transuranic waste (TRU), High Level Waste (HLW), and Used Fuel (UF).

Of note is that in some countries, such as Finland, the regulatory body provides very advanced and detailed guidance, and specifies a more straight forward approach in deterministic assessment of accident scenarios (STUK 2013a and b) than a detailed hazard identification process. This is only possible when the process is relatively well established and when regulations are quite concept specific.

Regarding the overall review results, there is variability in the waste types as well as the manner in which the site is accounted for (i.e., in some cases there is an actual site and in some cases a "generic" or a "reference" site is used). In the NWMO's case, the site has been defined by a hypothetical geology.

Most of the literature reviewed focusses on the Low and Intermediate Level (LILW) repositories or repositories with multiple radioactive waste types. Regarding NWMO's Mark II conceptual design, doses calculated for used fuel are of interest for further work. However, in general, direct comparison of the dose results from the safety assessments is problematic, as there are methodological differences among the analyses and significant differences in the parameter values as well as differences in design, site, and environment.

In general, dose results for LILW and high level wastes differ due to the variable inventories and waste package types, and the LILW wastes tend to dominate the results and pose higher risks than used fuel. Therefore, based on the reviewed literature, sensitivity parameters of the used fuel results cannot be derived from studies that compare variable waste types. The only sensitivity analysis done solely for CANDU fuel is OHN (1994). In this study, system parameters are varied to better understand the safety relevant components in the system.

The AOOs, DBAs and BDBAs identified in the reviewed reports are listed in Appendix A. It should be noted that terminology for scenarios, as well as probability limits, differ from study to study. For NWMO, terminology already in use has been adopted.

In the reviewed literature, both deterministic and probabilistic methods have been employed in the hazards assessments. A summary on these methodologies is provided in the Table 2 below.

Table 2: Methodologies Employed Within the Reviewed Literature

Report (or Operator)	Deterministic Methods	Probabilistic Methods	Comments
OPG (2011)	Identification of initiating events Establishing potential hazardous events and identification of consequences Identification and screening of accident scenarios Identification of bounding scenarios	-	The hazard identification process was based on a systematic review of relevant site and facility features and processes in order to identify credible accident scenarios that could lead to harm.
OHN (1994)	A subset of possible accident scenarios was considered by identifying the worst consequence scenario within each accident class	Sensitivity analysis	Design at a conceptual stage
NDA (2010)	Hazard and Operability Study (HAZOP) for Phased Geological Repository Concept for ILW and LLW in 1990 Hazard identification studies for UK HLW and UF reference Updates and reviews of similar facilities	Probabilistic safety assessment (ROSA toolkit)	At this stage, NDA does not have sufficiently detailed designs to develop comprehensive fault schedules.
U.S. DOE (2009)	Master Logic Diagram (MLD) HAZOP	-	The combination of the systematic, deductive logic of MLDs with the systematic and detailed inductive logic of HAZOP evaluations produces a comprehensive identification of internal initiating events, including equipment and human failure events.
U.S. WIPP (2013)	What-if Preliminary hazard assessment Failure Modes and Effects Analysis HAZOP	-	This combination of methods was selected based on its widespread use and DOE acceptance at other TRU waste handling/storage facilities in the DOE complex.
Posiva (2013)	Regulatory requirement based consideration of accidents	Probabilistic risk assessment (Holmberg et al. 2012)	Posiva's publications are: Kukkola 2009, Rossi et al. 2009 and Rossi and Suolanen 2013
SKB (2010)	Recognising risk possibilities in scenarios and dividing them into event groups, and then identifying possible results for the event groups (emission, effect on barrier, increase in doses for people)	-	SR-Operation, in Swedish.

2.2 METHODOLOGY DESCRIPTION

Hazard assessment methodology (Figure 1) is identified based on literature review and considering the need for NWMO's preliminary hazard identification for the Mark II conceptual design. The proposed methodology includes compilation of the disposal process steps and their logical screening to identify relevant accident scenarios that could lead to radiological consequences. The process steps for the conceptual design are based on the preliminary ALARA (as low as reasonably achievable) dose assessment of the Mark II concept (Reijonen et al. 2014). In this report, the process steps are modified slightly for the recent development in the UFPP design, and are included in Appendix B. The identified process step list, together with the conceptual design, is the starting point in the hazard/scenario identification.

The first step of the hazard identification is the identification of initiating events. The process steps are reviewed and screened for potential hazards or accidents, leading to a list of internal initiating events. (Internal initiating events are those internal to the process or operations and are generally associated with equipment failure and human actions). The methodology selected for the screening process should be comprehensive to allow for future iterations, as there are no specific Canadian regulations that identify the accident scenarios. Methodology employed should also be transparent and traceable, to allow systematic documentation that can be updated based on the future iterations in design and hazard assessments during the design development stage.

Failure Modes and Effects Analysis (FMEA) is selected to identify the internal initiating events based on the operation steps from the arrival of a Used Fuel Transport Package (UFTP) at the Used Fuel Packaging Plant (UFPP) to the end point of backfilling a deposition tunnel, drift and placement room. In FMEA, process steps are evaluated and potential hazards are detected based on team effort and expert judgement. The Hazard and Operability Study (HAZOP) method is also considered (see more details in Chapter 4). For each potential disturbance or hazard with identified potential to cause radiological consequences, the following properties are defined: severity, probability of occurrence, and detection. Based on these properties, a general Risk Probability Number (RPN) is calculated, against which the effects of the mitigating actions can be compared (for design iterations in the future). Further details are given in Section 4.1.1.

In internal initiating events, certain accident events are discussed separately from the FMEA process due to their nature of being only partially tied to operation steps. These accident events are identified, when appropriate, from literature findings for the Mark II conceptual design and are given below:

- Ventilation and filter system failure;
- Power failure;
- Shielding system failure;
- Criticality;
- Fire;
- Explosion;
- Inadvertent entry; and
- Flooding and leakages (water and gas).

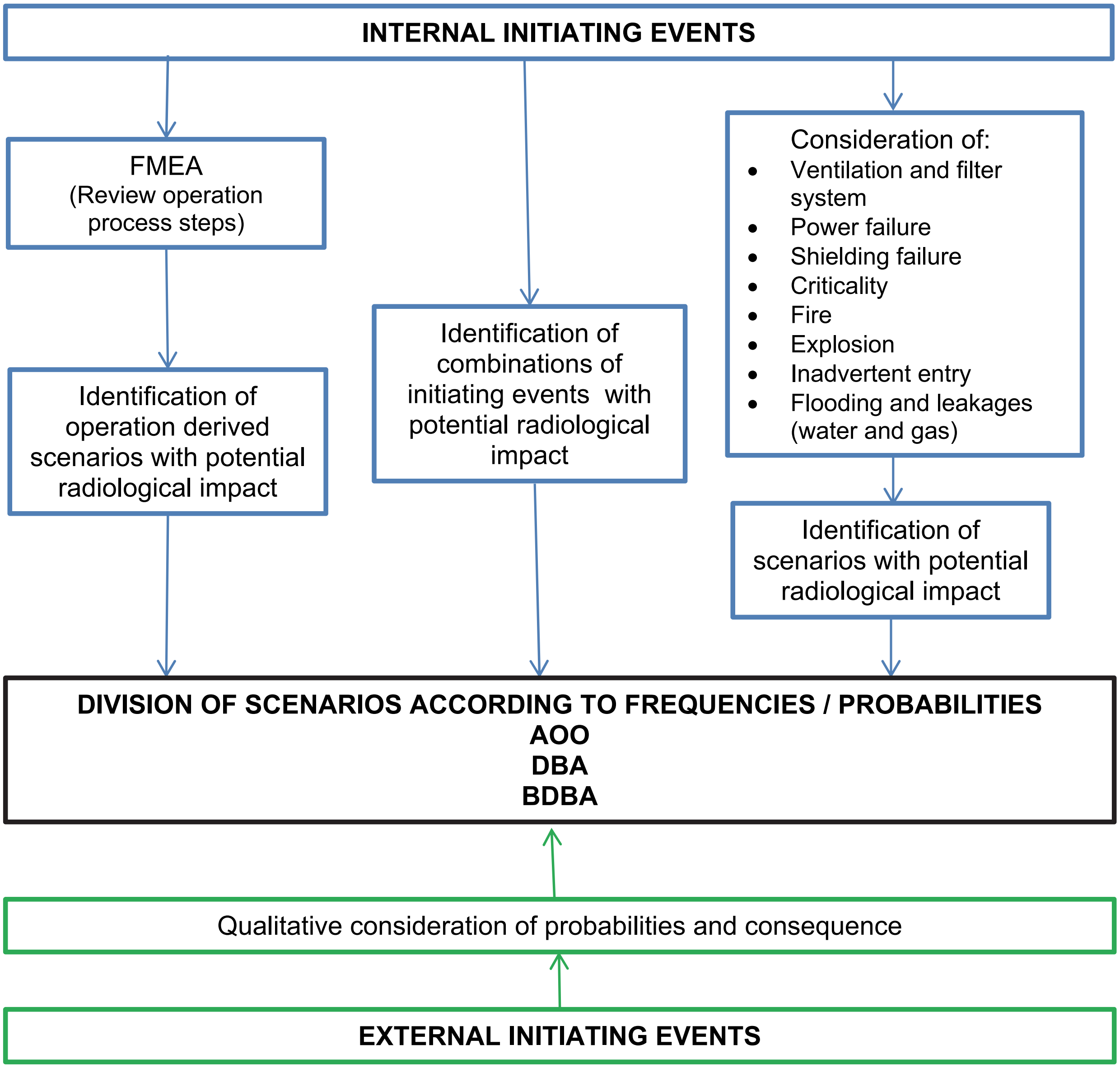


Figure 1: Methodology and Work Flow for Preliminary Hazard Identification

After identification of single failure modes with potential radiological impacts, combinations of initiating events that have common cause and could lead to additional worker exposure or radionuclide release are also defined. These event chains are defined based on the identified DBAs and BDBAs in the literature (Appendix A) as appropriate for the Mark II conceptual design. Event chains are also recognised from the conceptual design.

In the next step, external initiating events are then identified from earlier OPG work (OPG 2006a, 2006b, 2007 and OPG 2011). See Chapter 5 for initial list of the external initiating events. (The external initiating events are those that are external to the process or operations and include human-induced events as well as naturally occurring events).

Figure 2 shows the schematic on how the accident scenarios are identified. In general, the process begins with identification of initiating events, followed by determination of failure mode (i.e., where and how the failure mode could occur?). Failure mode may be detailed and a cause of the failure is postulated (i.e., what causes the failure?). From these, an accident scenario with a radiological consequence is formulated. If failure modes have similar frequency and consequence, they can be binned as only one accident scenario. At the end of this report identified accident scenarios are divided according to frequencies as AOOs, DBAs or BDBAs.

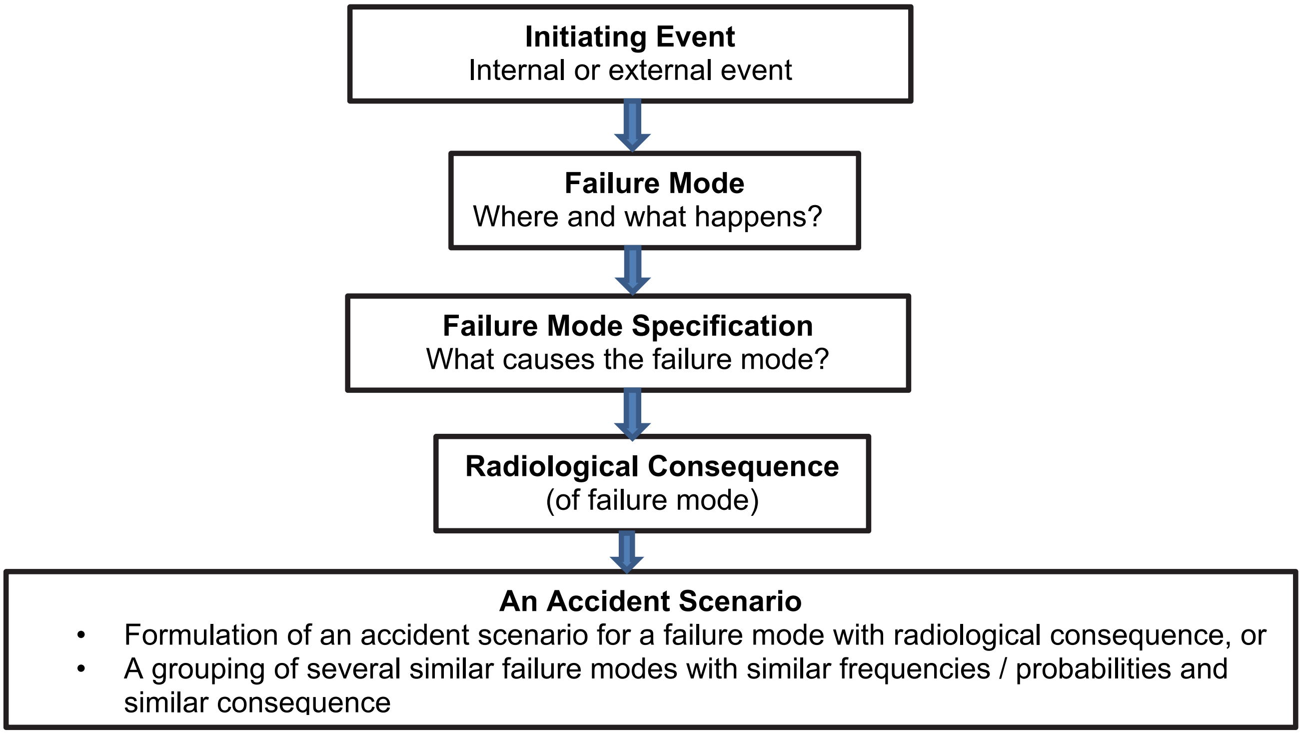


Figure 2: Schematic of Scenario Identification Process

An identification name is assigned to each individual failure mode. An individual failure mode can become an accident scenario on its own, but several failure modes can also be grouped as one accident scenario. In both cases, a linear number is given for accident scenarios, which is introduced in the summary of both internal and external initiating events (Sections 4.11 and 5.14).

In failure mode identification, the following abbreviations are used:

II	Mark II conceptual design
FMEA 1.1	FMEA derived failure mode, from process step 1, and the first postulated failure mode
Fire	Fire occurrence
IE	Inadvertent entry
DF	Drop/Failure, referring to combined occurrence of dropping a package that is flawed
EC	Event Chain
Flood	Flooding (or leaking of water or gas) incident

3. MARK II CONCEPTUAL DESIGN DESCRIPTION

3.1 GENERAL DESCRIPTION

The APM facility consists of various surface handling facilities and an underground repository. The underground repository is located approximately 500 m underground in a hypothetical generic geology - sparsely fractured crystalline rock or low-permeability sedimentary rock (Heystee 2015). The surface facilities include a UFPP, which receives used fuel from interim storage locations and re-packages it into long-lived containers for placement in the repository. The Mark II container is a copper-coated container handling 48 used fuel bundles. The Mark II engineered barrier system (EBS) is illustrated in Figure 3.

The number of Used Fuel Transport Packages (UFTP) arriving at the UFPP is assumed to be 630 package per year. The annual throughput of the UFPP is therefore 1,260 used fuel modules, 120,960 used fuel bundles, and 2,520 used fuel containers (UFCs). The main processes within the UFPP are listed in Table 3.

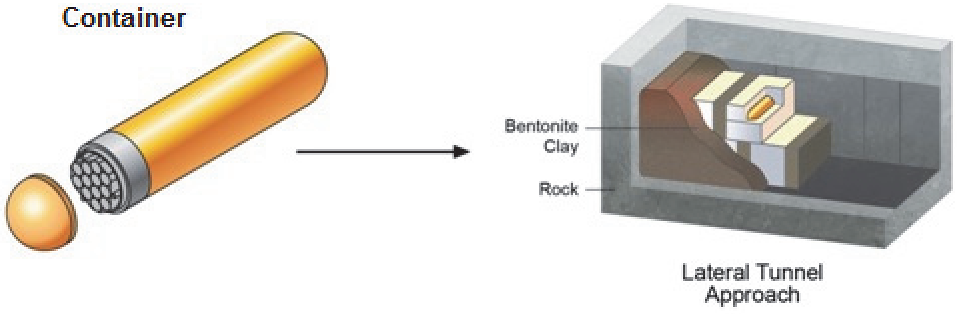


Figure 3: Schematic Illustration of the Mark II EBS

Table 3: Main UFPP Processes for the Mark II EBS

1. Pre-assembled empty UFC receipt	8. Machine closure weld
2. UFTP receipt at UFPP	9. Inspection
3. Unloading of used fuel modules from UFTP	10. Cold spray copper
4. Fuel transfer from module to basket	11. Machine applied copper coating
5. Steel lid installation	12. Copper coating inspection
6. Pre-heat	13. Stage in preparation for buffer box
7. Closure weld steel lid	14. Buffer box assembly

3.2 DESCRIPTION OF DISPOSAL PROCESS

3.2.1 Used Fuel Packages

Used fuel to be disposed in the planned DGR is CANada Deuterium Uranium- **CANDU fuel** (Figure 4) that uses natural uranium. Canadian used fuel consists primarily of used CANDU fuel, which is generated at commercial nuclear power reactors in Ontario, Québec and New Brunswick. In addition, there are very small quantities of used fuel from research and isotope-producing reactors in Canada.

Figure 4: A CANDU Fuel Bundle

A CANDU **fuel bundle** consists of 28 to 37 elements containing uranium pellets. The fuel sheath is manufactured from Zircaloy 4, a zirconium metal alloy. Once filled with uranium pellets, the sheathing material is sealed at both ends with zircaloy plugs and welded together into a cylindrical matrix with plates at each end. A typical CANDU fuel bundle is shown in Figure 4. Each fuel bundle is approximately 500 mm long, 102 mm in diameter and weighs about 24 kg.

Modules are rectangular rack systems used for storing used fuel bundles at interim storage locations and when transporting and transferring the used fuel bundles into the UFPP from the nuclear power plant. A module contains 96 used fuel bundles (Figure 5). After use, the modules are decontaminated, compacted and shipped to off-site metal recycling facility or to a storage location for future reuse (Heystee 2015).

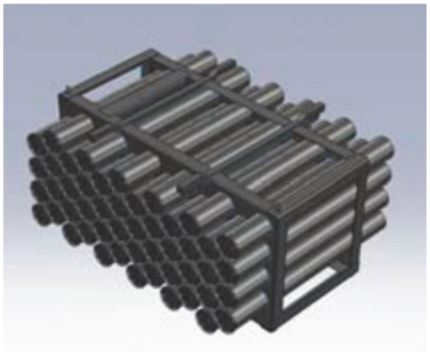


Figure 5: Module for 96 Used Fuel Bundles

Used Fuel Transport Packages (**UFTP**, Figure 6) are used for transporting used fuel from the nuclear power plant interim storages sites to the UFPP. Two modules fit in one UFTP. The UFTP is closed by a lid that is bolted on the container. On top, there is an impact limiter that is attached to the UFTP during transportation and removed at UFTP storage in the UFPP. When filled with used fuel, a transport cask weighs approximately 35 tonnes.

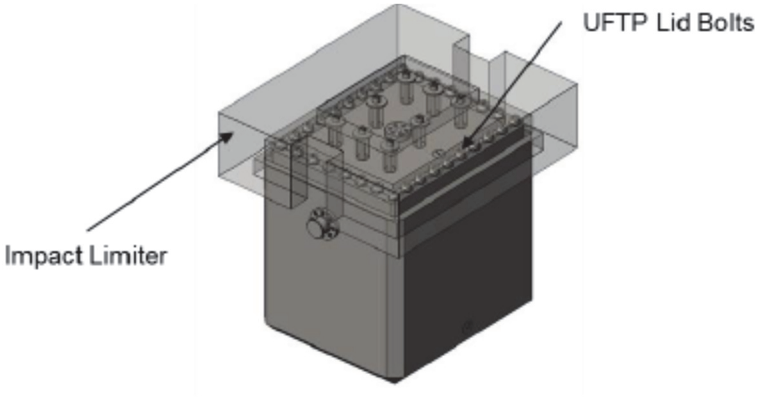


Figure 6: UFTP Shown with Impact Limiter

In the UFPP, the used fuel bundles are transferred to a **Used Fuel Container** (**UFC**), in which the used fuel will be placed in the DGR (Figure 3). The Mark II UFC is small containing 48 used CANDU fuel bundles and has semi-circular heads. The weight of the container loaded with used fuel is 2,795 kg.

3.2.2 Lifting and Transfer Equipment

At the UFPP, overhead transfer cranes (OTCs) or overhead transfer gantries are used to lift packages (UFTPs, modules, empty UFCs, and loaded UFCs) from one location to another.

An elevator (with open top) is used to lift the UFTP in the UFTP vent cell from the basement to the ground level in the module handling cell and to return the empty UFTP to the basement.

A positioning table (with scissor lift) is used to align the tubes holding the used fuel bundles in a module vertically and horizontally with the basket in an empty UFC in the fuel handling cell (Figure 7). A similar positioning table is used to position the basket in the empty UFC.

There are various vehicles (e.g., transfer pallets for UFTPs in the UFTP shipping and receiving area, inter-airlock trolleys for modules in the module cells, flask trolleys for UFC in processing and decontamination cells) for transfer of packages from one area to another.

The Transfer Flask, a shielded container, is used to move the loaded UFC on the flask trolley to the welding, copper application and decontamination cells in the transfer hall within the UFPP (Figure 8). Trolley movement is controlled via a customised Automatic Guided Vehicle (AGV) system (Figure 9).

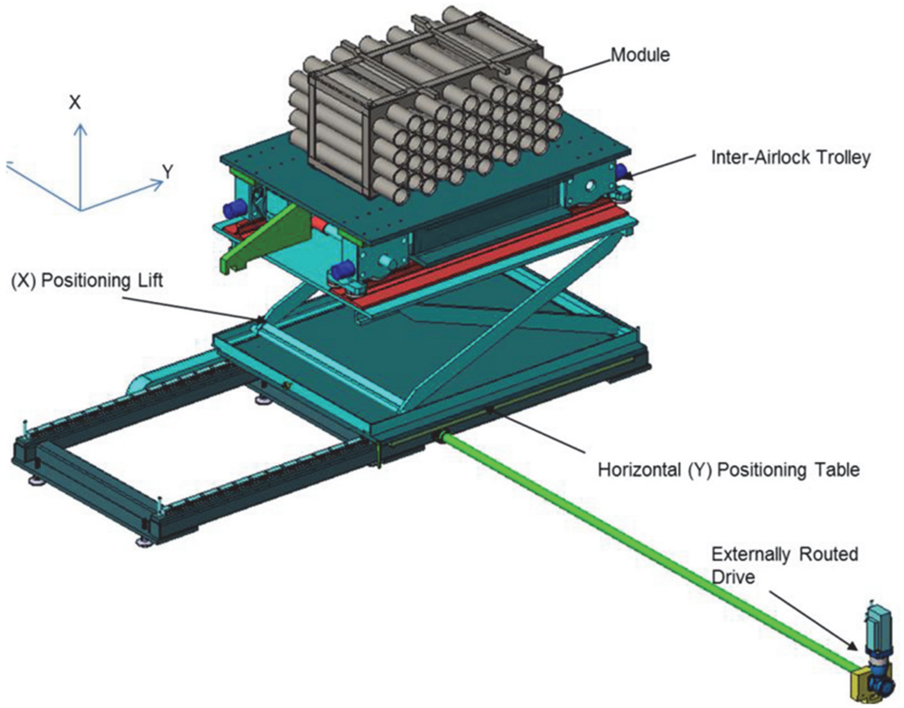


Figure 7: Module Trolley and Positioning Table with Scissor Lift

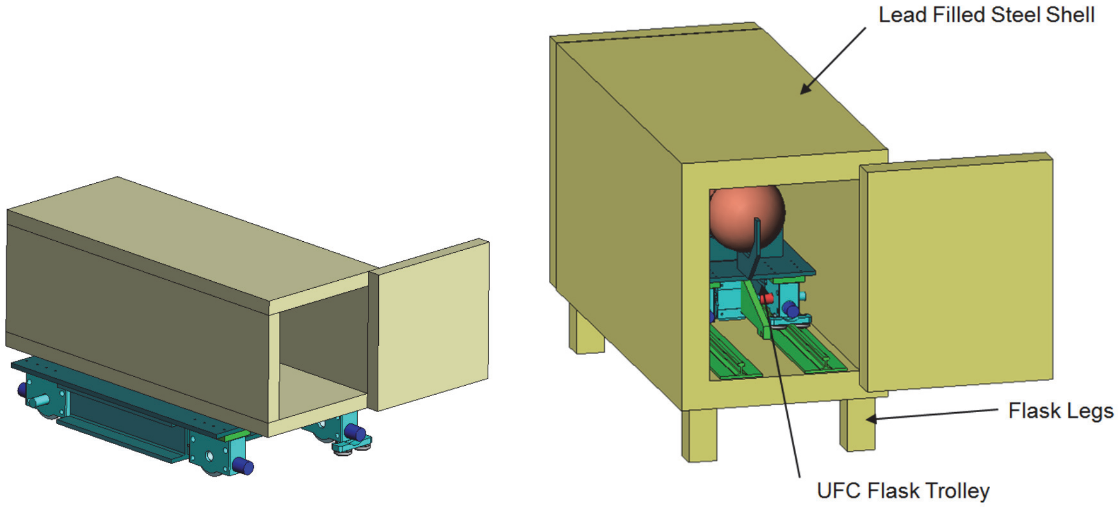


Figure 8: Shielded Transfer Flask on AGV for UFC Transfer in UFPP (Left) and Transfer Flask Showing UFC on Flask Trolley (Right)

Figure 9: Example Low Profile AGV Transporter- 50 Ton Cap

When the UFC is completed, it is enclosed within blocks of highly compacted bentonite to form a buffer box that is moved inside a transport cask (shielded container) which is then towed to the shaft and ultimately to a placement room underground (Figure 10). The buffer box is transferred from the transport cask to a placement vehicle (forklift), through a shielding canopy at the entrance of the placement room. The shielding canopy serves to aid the transfer of the bentonite buffer box out of the transport cask onto the placement forklift. The placement forklift is used to place the buffer box remotely in its final location in the placement room (Figure 10).

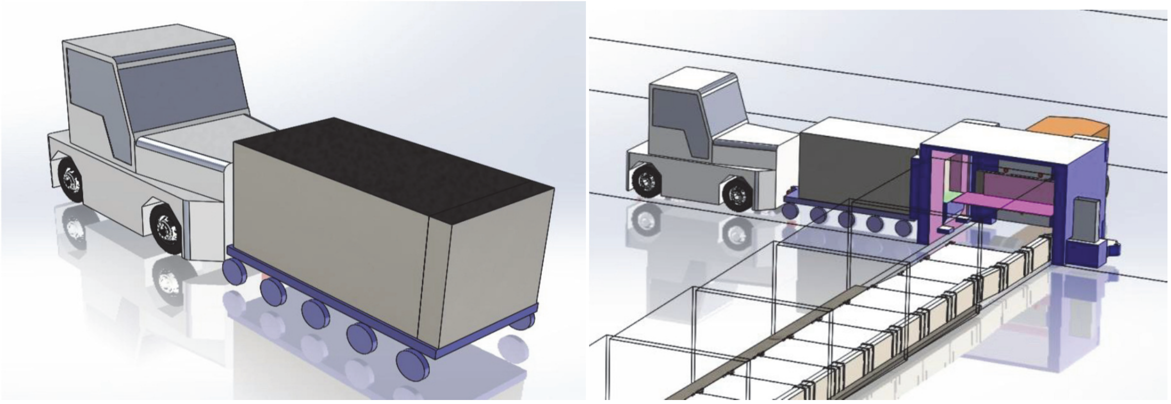


Figure 10: Transport Cask with Tow Vehicle

3.2.3 Process Descriptions for the Mark II EBS

3.2.3.1 UFPP Activities

The Mark II EBS is currently in the development stage. The following description is based on information available at the time of this assessment.

The Mark II UFC consists of several components. The basic terminology and relationship among these components is illustrated in Figure 11.

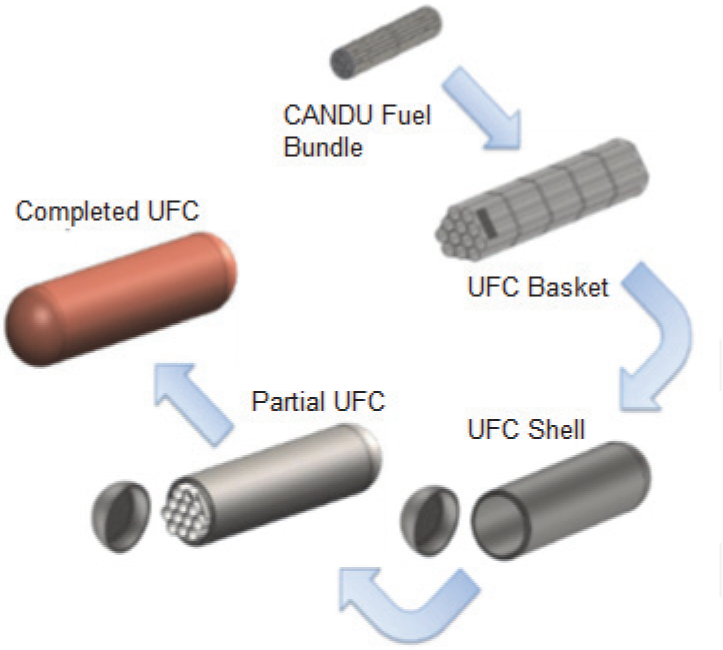
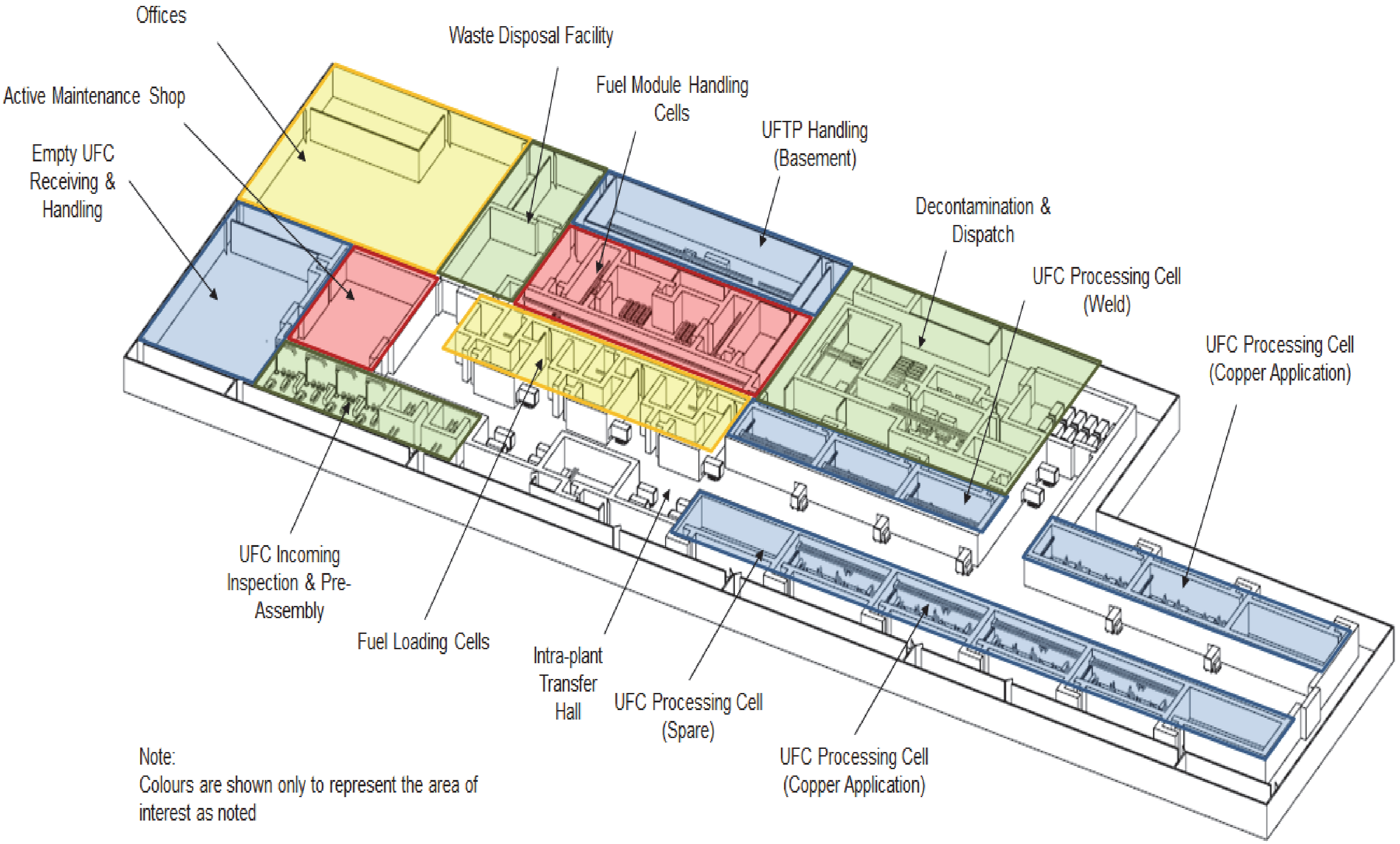


Figure 11: UFC Components and Terminology for the Mark II Conceptual Design

The UFPP construction is planned as a ground level building to accommodate the material process flows, with a small basement level to accommodate UFTP handling and UFC dispatch operations. The ground floor of the UFPP is approximately 88 x 254 meters. Each floor (ground level building and basement) is approximately 5 m high. Figure 12 illustrates the UFPP layout. A detailed layout is shown in Appendix B.



Note:
Colours are shown only to represent the area of interest as noted

Figure 12: UFPP Layout Illustration

Figure 13 shows the UFPP process flow with the proposed radiation zones. In the following sections, the processes within the UFPP and DGR are described. The full list of process steps is given in Appendix B.

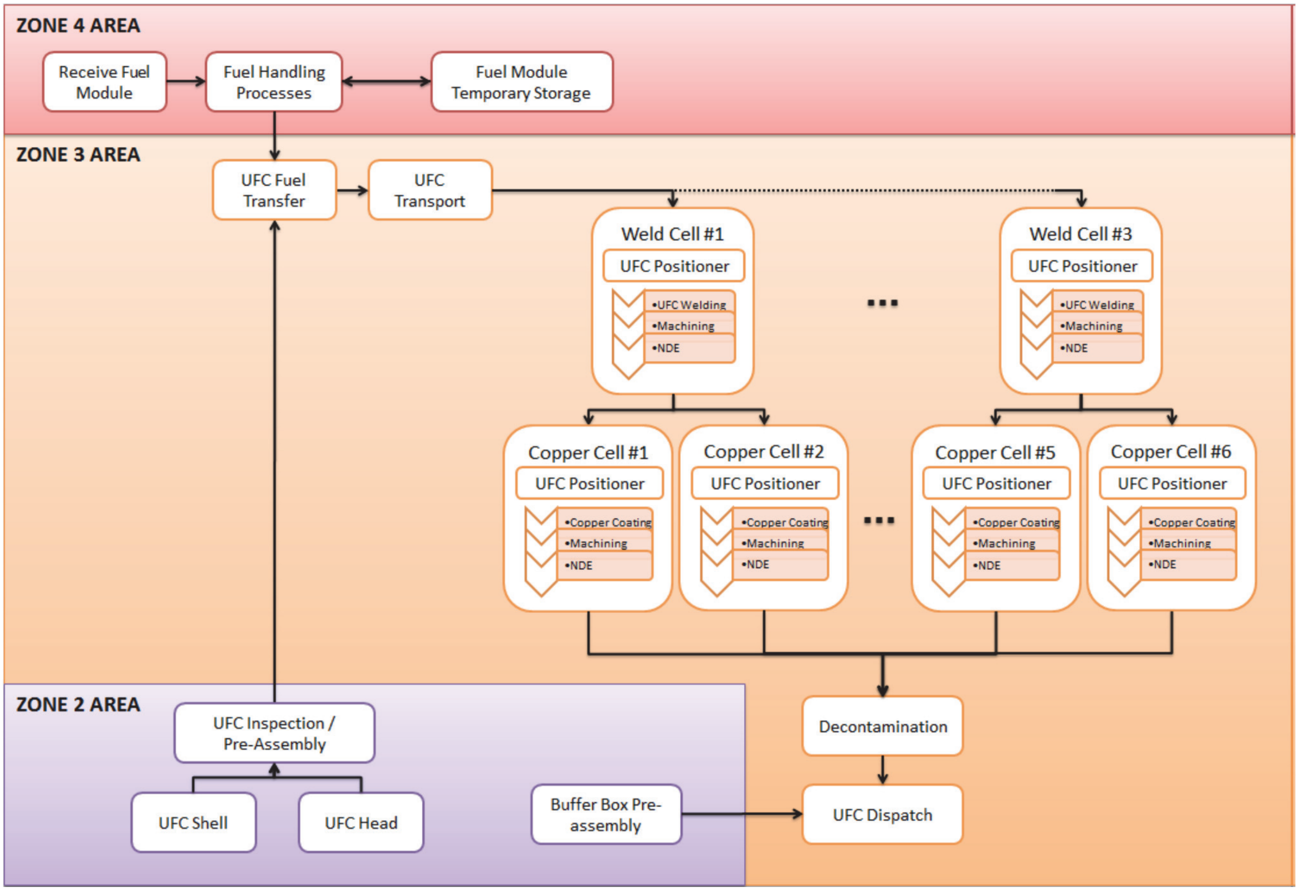


Figure 13: UFPP Process Flow

There are two UFTP handling cells, two module handling cells, three fuel handling cells, three welding cells, six copper application cells, and two UFC decontamination and dispatch cells. All the cells except the UFTP handling cells and dispatch hall are on the same ground level. Each of the cells required for UFTP handling, module handling, fuel handling, processing (weld and copper application), and decontamination and dispatch is isolated from one another with airlocks and shielding walls. The hot cell areas are shielded by 100 cm-thick concrete shielding walls with lead glass windows, and CCTV cameras for remote viewing. A Master Slave Manipulator permits access to all areas within the cell for potential fault recovery and maintenance operations. Active ventilation is maintained to prevent contaminated airflow to connecting cells.

The UFPP is divided in four zones according to ambient radiation and access control (Table 4).

Table 4: Radiological Classification of Disposal Facility Areas

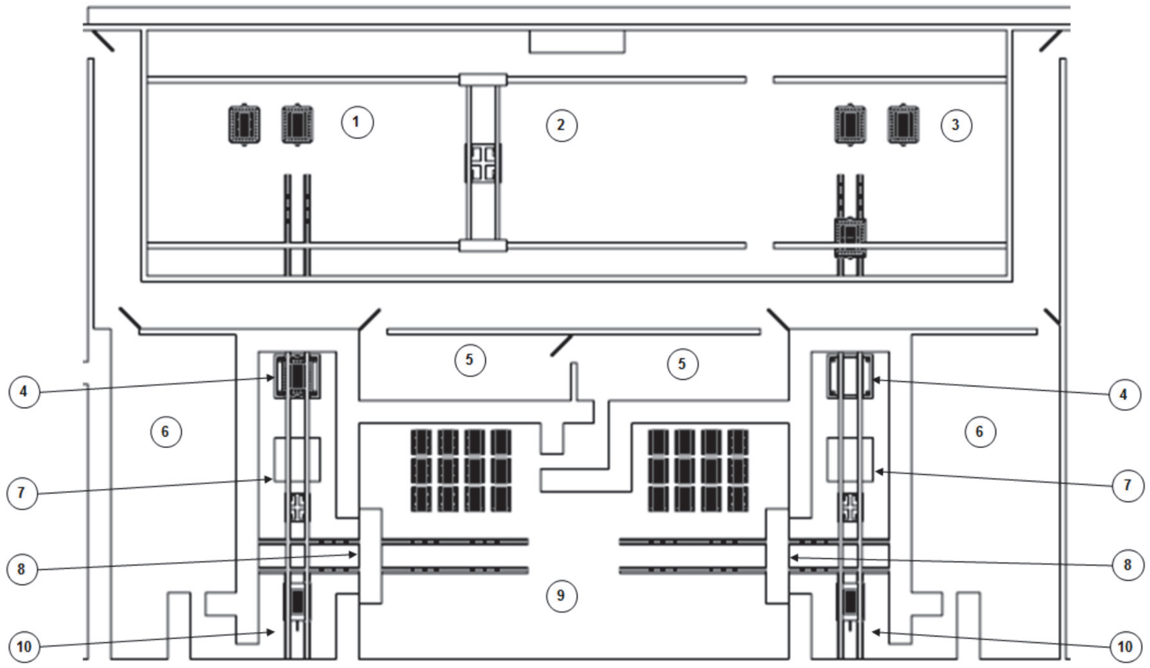
Zone	Potential for Internal Contamination	Access Status
1	No potential for contamination.	Entry is allowed to all staff. Access area to members of public.
2	Potential for contamination. Contamination is not tolerated and is eliminated once discovered.	Work zone for Nuclear Energy Workers (NEWs) only.
3	Contaminated area. Contamination levels are less than certain quantified levels*.	Controlled access. Protective clothing is required.
4	High levels of contamination. Levels are higher than certain quantified levels*.	Normally inaccessible area. Special protective clothing and equipment is required. Special equipment should also be provided for handling fuel bundle separation accident or for decontamination purposes in the UFPP.

*Not quantified in this report.

3.2.3.1.1 Used Fuel Module Receipt from Incoming UFTP

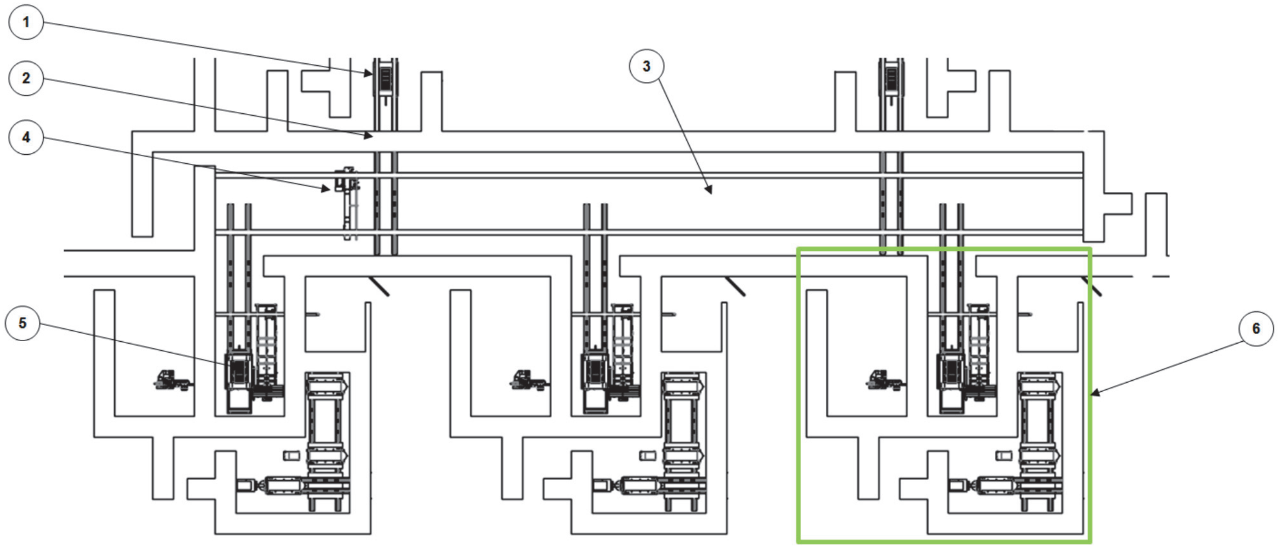
From the interim storage locations, a UFTP arrives at the UFPP shipping and receiving area located in the basement level of the plant (Figure 14). The UFTP is removed from the transport trailer using an overhead transfer crane (OTC) and placed onto a transfer pallet and, through an airlock, moved to either a dedicated storage space or directly to one of the two UFTP handling cells.

Prior to entering the handling cells, the impact limiter is removed manually with the assistance of the OTC. The UFTP on the pallet is then transferred through an airlock into the UFTP vent cell, where the lid bolts are removed by a Master Slave Manipulator. It is lifted via an elevator (open top) vertically from the basement to the ground level to one of the two module handling cells, where the UFTP lid is removed by an OTC. Each fuel module (two in one UFTP) is then retracted by the OTC to either a temporary dry storage area or to a laydown area in the module handling cell. The dry storage area can accommodate up to 24 modules during operation (Figure 14). From the laydown area, the module is retracted by the OTC onto an inter-airlock trolley and moved through the common module distribution hall to one of the three fuel handling cells (Figure 15).



1. UFTP Storage Area (Basement)
2. UFTP Shipping and Receiving Hall (Basement)
3. Impact Limiter Removal Area (Basement)
4. UFTP Vent and Transfer Cell
5. Control Room
6. Operator Room
7. Module Drying Cell
8. Module Transfer to Dry Storage
9. Dry Storage Area
10. Module Transfer to Distribution Hall

Figure 14: UFTP Receiving and Module Handling (Ground Level)



1. Module Distribution Inter-airlock Trolley
2. Airlock
3. Module Distribution Hall
4. Module Distribution Hall OTC
5. Fuel Loading Inter-airlock Trolley
6. Fuel Handling Cell (x3)

Figure 15: Module Handling and Fuel Handling Cells (Ground Level)

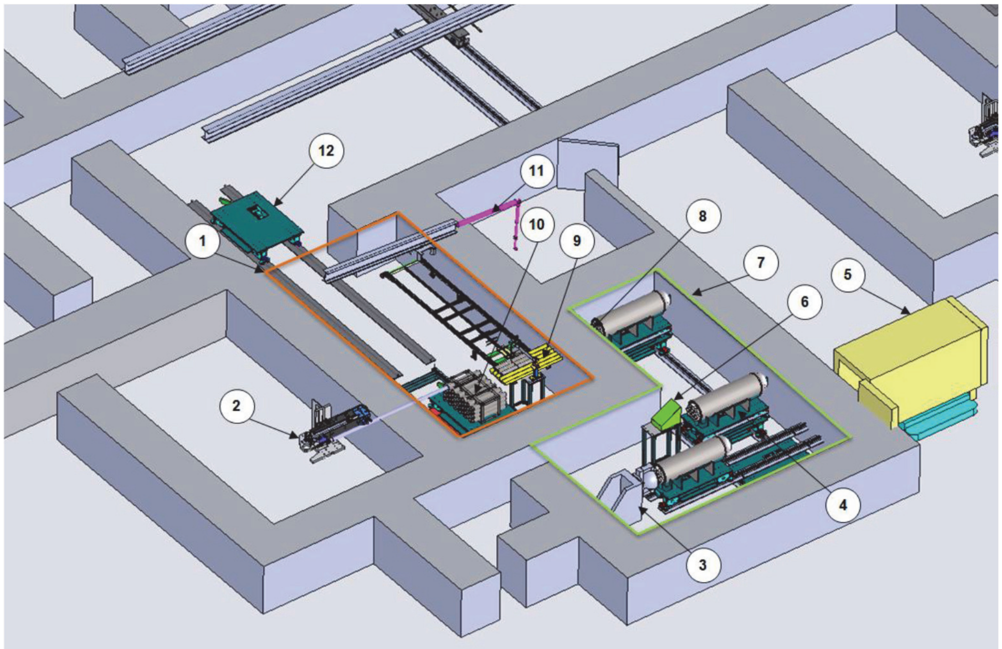
3.2.3.1.2 Empty UFC and Fuel Handling Cell Activities

On the ground floor, an empty UFC on a flask trolley in a transfer flask (Figure 8) is moved by an AGV (Figure 9) to one of the three UFC fuel handling cells (Figure 15). The empty UFC on the flask trolley is extracted from the transfer flask to the handling cell, where the hemispherical head is removed. The empty UFC is then transferred to the UFC trolley positioning worktable for aligning the location of the empty UFC Basket tubes with the fuel push tooling (See Figure 16).

Once aligned, the empty UFC is advanced to the transfer port and shroud position. An awaiting module on the trolley is advanced onto the module positioning worktable in the fuel handling cell, where the used fuel bundles are inspected and pushed two at a time into the basket tube in the empty UFC until the basket is filled. Each module contains 96 used fuel bundles and each basket contains 48 used fuel bundles. The basket has 12 tubes that host 4 bundles each.

After filling the basket, the hemispherical head is reinstalled. The loaded UFC on the flask trolley is returned to the UFC transfer cell and retracted back to the transfer flask. It is then moved via UFC transfer hall to the UFC processing cell.

To achieve the specified maximum daily throughput, a total of 12 UFC baskets will be loaded per day, which corresponds to 6 modules. To accomplish this, three parallel and independent processing lines are planned, with each line processing an average of two modules and four UFC baskets per day.



1. Fuel Handling Cell
2. Fuel Push Ram
3. UFC Head Removal and Re-attach
4. UFC Trolley Positioning Table
5. AGV with UFC Transfer Flask
6. UFC Vision System for Basket Position
7. UFC Fuel Loading Cell
8. Transfer Port and Shroud
9. Bundle Inspection Table and Vision System
10. Fuel Module Positioning Table
11. Defect Bundle Handling Area and Tele-manipulator Re-work / Reject Station
12. Inter Airlock Trolley

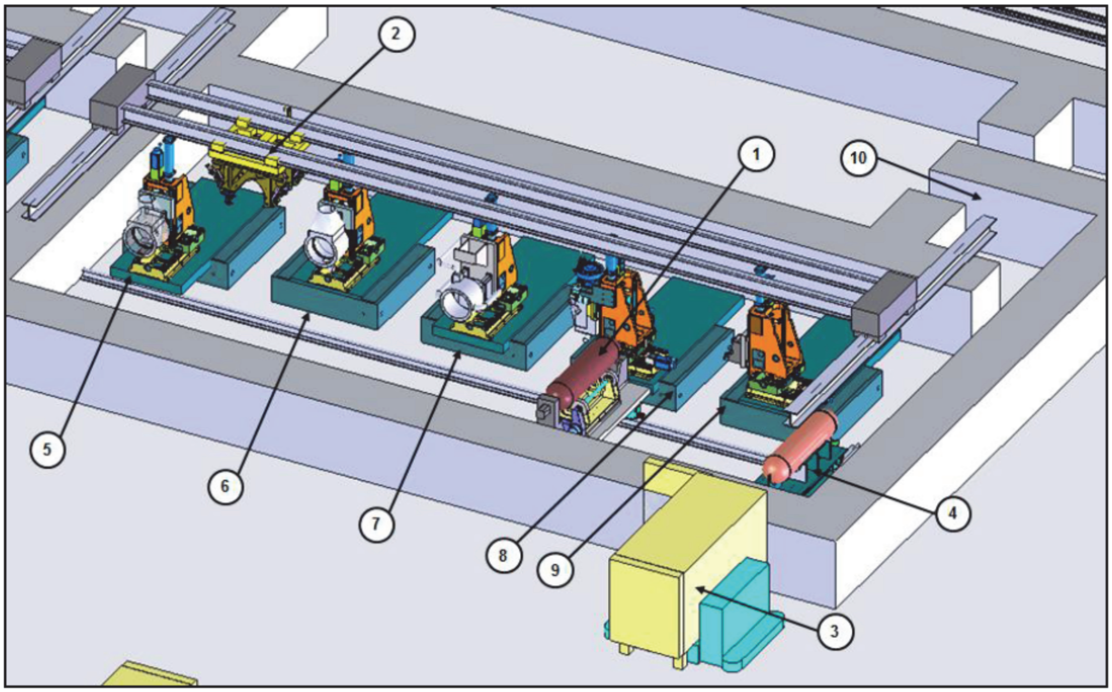
Figure 16: Fuel Handling System Components (Ground Level)

3.2.3.1.3 UFC Processing Cell Activities

Now in its transfer flask, the UFC on its flask trolley is moved to the processing cell entrance (Figure 17), where it is retracted from the transfer flask and inserted by an OTC onto a UFC rotary positioned for processing in one of the three weld cells (Figure 17). The facility has three welding cells and six copper application cells.

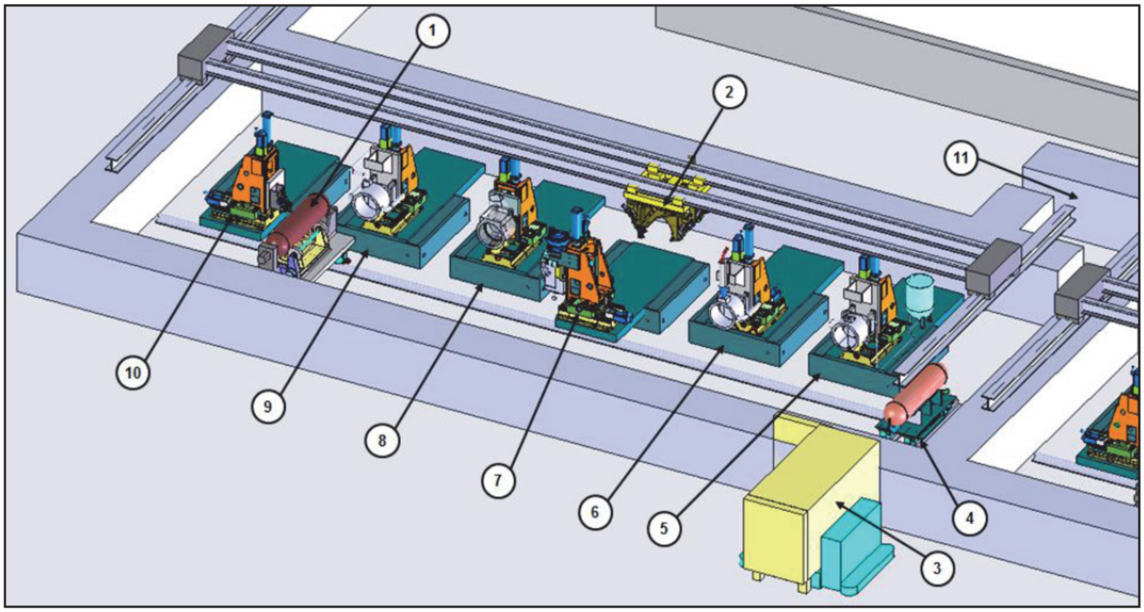
In the UFC weld cell, the UFC is first welded, inspected and machined. It is then moved by an OTC back to the flask trolley and retracted to the awaiting transfer flask. It is then transferred to one of the six copper application cells where the welded UFC is extracted by an OTC onto a UFC rotary positioner where copper is applied and annealed to finalize the UFC concealment.

After inspection, the UFC is ready to be released from the cell, and it is lifted by the OTC back to the flask trolley and returned to the awaiting transfer flask. The detailed list of process steps within the processing cells is given in Appendix B. Figure 17 and Figure 18 show the UFC weld cell and copper application cell respectively.



1. UFC Rotary Positioner
2. UFC Transfer Gantry
3. UFC Transfer Flask
4. Flask Trolley
5. Pre-heat Worktable
6. Welding Worktable
7. Cooling Worktable
8. Machining Worktable
9. NDE Worktable
10. Maintenance Entry/Exit Airlock

Figure 17: UFC Weld Cell (Ground Level)



1. UFC Rotary Positioner
2. UFC Transfer Gantry
3. UFC Transfer Flask
4. Flask Trolley
5. Grit / Air Blast Worktable
6. Copper Cold Spray Worktable
7. Machining Worktable
8. Annealing Worktable
9. Cooling Worktable
10. NDE Worktable
11. Maintenance Entry/Exit Airlock

Figure 18: UFC Copper Application Cell (Ground Level)

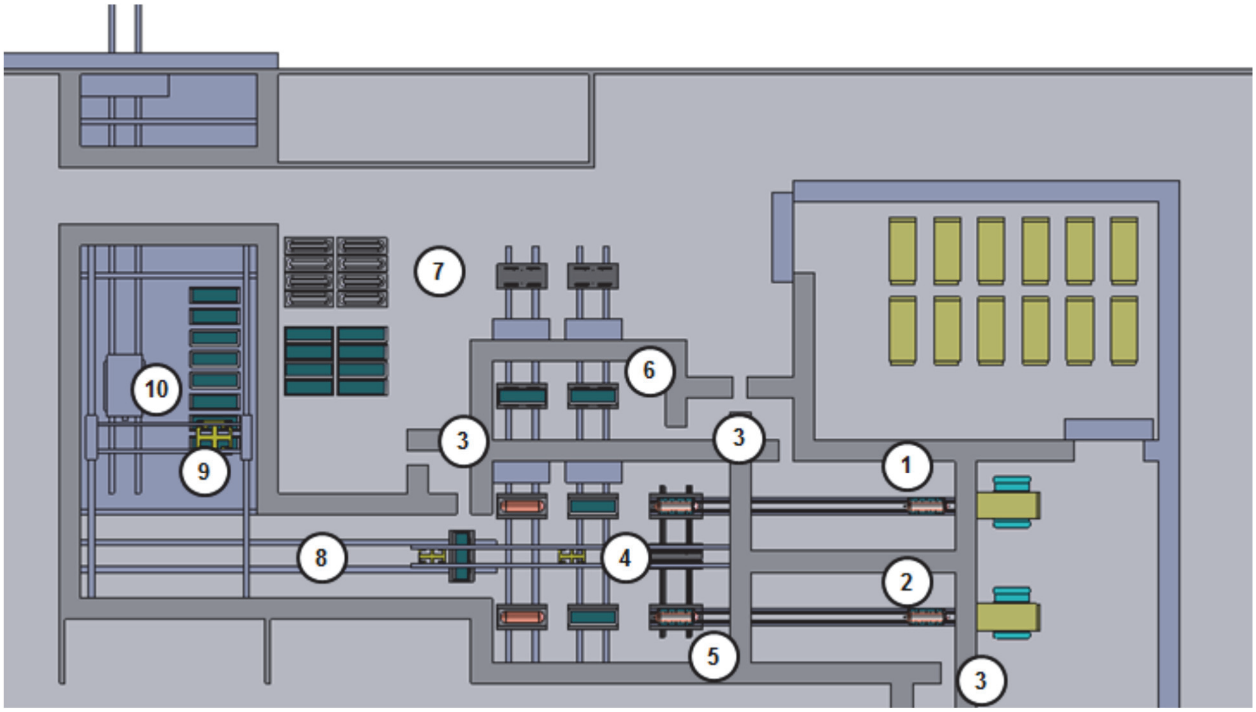
3.2.3.1.4 UFC Decontamination and Buffer Box Assembly

After the UFCs have been completely processed, they are transferred to the decontamination cell using the transfer flask. There are two decontamination cells in the UFPP in connection to the buffer box assembly (see Figure 19).

The UFC on a flask trolley is extracted from the transfer flask and surveyed for potential contamination on the surface of the UFC. Once deemed acceptable, the UFC on the trolley is transferred through an airlock to the UFC Buffer Box Loading area (Figure 19). An OTC is used first to place the UFC inside the buffer box bottom and then to lift the pre-staged buffer box lid on the top of the UFC. The final assembly is transferred to the buffer box transfer area and lifted by another OTC to the Dispatch Hall in the basement for transfer underground or stored in a lay down area.

The buffer box consists of prefabricated buffer blocks that are assembled in 4 stages (Figure 20):

1. The bottom blocks are installed on a platform within lower steel cover;
2. The UFC is placed over the bottom blocks;
3. Top blocks are installed; and
4. Top steel cover is installed.



1. Decontamination Cell #1
2. Decontamination Cell #2
3. Maintenance Access Airlocks
4. UFC Buffer Box Loading Area
5. UFC on Transfer Flask
6. Buffer Box Airlock
7. Buffer Box Pre-Assembly / Staging area
8. Assembled Buffer Box Transfer Area
9. Assembled Buffer Box Laydown Area
10. Buffer Box Transport Cask

Figure 19: Decontamination and Dispatch Cell and Buffer Box Assembly (Ground Level)

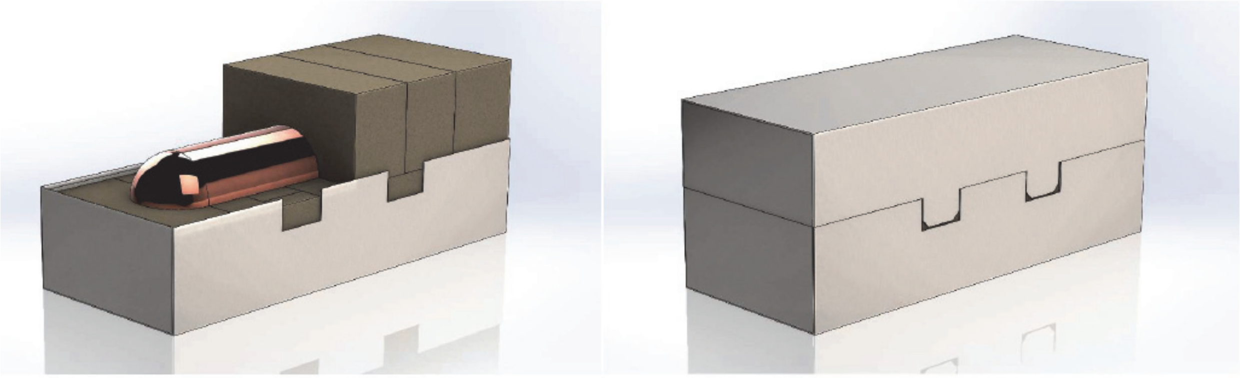


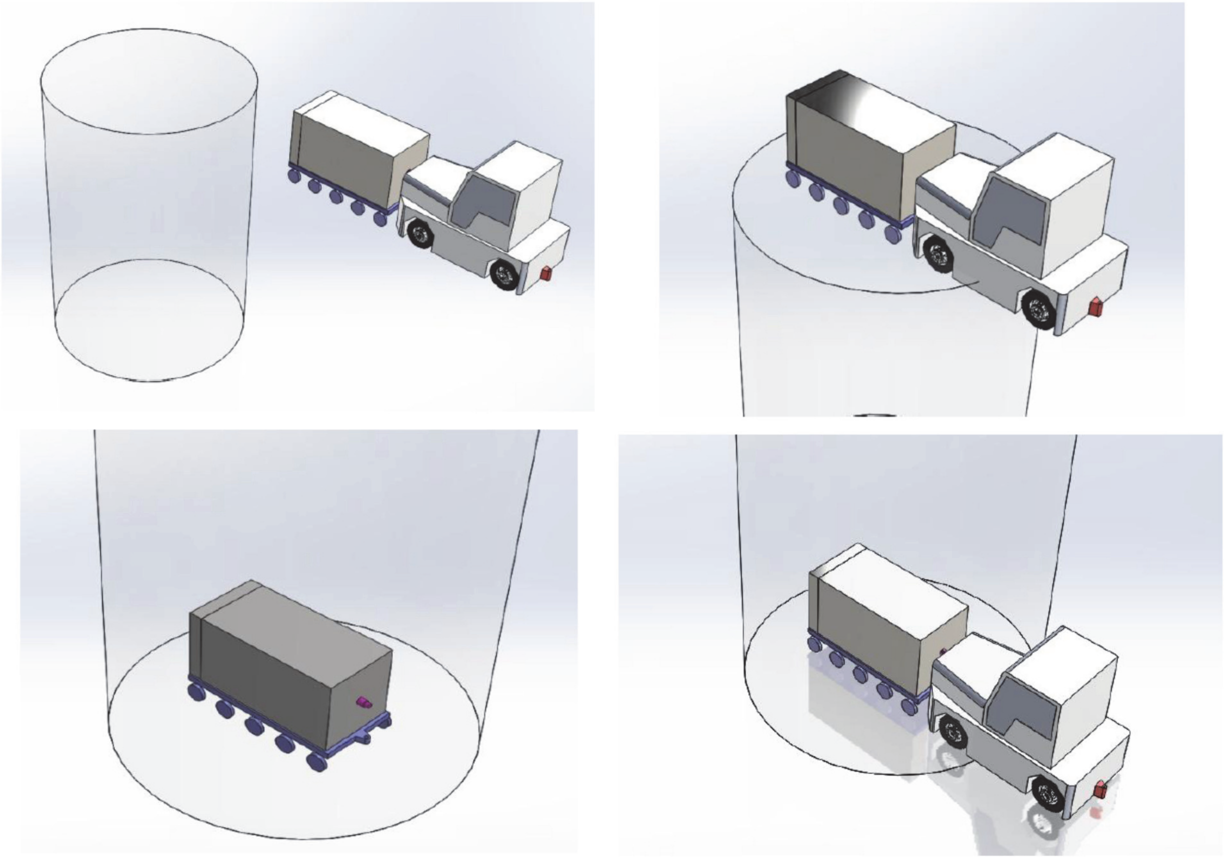
Figure 20: Buffer Box Assembly

3.2.3.1.5 Transferring UFC/Buffer Box in Shielded Cask from UFPP

The buffer box assembly is then remotely placed in the shielded transport cask (Figure 10) in the Dispatch Hall in the basement for transfer to the shaft and placement in the repository. The transport cask is towed to the main shaft hoist area using a tow vehicle (Figure 10 and Figure 21).

3.2.3.2 Shaft Operation Activities

The transport cask is driven to the main shaft hoist area, pushed into the shaft cage and secured. The hoist moves it to the underground repository where it is connected to another tow vehicle for transfer to the placement room. A generalized illustration of the shaft operation is shown in Figure 21.



Note: Top Left: Trolley Moved with the UFC Transfer Cask to the Main Shaft Area; Top Right: Trolley Placed with the UFC Transfer Cask into the Shaft Hoist and Secured; Bottom Left: Trolley Lowered to the Underground DGR; Bottom Right: Trolley Unsecured and Dispatched.

Figure 21: Schematic Presentation of Shaft Operations

3.2.3.3 Underground Facility Activities

The current design of the repository does not include plans to store filled transport casks underground.

The transport casks are moved directly to the placement rooms. A schematic illustration of a filled placement room is given in Figure 22.

Before placement of the buffer boxes can begin, the placement room is prepared by installing a bentonite levelling layer on the floor and placing floor plates with ventilation ducts on the bentonite layer. Then, a shielding canopy is transferred and installed at the entrance of the placement room.

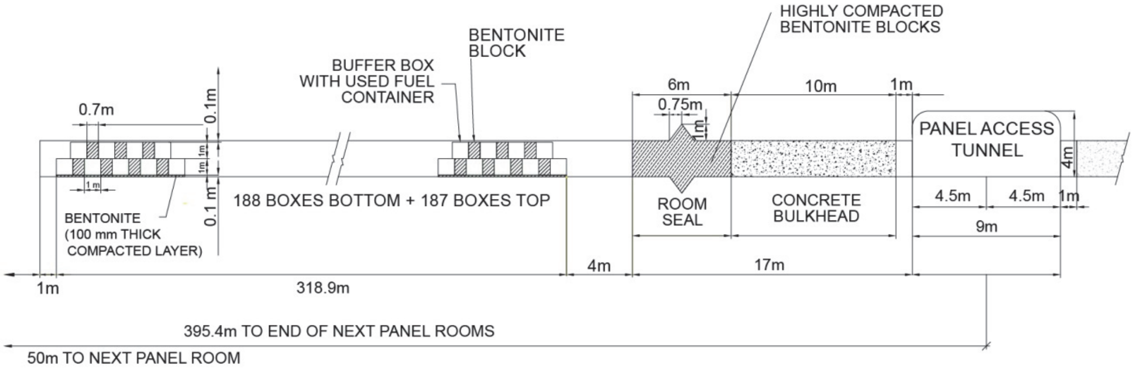


Figure 22: Filled Placement Room Layout

3.2.3.3.1 Shielding Canopy Reload Area and Placement Operation for Buffer Boxes

The transport cask is driven to the active placement room, which is now equipped with an awaiting movable shielding canopy at the entrance and a remotely operated placement vehicle parked in the access tunnel across from it. The transport cask connects with the canopy and the shielding door is opened (Figure 23). A hydraulic cylinder cart is used to push the buffer box out of the transport cask, into the shielding canopy and onto a placement vehicle wedge tray. Once the shielding door of the shielding canopy is closed, the placement operations begin. The actual placement of the buffer box is performed with the remotely operated forklift (Figure 24 and Figure 25). There is a shielding wall on the front of the remote forklift to assist with potential recovery efforts if needed. However, it is assumed that the forklift would be winched out if it fails while in the room. Between each buffer box, a bentonite spacer block is installed (Figure 25).

3.2.3.3.2 Removing Floor Plates and Pellet Installation

After placement of the buffer boxes, the floor plates and ventilation ducts are remotely removed. Pellets are remotely blown in around the placed buffer boxes and the bentonite spacer blocks. Since all operations are remote, no worker exposure is anticipated from these operations.

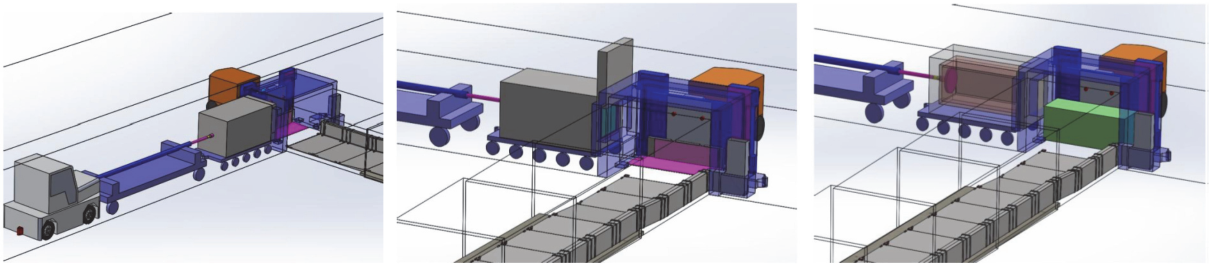


Figure 23: Transfer of the Buffer Box from Transport Cask to Placement Forklift Using Hydraulic Cylinder Equipment

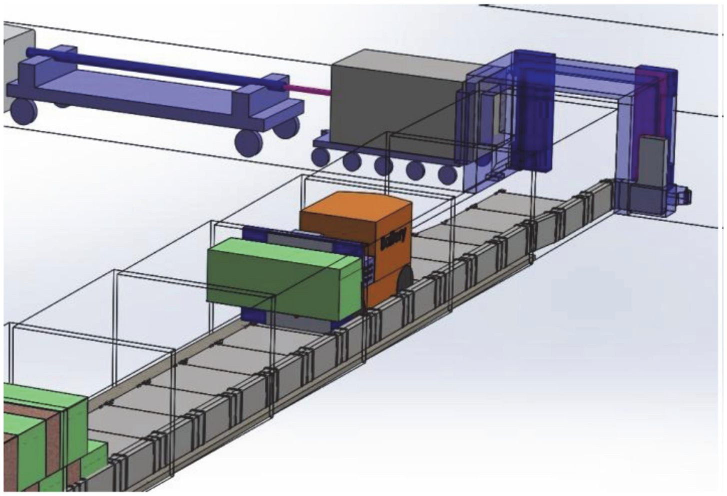
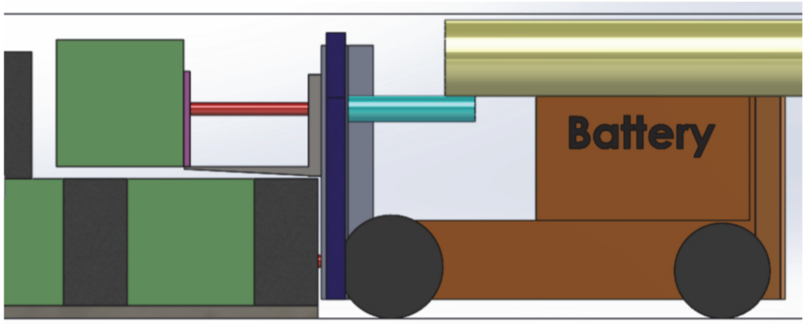


Figure 24: Transferring Buffer Box to Placement Room



Note: Green Boxes (Buffer Box); Dark Grey Boxes (Bentonite Spacer Blocks)

Figure 25: Buffer Box Placement

3.3 WORKING ASSUMPTIONS

The excavation will most likely be done as a step-wise process, panel by panel. Since excavation would occur far from the areas where placement is ongoing, excavation is not included in the hazard consideration at this stage. The excavation related hazards will need to be assessed when more detailed plans are available.

The height of each floor (ground level and basement) is about 5 m. Therefore, the maximum height of the fall/drop is taken to be 5 m.

The number of failure modes is affected greatly by the durability of the used fuel packages. The working assumptions for the durability of the used fuel packages in drop scenarios are listed below:

- The UFTP endures all drops (less than 9 m) potentially occurring in UFPP without failure; and
- The Mark II UFC endures all drop events in the facility, except for the cage fall scenario.

The 9 m drop test of a UFTP is assumed to bound most severe accidents including collision with another vehicle or wall (Easton 2014).

In addition, transfer vehicles (e.g., transfer pallet, towed transport cask, transfer flask on AGV, and flask trolley) are assumed to operate at low speed and/or on rails such that any collisions (e.g., with walls or other vehicles) could not damage the durable used fuel packages.

On the other hand, a module or a UFTP (without impact limiter and with loose lid) in the elevator, if dropped, could damage the used fuel resulting in the release of some radionuclides and could expose workers nearby.

Other working assumptions for the preliminary hazard identification are given below:

- The UFPP and DGR are designed for probable maximum flood, and the facility is located sufficiently in-land from a lake or large river, to avoid large scale flood events.
- The facility is sited far away (e.g., 1 km) from any rail line transporting flammable or toxic/corrosive materials.
- Diesel fuel storage above ground is located sufficiently far from the UFPP to note present a fire/explosion hazard.
- Wet storage is not required because all fuel received at the UFPP will be sufficiently cool for dry storage.
- Permanent water lines are not present in the radiation zones to avoid any potential flooding in the radioactive areas.
- Direct-gas-fire heating system for ventilation heating is located in a dedicated building far from the UFPP to not present a fire/explosion hazard.
- Fuels other than CANDU can be managed in the UFPP/DGR if they have similar characteristics. Re-assessment is needed in the case of different fuel types.
- Any failed UFTPs/UFCs due to manufacturing errors are detected before shipping to UFPP.

- Any large voids in the concrete shielding walls of the UFPP are detected by QC/QA activities; therefore, loss of shielding due to material deficiencies is not considered (except the undetected flawed UFTP and UFC cases).
- No inadvertent entry into hot cells is considered possible.
- In the hot cells:
    - No water pipes are located inside.
    - Compressed gas is used in the cold spray cell. Appropriate safety device is available for the gas tank, such that if the compressed gas line is broken accidentally, compressed gas in the tank would be released slowly to the cell.
- Ventilation HEPA filter system is valved in 100% of the time for UFPP, and valved in only when needed for the underground facility.
- Electricity/battery-run transport/lifting equipment is used in UFPP and DGR, except for the UFTP transport vehicle, back-up generators (e.g., for shafts), and placement room forklifts in the underground facility which are diesel operated.
- In the underground facility:
    - The battery charging station is located far from the UFCs so that the potential impact from a hydrogen explosion on the UFCs is insignificant.
    - Potential diesel storage is located far from UFC placement rooms.
    - Vault cave-in does not damage the intact UFCs, only undetected flawed UFCs, as the intact UFCs can withstand 45 MPa.

3.4 SAFETY CULTURE IN A NUCLEAR FACILITY

In general, nuclear facilities have a high safety culture. Personnel are appropriately selected and trained, including emergency training. Therefore, this preliminary hazard identification does not include unlikely human errors such as failing to leave the site or intentionally turning off alarm systems during an accident. It is also assumed that work schedules are followed, to prevent or minimize overworking and resulting fatigue and unintentional mistakes.

Safety include commissioning tests for facilities (buildings, processes, and equipment/vehicles) before the facility is approved for operation. It is assumed in this preliminary hazard identification that these tests discover and fix any major flaws in the building designs and processes.

It is worth noting that in recent accidents that have occurred within repositories (e.g., U.S. WIPP) and mines (e.g., Beaconsfield Gold Mine), the accidents have been for the large part due to not following guidelines, or neglecting safety culture. Human errors/mistakes can be greatly mitigated by good planning and continuous training of staff. Operational safety in a deep geological repository will be similar to that of nuclear power plants.

4. INTERNAL INITIATING EVENTS

4.1 OPERATION DERIVED FAILURES

4.1.1 Failure Identification Process

The methodology for the hazard identification process is described in Section 2.2. An initial list of process steps for the Mark II conceptual design has been compiled from the NWMO concept design documents including the Mark II conceptual design report (Heystee 2015), most recent design updates, and from interviewing NWMO personnel. The full list is provided in Appendix B. There are a total of 147 steps from UFTP receipt at the UFPP and final placement underground. Some steps are also subdivided.

Failure Modes and Effects Analysis (FMEA) is used to identify potential hazards that could result in worker/public doses. The FMEA table is modified based on standard FMEA by combining features from both design and process FMEAs to fit the needs of this project. Parts of the 'Hazard and Operability Study (HAZOP) procedures are also employed to help ensure completeness in the FMEA process. Both the FMEA and HAZOP processes are widely-used methodologies for hazard identification in diverse industries (see e.g., Stamatis 2003). The FMEA process identifies single failures and is not used for combined accidents. Therefore, certain event chain combinations postulated during the FMEA process are separately discussed in Section 4.10.

The FMEA table (Appendix C) is produced by going through the entire process of waste handling operations from receiving the used fuel at the UFPP until it has been placed in the repository, surrounded by the buffer, and the backfill has been installed. Potential failure modes are identified using two different approaches:

1. When design works well and workers make mistakes; and
2. When design (equipment) fails but workers perform their job correctly.

The FMEA identifies which failure modes can potentially lead to radiological consequences and which cannot; only those in the first category are considered further. Key words (see Table 5), based on HAZOP, have been used when producing FMEA. These key words aim to make sure that consideration of potential hazards is equally thorough at every assessed step. Please note that not all 147 steps are included in Appendix C, as some of the steps do not involve handling and transfer of used fuel packages. For examples, Steps 53 to 62 (listed in Appendix B) are concerned with empty UFC preparation activities.

The potential radiological hazards have been evaluated based on the detection, severity, and probability of event occurrence. A numerical value is assigned to each of these properties (detection index, severity index and probability of occurrence index), following the definition that the higher the index the greater the relevance of the hazard. Explanations of the meaning of the different possible values of the indexes are included in Table 6.

Based on the numbering, a Risk Priority Number (RPN) has been calculated as the product of the three indices for each potential hazard. The RPN is not used in this report to rank the potential accidents in order since the design is at the development stage. Hazard assessment will be done for all identified potential accident scenarios with potential radiological consequence, when detailed designs are available. However, the RPN can be used for assessing the effects of any mitigation action or design change in the future, comparing the values of the RPN before and after the mitigation action.

Table 5: Keywords Used in FMEA and Their Explanations, Based on HAZOP Method

Key word	Explanation
LESS	A process works less than designed to
MORE	A process works more than designed to
NOT	A process does not work
OTHER THAN	Something else happens other than the designed process
AS WELL AS	Something else happens during the designed process
REVERSE	The process happens in reverse order

Table 6: RPN Numbering Explanations- A) Detection, B) Severity and C) Probability of Occurrence

Nbr.	A) Detection (initial estimate)
1	Quick detection (< 1 minute)
2	Detection during interval of 1 to 5 minutes
3	Detection during interval of 5 minutes to 1 hour
4	Detection takes from 1 to 8 hours
5	Detection takes 8 hours or more
Nbr.	**B) Severity (radiological)**
1	No additional exposure
2	Exposure to ambient radiation that otherwise would not occur
3	Additional exposure to radiation from UFTP/UFC in transport cask that otherwise would not occur (moderate distance)
4	Additional exposure to radiation from UFTP/UFC in transport cask that otherwise would not occur (next to source)
5	Exposure to direct radiation from modules/bundles/UFC (including ruptured shielding)
6	Release of radionuclides without additional damage to the fuel
7	Release of radionuclides with additional damage to the fuel
Nbr.	**C) Probability of Occurrence**
1	Extremely improbable
2	Very improbable
3	Improbable
4	Potential to occur once during the operation of the facility
5	Potential to occur more than once during the operation of the facility

The number of failure modes is affected greatly by the durability of the used fuel packages. The working assumptions for the durability of the used fuel packages are discussed in Section 3.3 - i.e., the UFTP and the Mark II UFC remain intact if dropped.

Deficient UFTPs and UFCs are discussed separately in Section 4.10. It is acknowledged that in UFTPs, there is a potential of failed shielding due to manufacturing errors (e.g., voids); but in this report, these errors are assumed to be detected during manufacturing or before shipping to the UFPP.

As mentioned in Section 2.2, certain accident scenarios, e.g., those initiated externally, are discussed separately from FMEA due to their nature of being only partially tied to operation steps (see Sections 4.2 - 4.10).

In the FMEA, each postulated accident scenario is assigned with a FMEA number. This number is formed by the Mark II conceptual design (R), followed by a process step number (from Appendix B) and the number of the postulated accident for this particular step. For example, the FMEA number of II-3.1 means the first postulated failure mode scenario (jamming of the weather cover) identified for the Mark II conceptual design process step 3 (open weather cover on UFTP transport vehicle). See Appendix C for complete list of accident scenarios for the conceptual design.

Workers in the repository facilities can be exposed to small doses of radiation that arise from normal operations. The doses from normal operations are designed to be as low as reasonably achievable and are controlled by the dose limit acceptance criteria. Due to accidents, normal worker dose may be exceeded, for example, in cases where failure mode causes delay in operation, subjecting workers to longer radiation exposure than intended in normal operation. Accidents could also add to worker doses in case of, for example, loss of shielding. These are usually related to situations where shielding that is intended to be in place in a given operation, is not functioning as planned.

In cases where the shielding packages could break due to accident, release of radionuclides could be the source of additional doses to workers and members of the public near the facility.

Therefore, the possible accident consequence can be grouped into the following categories:

- Longer or additional worker exposure;
- Loss of shielding; and
- Release of radionuclides.

Public exposure is only possible in cases where radionuclides are released. In most identified accident scenarios where radionuclides are released and public exposure is considered to occur, the workers are within UFPP and shielding structures should protect them accordingly. However, in accident scenario where there is no additional shielding barrier, an increase in workers dose could happen in addition to public exposure. (This scenario has not been identified in this report, but shaft cage fall would have the greatest potential for causing dose to workers).

The accident scenarios, identified based on possible accident consequence from the FMEA list, are summarized in Table 7. These scenarios are discussed in the following sections.

Table 7: Summary of FMEA Findings for the Mark II Conceptual Design

Accident Scenario	Enabling Process	Component or Failure Mode
Elevator fall leading to damage of a loaded UFTP and release of radionuclides	Equipment (elevator) malfunction	Modules in UFTP (loose lid and without impact limiter)
Shaft cage fall leading to damage of a loaded UFC and release of radionuclides	Equipment (shaft hoisting) malfunction	UFC buffer box in transport cask in cage
Drop scenarios leading to release of radionuclides and/or loss of shielding	Equipment (e.g., OTC, scissor lift) malfunction	Module, potentially dropping on other module(s)
		Used fuel bundle(s)
Drop scenarios leading to longer worker exposure	Equipment (e.g., weather cover on UFTP, OTC) malfunction	UFTP, potentially dropping on other UFTP(s)
		Module, potentially dropping on other module(s)
		Used fuel bundle(s)
Equipment/vehicle malfunction leading to longer/additional worker exposure scenarios	Equipment/ vehicle (e.g., tow vehicle and trolley with transport cask, OTC) malfunction	Equipment/ vehicle stops
		Equipment/ vehicle slower than anticipated process speed
		Vehicle collisions
Operator error leading to longer/ additional worker exposure scenarios	Operator error in handling equipment/vehicle (e.g., tow vehicle and trolley with transport cask, OTC)	Equipment/ vehicle stops
		Equipment/ vehicle slower than anticipated process speed
		Vehicle collisions
Power loss leading to longer/additional worker exposure scenarios	Power loss to equipment (e.g., OTC)	Equipment/vehicle stops
		Equipment/vehicle slower than anticipated process speed

Note: The complete list of all individual accident scenarios postulated in the FMEA process is in Appendix C.

4.1.2 Grouping and Frequency Estimations for Postulated Failure Modes and Operation Derived Internal Initiating Events

As there is a significant number of failure modes identified in the FMEA process that could lead to longer or additional worker exposure, these failure modes are grouped according to their similarity (Figure 2). For example, the FMEA failure modes identified under “Perform smear test” II-4.1 and II-4.2 are grouped together under “Smear test failure”. See Appendix C. Another example is the failure modes identified under “Detach tie-downs of loaded UFTP” II-6.1 and II-6.2, which are grouped under “Tie down detachment problem”. This grouping is presented in Appendix C last column. Appendix C also identifies potential accident scenarios that could cause release of radionuclides and/or loss of shielding. Potential loss of shielding is discussed separately in Section 4.4.

With this initial qualitative grouping, annual frequencies were estimated for failure modes resulting in longer or additional worker exposure (Table 8) and release of radionuclides (Table 9). However, the estimation is less detailed for the cases involving longer or additional worker exposure due to significant number of identified failure modes and their estimated small effect on personal dose. Details on how these frequencies were derived are given below.

Table 8: Failure Modes Leading to Longer or Additional Worker Exposure and Frequency

Failure Mode	Failure Mode Specification*	Failure Mode Frequency per Operation	Quantity of Potential Occurrences (a^{-1})	Frequency (a^{-1})
UFTP transport vehicle equipment malfunction	1. Tie-down detachment problems	5.0E-05	630	3.15E-02
	2. Weather cover opening problems	5.0E-05	630	3.15E-02
Test procedure failure	3. Smear test failure	5.0E-05	1260	6.30E-02
	4. Vent cell inspection equipment failure	5.0E-05	630	3.15E-02
Overhead transfer crane/gantry failure	5. Drop, slow operation/jamming, failure to grip, stop, unexpected location, collision	5.0E-05	18,900	9.45E-01
Electrical door failure in process line	6. Door does not open, opens half way, does not close	5.0E-05	22,050	1.10E+00
Failure of pallet on rail / rail cart / flask trolley on rails	7. Does not move, moves too slow, only part of the way, too fast, collides	5.0E-05	16,380	8.19E-01
Tow vehicle failure	8. Does not move, moves too slow, only part of the way, too fast and de-rails, collides	5.0E-05	20,160	1.01E+00
AGV system failure	9. AGV failure, stop and delay	5.0E-05	12,600	6.30E-01
Vent equipment failure	10. Does not operate, takes longer than expected	5.0E-05	630	3.15E-02
Attachment / detachment problems (UFTP lid)	11. Does not attach / detach, or takes longer than expected	5.0E-05	630	3.15E-02
Attachment / detachment problems (UFTP, Disposal process vehicles and equipment)	12. Does not attach / detach, or takes longer than expected	5.0E-05	17,010	8.51E-01
Disposal process equipment failure (buffer box)	13. Does not operate, stops, takes longer than expected	5.0E-05	17,640	8.82E-01
Disposal process equipment failure (underground)	14. Does not operate, stops, takes longer than expected	5.0E-05	10,080	5.04E-01

* Second column provides failure mode number for grouping of failure modes. These are combined In Table 13 of Section 4.11 to form accident scenarios. Here, the annual frequency is calculated for each grouping of failure modes number 1 to 14.

Table 9: Potential Scenarios Causing Release of Radionuclides and Frequency

FMEA no.	Failure Mode	Scenario Specification	Frequency (a^{-1}) *
II-16-1	When an UFTP is lifted on elevator from the basement to the ground level, the elevator fails and drops to the basement with the loaded UFTP (without impact limiter and with loose lid)	The elevator with UFTP falls down to the basement and the UFTP lid and the upper module fall over releasing some radionuclides (used fuel damage)	7.56E-04
II-17.2	When the UFTP lid is raised using OTC in the module handling cell, the OTC drops the lid on modules in the open UFTP	The UFTP lid falls (corner first) and breaks top part of the upper module damaging uppermost fuel bundles	3.15E-02
II-19-2.2	When a full module is transferred using OTC from the open UFTP in the module handling cell, the OTC fails dropping the module	The module is tilted or dropped and the fuel bundles fall out or fall with the module, resulting in the release of some radionuclides but no loss of shielding (used fuel damage)	6.30E-02
II-19-3.2	When a full module is transferred using OTC from the module handling cell to the dry storage, the OTC fails dropping the module	The module is tilted or dropped and the fuel bundles fall out or fall with the module, resulting in the release of some radionuclides but no loss of shielding (used fuel damage)	6.30E-02
II-19-6.2	When a full module is transferred using OTC from the dry storage to the module handling cell, the OTC fails dropping the module	The module is tilted or dropped and the fuel bundles fall out or fall with module, resulting in the release of some radionuclides but no loss of shielding (fuel damage)	6.30E-02
II-19-7.2	When a full module is lifted using OTC to the lay down area in the module handling cell, the OTC fails dropping the module	The module is tilted or dropped and the fuel bundles fall out or fall with module, release of some radionuclides but no loss of shielding (used fuel damage)	6.30E-02
II-31.2	When the upper module is loaded from the open UFTP using OTC to the lay down area in the module handling cell, the OTC fails dropping the module	The module is dropped (on lower module) and the used fuel is damaged	3.15E-02
II-32.2	When the lower module is loaded from the open UFTP using OTC to the lay down area in the module handling cell, the OTC fails dropping the module	The module is dropped on open empty UFTP or floor and the used fuel is damaged	3.15E-02
II-33.2	When a module is transferred using OTC from the lay down area in the module handling cell onto an inter-airlock trolley, the OTC fails dropping the module	The module drops on other modules (estimated maximum 4 of 5) in the module handling cell and the used fuel is damaged	6.30E-02
II-33.3	When a module is transferred using OTC from the lay down area in the module handling cell onto an inter-airlock trolley, the OTC fails dropping the module	The module drops on the inter-airlock trolley or floor and the used fuel is damaged	6.30E-02
II-35.2	When the full module and empty module are exchanged using OTC in the fuel module distribution hall, the OTC fails dropping the full module	The module and air- interlock trolley drop on floor and the used fuel is damaged	6.30E-02
II-36.1	When an empty module is returned from the fuel module distribution hall and transferred to the lay down area in the module handling cell, the OTC fails dropping the empty module	An empty module drops on other modules (estimated maximum 4 of 5) in the module handling cell and the used fuel is damaged	6.30E-02
II-38-1.2	When the module tube on the position table is aligned to the push location, the position table scissor lift fails dropping the module	The module is dropped (on scissor lift or slides from scissor lift) and the used fuel is damaged	2.02E-03

FMEA no.	Failure Mode	Scenario Specification	Frequency (a^{-1}) *
II-38-5.2	When the used fuel bundle is pushed (2 bundles at a time) to the UFC basket tube, the bundle is forced to an already filled places in basket tube	The used fuel bundles break	3.02E+00
II-38-5.3	When the used fuel bundle is pushed (2 bundles at a time) to the UFC basket tube, the basket is not in place due to malfunction of chaining of events	The used fuel bundles fall on floor, damage of the used fuel	3.02E+00
II-90.1	When the transport cask with the loaded UFC is lowered to the repository, the main shaft hoist fails dropping the cage with loaded UFC	The shaft cage falls and the loaded UFC is severely damaged and all fuel bundles are damaged	5.00E-7

*Values for calculating the annual frequencies are presented in Appendix D.2.

The following sections present the method of how frequencies are determined for the operation derived accidents identified in the FMEA process due to failure of the following:

1. Elevator malfunction leading to elevator fall with loaded UFTP (loose lid without impact);
2. Scissor lift failure leading to module drop from module positioning table;
3. Shaft hoist system failure leading to cage fall with loaded UFC;
4. Overhead transfer crane/gantry failure leading to the drop of a suspended load;
5. Fuel transfer machine operation failure leading to used fuel bundle break; and
6. Equipment/ vehicle failure or human errors leading to longer or higher worker exposure.

A summary of the failure frequency values used in this study is given in Appendix D.1.

4.1.2.1 Elevator Malfunction Leading to Elevator Fall with Loaded UFTP (Loose Lid without Impact Limiter)

For elevator fall leading to used fuel damage and release of radionuclides from loaded UFTP (loose lid without impact limiter), the frequency per operation is derived from OHN (1994) that used an annual shaft hoisting failure frequency of 4E-3 a^{-1}. The OHN assessment was done for an average used fuel packaging rate of 250,000 bundles, or 1300 UFTPs received annually and 3,472 UFCs filled and emplaced in the DGR per year (since each UFC had capacity for 72 bundles). Therefore, a failure frequency of 1.2E-6 per UFC lift is estimated.

In OPG (2011), the cage fall accident is identified as unlikely (i.e., with an annual frequency between 10^{-7} and 10^{-2}). It is stated that in modern mines, hoist or cage failures leading to cage falls are very unlikely, as discussed in Section 4.1.2.3.

Due to elevator not being similar to regular shafts and cage systems, the conservative approach by OHN (1994) is still kept in this preliminary hazard identification phase. As detailed design is done, the frequency will need to be reconsidered. With an annual throughput of 630 UFTPs per year for the Mark II conceptual design, the annual frequency for elevator failure is 7.6E-4 a^{-1} for moving UFTPs from the basement to the ground level. This annual frequency estimate puts this accident in the design basis accident group.

4.1.2.2 Scissor Lift Failure Leading to Module Drop from Module Positioning Table

In an operational safety assessment study (OHN 1994), an annual scissor lift failure frequency of 2.1E-3 a^{-1} was used. This frequency was derived from performance data for hydraulic jacks, assuming continuous duty during two shifts per day, 52 weeks per year. Taking into account the number of UFTPs received and processed at the UFPP (1,300 per year in OHN 1994), a failure frequency of 1.6E-6 per UFTP lift is obtained. In the Mark II conceptual design, a scissor lift is used in aligning used fuel bundles in the module for fuel push operation. Using the same derived frequency, the annual failure frequency would be 2.0E-03 a^{-1}, due to the quantity of modules being twice as large as the quantity of UFTPs (630 per year). Calculation values for scissor lift failure mode are also presented in table format in the beginning of Appendix D.2.

No other information has been found for the failure frequency of scissor lifts, and hence the values in OHN (1994) have been adopted. With this value the scissors lifter failure is a DBA for the conceptual design, with frequencies in the order of 1E-3 a^{-1}. It would be necessary to drop the failure frequency of the scissor lifts at least two orders of magnitude to lower the classification of this accident from design basis accident to beyond design basis accident.

4.1.2.3 Shaft Hoist System Failure Leading to Cage Fall with Loaded UFC

For shaft cage fall leading to fuel damage and release of radionuclides, an annual shaft hoisting failure frequency of 4E-3 a^{-1} was used in a preclosure safety assessment study (OHN 1994). This value is based on failures from shaft hoisting system. The assessment was done for an average used fuel packaging rate of 250,000 bundles, or 1300 UFTPs received annually and 3472 UFCs filled and placed in the DGR per year (since each UFC had capacity for 72 bundles). Therefore, a failure frequency of 1.2E-6 per UFC lift was used.

In OPG (2011), the “cage fall” accident was identified as unlikely (i.e., with an annual frequency between 10^{-7} and 10^{-2}). It is stated that in modern mines, hoist or cage failures leading to cage falls are very unlikely, that the DGR will be built with current best practices, and there will be routine inspection of hoist safety system. In addition, the DGR shaft operation is expected to be lower than for typical mines. Therefore, cage fall was considered as an unlikely initiating event, and the consequences of such an accident were evaluated as a bounding scenario.

In ANDRA (2005), a frequency for a cage falling down the shaft of 5E-7 a^{-1} (for 5,000 hours of operation per year) is mentioned. The last serious accident of this class in France occurred at Reumaux (Lorraine) in 1925. The analyses of the mechanical consequences of a cage fall found that there is no loss of containment of radioactive materials in such accident. However, because of the uncertainties on how the fall in the shaft takes place and the definition of the moving body, scenarios of a release of radionuclide materials were defined to estimate the associated radiological risk.

In this preliminary hazard identification, the annual frequency of cage fall is assumed to be the same frequency that ANDRA (2005) has used, without determining whether the operation time is the same or not. This makes it a beyond design basis accident. After more detailed process descriptions and time estimations, the frequency can be scaled or reconsidered.

4.1.2.4 Overhead Transfer Crane/Gantry Failure Leading to the Drop of a Suspended Load

In many failure modes, the initiating event is the drop of a suspended load, which could be a used fuel module, a UFTP or a UFC lifted by overhead transfer crane/gantry. The frequency of drop of the suspended load is an important parameter, whose value is estimated in this section. The load can weigh about 2.3 tonnes for a module, 35 tonnes for a loaded UFTP, and 2.8 tonnes for a loaded UFC.

U.S. NUREG (2003) presents information regarding the frequency of load drops in U.S. nuclear power plants. Results are presented mainly in terms of drop per reactor for a given year. Only for the very heavy loads (>27 tonnes) is the number of lifts available and a frequency of drop per lift can be calculated. The total number of very heavy load lifts for all U.S. nuclear power plants that operated from 1980 through 2002 was approximately 54,000; there were 3 load drops during this period. The 3 heavy lift drops were caused by rigging failures. On the basis of these data, the load drop frequency was calculated in U.S. NUREG (2003) to be approximately 5.6E-5 drop/lift (3/54,000) for very heavy load lifts.

A second estimate can be made using data from the period 1968-2002, when U.S. nuclear power plants in operation reported 47 events involving load drops (U.S. NUREG 2003). Over half of these load drop events were fuel assembly drops caused by grapple operation malfunction or human errors. Although the exact number of lifts is not known, it is possible to make a rough estimation of the frequency of fuel assembly drops. During the period 1968-2002 the average number of reactors in operation in U.S. was about 60, of which it is assumed that one third were BWR and two thirds were PWR. Assuming that the cores of the BWR contain 500 fuel assemblies and the cores of the PWRs contain 150 fuel assemblies, and 18 month cycles, the number of fuel assembly movements during the refueling outages was about 21,000 per year. Assuming that during the 34 year period there were 25 fuel assembly drops resulting in radioactive release, the calculated frequency of load drop is 3.5E-5 drop per lift. It is noted that this frequency is similar to the frequency obtained in U.S. NUREG (2003) for very heavy loads.

A third estimate can be obtained from U.S. NUREG (1980) based on data available from:

- Occupational Safety and Health Administration (OSHA), involving root cause data on over 1000 crane accidents during an unspecified time period;
- The Department of the Navy, involving 466 crane events occurring between February 1974 and October 1977; and
- U.S. Nuclear Regulatory Commission Licensee Event Report involving 34 crane events occurring between July 1969 and July 1979.

Multiple probabilities are given for various scenarios in U.S. NUREG (1980). However, the study states that "Based on the data collected from the Navy, it is expected that the probability of handling system failure for nuclear plant cranes will be on the order of between 1.0E-5 and 1.5E-4 per lift." This frequency of failure was a best estimate, since the Navy crane data do not indicate how many lifts were actually performed, i.e., only the number of problems has been quantified.

The frequency assumed in OHN (1994) for an overhead carriage dropping of a loaded fuel module is 3E-6 to 5E-6 per lift. This value is smaller than the values estimated above using U.S. NUREG (2003) and U.S. NUREG (1980) data.

U.S. DOE (2009) provides data about the number of drops of TAD (Transportation, Aging and Disposal) canisters during transfer by a Canister Transfer Machine (CTM) over the preclosure period of Yucca Mountain. A mean value of 0.21 drops was obtained following a complex methodology using event trees. A total of 15,121 TAD transfers by the CTM were expected to be done (Table 1.7-5 of U.S. DOE 2009). With the previous data the TAD drop frequency is 1.4E-5 per lift, similar to the values obtained in other sources.

Due to the preliminary character of the hazard assessment, it is appropriate to use conservative drop frequencies. Therefore, a frequency of 5E-5 drop per lift for all the lifts in the UFPP (lifts of an UFTP, a module, and an UFC with and without buffer box) is used.

As discussed in Section 3.3, an intact UFTP is considered to endure all potential drop heights in the UFPP (all are less than 9 m). In the Mark II conceptual design, an intact UFC is considered to endure all potential falls possible in current UFPP and DGR design (maximum height 5 m). As implied by the header of Section 4.1.2.3, the high shaft cage fall would result in the breach of a loaded UFC.

4.1.2.5 Used Fuel Transfer Machine Operation Failure Leading to Used Fuel Bundle Break

For the Mark II conceptual design when used fuel bundles are pushed (two bundles at a time) from module to basket in the fuel handling cell, they may accidently drop to the floor or may be crushed if the basket is not correctly in place in the fuel transfer cell to receive them. Due to the quantity of repetitions of this action annually, 60,480 (120,960 used fuel bundles/2), the frequency of this failure mode increases into AOO range with even very low frequency per action. There are very little quantified data of occurrence for these types of actions and, therefore, the frequency for lifts is used here as 5E-5 failure per push, to display the significant role of repetition. With current repetition numbers and considered frequency, the annual frequency would be 3 for this accident (anticipated operational occurrences). This initial frequency is used in this preliminary stage of design to point out a potential large frequency for a process step failure mode, for which mitigation plays a very important role.

4.1.2.6 Equipment/ Vehicle Failure or Human Errors Leading to Longer or Additional Worker Exposure

The FMEA table in Appendix C lists the operation-derived accidents that could cause longer or additional exposure to workers, which are summarized in Table 8. The estimated frequencies for these accidents are also presented in Table 8. The majority of the accidents recognized in the FMEA process are due to failure in equipment and vehicle (UFTP transport vehicle equipment, overhead transfer crane/gantry, electrical door, pallet on rails/ rail cart/ flask trolley on rails, tow vehicle, AGV, vent equipment, attachment/detachment device, and disposal process equipment) or personnel mistake, e.g., in smear test.

Due to the preliminary character of the hazard assessment, the frequency for an operation resulting in prolonged operating time with minor additional worker dose is set here to be similar to that for drop scenarios, 5E-5 per operation[1]. This is done to provide a guideline on an approximate annual frequency of these accidents. Many of these accidents, particularly the

---

[1] Chapter 7 discusses this decision and a note to reader that there are no correct frequency estimations for these found in literature; these frequencies are used as examples only.

ones with the least severe dose consequences, have high probabilities to occur during the operation of the facility. To acquire annual quantity of this kind of operations, the quantity of these failure mode producing steps were counted from the FMEA table.

4.2 VENTILATION AND FILTER SYSTEM FAILURE

The Mark II conceptual design considers high Efficiency Particulate Air (HEPA) filter systems at the UFPP and underground facility. Because of low iodine inventories, charcoal filters are not included in the current design.

All rooms in the UFPP are classified at least as Zone 2 (Figure 13), but final classification of zones will not be done until after the detailed design is verified by the appropriate Radiological Protection Adviser (RPA). Small negative pressure in respect to the atmospheric pressure is maintained in the process rooms. Clear air enters the rooms with high radiation fields through HEPA filters to exclude hazard of potential back flow. Ventilated air also passes through a HEPA filter prior to discharge.

There are three separate air exhaust systems at the UFPP:

1. Zone 2 Space Exhaust air will not usually be HEPA filtered, but will be monitored for entrained radioactivity.
2. Zone 3 Space Exhaust will be filtered by single stage HEPA filter, with monitoring equipment provided after the filters.
3. Zone 4 Cell Active Exhaust will be filtered by two stages of HEPA filters, with monitoring equipment provided at the filters.

All exhaust systems act separate from each other. HEPA filters are situated in a separate HEPA filter room, where filters are changed safely to maintain acceptable discharge limits. Each exhaust system is stand-alone, with air being ducted out of each space via exhaust grilles. HEPA filters will undergo a further hazard evaluation in the detailed design phase to comply with the requirements. After filtering, air is released to the atmosphere.

Fresh air flows into underground facility via the main shaft and exhaust air is routed along the ventilation shaft and service shaft. Figure 26 presents a simplified illustration of ventilation. The design flow requires five primary fans on the surface and five more underground to redistribute flow. The fresh air heating plant will be located at the surface. Exhaust is designed to flow through unoccupied areas, and from less contaminated areas to more contaminated, should contamination occur. HEPA filtering for the underground facility is not on at all times, but will switch on if contamination and radioactive release is detected above threshold. HEPA filtration can be installed in exhaust routes, ventilation and service shafts. In preliminary hazard identification, a stand-by HEPA ventilation system is assumed in both of these locations.

For the frequency of failure of the HEPA filters, an annual value of 7.6E-2 is recommended on the basis of U.S. NRC (1987), meaning a failure where HEPA filter is not available for use at the needed location. As a consequence, the frequency of a given accident without filtration is 0.076 times the frequency of the accident with filtration. During normal DGR operation process, there are no contaminants in the air due to good containment of the UFCs. Therefore, as a single event, HEPA filter failure would not cause a radiological accident in DGR during normal operation. Only if containment is breached will radionuclides be released; this triggers the HEPA filters to action. At this point, a HEPA failure would allow release of radionuclides to the atmosphere. In considering DGR hazards, the potential consequence on people outside the

DGR will need to be considered both with working HEPA filtering and without it; however, these situations are not presented as separate accident scenarios in this report. In UFPP and DGR, the frequency of HEPA filtration failure is kept as 7.6E-2 a^{-1} in the preliminary hazard identification; as such, the filtration failure is presented as an accident scenario, even though the actual hazard would be a combined accident of release of radionuclides and then of HEPA filter failure. The need and the effectiveness of the HEPA system will be evaluated in the future design.

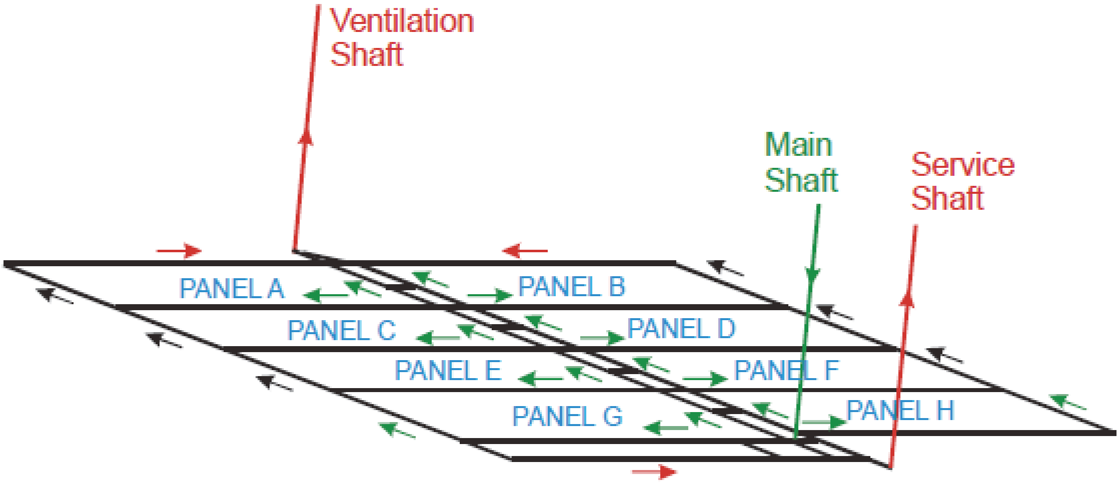


Figure 26: Simplified Illustration of DGR Ventilation

4.3 POWER FAILURE

The UFPP and underground facility are designed for power loss from main grid by having sufficient backup generators that start working if main power is lost. Total power loss could occur if the generator(s) does not function during power failure. This is improbable. Nevertheless, the systems in both UFPP and underground DGR are designed to shut down in case of power failure, so that passive shielding structures continue providing shielding against radiation. This power loss would then result in delay of operation, but it would not increase doses of workers, because workers would stop UFTP handling and UFC dispatch and move away from radiation fields for the duration of the power loss. In the active placement rooms, operators are exposed to an ambient radiation that is little affected by the operations being performed, and a delay in any operation would not increase the dose. A few cases where power failure would cause small increases in exposure time near a radiation source were identified in FMEA as examples.

The impact of power failure of both main power and generator(s) would be mainly on cost and efficiency of the facility.

4.4 SHIELDING SYSTEM FAILURE OR FLAWED OVERPACK (UFTP/UFC)

Shielding system failure can be induced with:

- Initial flaw in manufacturing of packages (UFTP, UFC, transfer flask or transport cask) prior to shipping to UFPP;
- Unintentional opening of gaps in shielding; or
- Damage to packages.

In this preliminary hazard identification, the scope has been limited to operation starting at the point packages are received in the UFPP and ending when the UFC has been placed and tunnel backfill has been installed. Therefore, manufacturing flaws, which will be investigated in manufacturing facility are excluded from the scope of this report and need further consideration by NWMO. Damage of packages is included in operation derived accidents and identified in the FMEA process (Section 4.1).

In the Mark II conceptual design, a gap in the shielding system could happen when the connection of the transfer flask with the welding or copper application cell is not correct. Radiation could then emanate from the UFC to the UFC transfer hall. These accidents would lead to a significant increase in dose rates in the affected areas that would be detected immediately by the radiation monitoring equipment. In this case, alarms would sound and workers would leave the area quickly. However, this does not affect the frequency of this occurring.

Probabilities for these accident types will strongly depend on the designs adopted. There will be interlocks to the hot cells to avoid this class of problems and hence the frequency will be low (but hard to quantify). For this preliminary hazard identification, a frequency of 5E-5 per operation is assumed.

However, the operations in which these failures happen are repeated many times during one year of operation of the UFPP. For instance, in the Mark II conceptual design, a UFC will be transferred from a transfer flask to a welding or copper application cell 10,080 times per year, based on the throughput of 2,520 UFCs per year, and entry/exit from each cell. This means that, even if the frequency of failure per operation (or per hour connected to the UFC docking station) is very small, the frequency of any of these accidents will be likely around 0.5 a^{-1} (making them anticipated operation occurrences).

4.5 CRITICALITY

Due to the characteristics of CANDU fuel, criticality can be ruled out. For other fuel types, such as enriched fuel from AECL, criticality has to be re-considered. CANDU reactors use heavy water because with ordinary water the chain reaction is not possible. In theory, light water reactor (uranium enriched in U-235) to be disposed of by most countries (e.g., Finland and Sweden) could, under specific circumstances, reach critical conditions. But for the CANDU fuel (natural uranium) criticality is not possible due to the low abundance of fissile isotopes.

The topic of criticality in the underground facility was studied in OHN (1994), where “analysis considered all possible arrangements and configurations that the used fuel might have in the vault. It was assumed that the vault was flooded and that the containers were full of water. In all conceivable situations, it was concluded that criticality was not possible”. The same conclusion applies to the UFPP and underground DGR. Also a newer NWMO study by Garisto et al. (2014) supports the conclusions. Here, criticality assessment was performed for 5 bounding scenarios:

1. A single intact container with intact used fuel geometry, bentonite-shielded, filled with water (flooded), and surrounded by rock;
2. A single intact container, with degraded used fuel geometry, bentonite-shielded, filled with water (flooded), and surrounded by rock;
3. A single degraded container, with degraded used fuel geometry, bentonite-shielded, where radionuclides have been released into the bentonite and rock surrounding the bentonite;
4. Radionuclides are released from multiple degraded containers (with degraded used fuel geometries) into the surrounding rock (far field); and
5. Calculation of critical volumes and masses for mixtures of plutonium in water. This scenario assesses plutonium criticality when the fissile materials are released from a container, mix with water, migrate, and potentially accumulate.

Criticality calculations were performed, with conservative burnup and decay time assumptions, for intact and degraded container scenarios. Overall, the results show that criticality is not possible. The only very unlikely case is where multiple containers must fail, releasing plutonium, which must then migrate to the same region and accumulate without other radionuclides in order to reach critical mass.

If other fuels, different from CANDU, are to be processed in the UFPP and disposed in the DGR, specific analyses should be done for them.

4.6 FIRE

4.6.1 Safety Culture and Fire Suppression

Fire detection and suppression systems will be used in the facility area.

- According to Heystee (2015), fire suppression in the DGR is done with hand-held foam based fire extinguishers mounted throughout the facility;
- Automatic, foam-based fire suppression systems mounted on all diesel equipment;
- An inert gas generator and a portable foam generator for extinguishing any fires that develop in the placement rooms;
- Normal sprinkler and/or fire hose systems for areas where appropriate;
- A water spray deluge system for hazardous environments where fires may spread very quickly or where valuable materials need to be cooled; and a water mist system for areas where appropriate.

The underground DGR concept includes refuge stations for personnel, with breathing equipment, emergency air systems, communication devices and emergency rations of food and water. Same fire suppression methods will also be used in the UFPP.

The potential for fires in the UFPP and underground DGR is minimised by design and equipment material selection. Equipment with ignition sparking potential will be fitted with fire suppression devices (automated or manual).

As there is minimal fire load, minimal igniting or sparking equipment, and fire suppression equipment with trained personnel is available, any possible fires in proximity or in contact with used fuel bundles, modules, baskets, a UFC and UFTP would be short-lived and quickly extinguished. Shielding, even if it may be heated by the fire, will remain intact, as both the UFTP and the UFC are able to withstand fires. Module and fuel handling cells have minimal fire load, so that if sparking is initiated, there is nothing to burn and suppression will suffocate any possible fire.

IAEA (2004) has compiled experiences from nuclear power plant fire incidents, and lessons learned can be summarised as follows:

- Safety culture
  - As most fires started directly or indirectly by human errors, it is necessary to maintain a good safety culture at the plant.
- Prevention
  - In several cases, a short circuit was the cause of fire. Material selection for cables and fuses should be appropriate with regard to fire safety.
  - In several cases, the insulation material itself contributed to the fire propagation. Insulation materials should be non-combustible or fire retardant.
- Detection
  - Fast detection of the fire is very important. Automatic detection and alarm systems should particularly be provided in unoccupied rooms. These systems should be reliable and be regularly tested and maintained.
- Suppression
  - Communication problems between the fire brigade and operators in the control room lead to firefighting delay. Appropriate communication means, together with emergency procedures, are necessary.
  - Manual fire suppression is often impossible due to smoke in the respective fire compartments (in particular in the turbine hall). Provisions for smoke removal are required.
- Mitigation
  - In the control room, smoke ventilation and fire barriers sometimes do not work as required because of cracks in walls and floors which are not well repaired.
  - A relative great number of hydrogen fires, mostly resulting in an explosion, occurred. Adequate provisions to prevent hydrogen fires should be taken.

Based on the review experiences, it can be said that the prevention measures seem to be the most important (IAEA 2004). In addition, since most events are due to human errors, the importance of good safety culture is highlighted.

4.6.2 Potential Fire Hazards in UFPP and Underground DGR (UFC Transfer and Placement Equipment)

The potential fire initiators were reviewed for the Mark II conceptual design.

In the UFPP, the fire hazards or potential initiators are listed below:

- electricity;
- hot work (welding);
- ignition of fuel or oil;
- sparking;
- static discharge; or
- flammable gases.

Electrically initiated fires are a potential hazard. The majority of equipment in the UFPP work on electricity (e.g., UFTP pallet/rail cart, overhead transfer crane/gantry, module and fuel handling machines), and the volume of used fuel bundles moving through the facility is large. Potential electrical fire sources are not only the equipment directly involved in the used fuel handling process, but also normal office work equipment such as printers, computers, etc. The mitigation of electrical fires is done by inspection and approval of electrical equipment. All electrical equipment in a nuclear facility is acquired from approved manufacturers, and grounded correctly. Electricity run transport/lifting equipment, which are used in the transfer of UFTP, module, used fuel, basket or UFC are:

- UFTP receiving and shipping hall OTC;
- UFTP rail cart;
- Module handling cell crane;
- Module transfer cart;
- AGV transfer system;
- Overhead transfer gantry in the processing cells;
- UFC rotary positioner on rails in the processing cells;
- Dispatch tow vehicle;
- Shaft; and
- DGR tow vehicle (which could also be diesel-powered).

In the Mark II conceptual design, Hybrid Laser Arc Welding (HLAW) has been suggested to be the reference welding method. Welding process is a remotely controlled small scale operation. In addition to the welding machine, there is other electrically operated machinery in the processing cells (e.g., machining and inspection). In principle, a fire could occur in, or propagate via, the additional in-cell equipment of the hot cell.

Due to the nature of welding process, mitigation by design features is imperative. It is, however, unlikely, that any potential fire initiated in the welding cell would damage used fuel or cause shielding failure or release of radionuclides. The metals are not combustible, in-cell fire suppression is designed, tested and maintained, and the fire load is minimal. Any ignition would be short-lived and mainly cause delay in operation for fire investigations, clean-up, and replacement of faulted equipment, testing and validation of safe process for re-launching. It is possible that due to an in-cell fire the HEPA filter could be damaged, but probability of this potential fire scenario is extremely low, especially with temperature and duration needed to cause HEPA filter failure.

Other welding work in the UFPP would occur in an active maintenance shop. This is small scale welding work performed by professionals with required work experience and certificates.

Above ground, diesel operated back-up generators (e.g., for shaft hoists) present no direct hazard that could have radiological consequences due to their location away from the UFPP. Diesel fuel storage above ground is located far enough from the UFPP to present no hazard. There is, however, a need to have underground diesel storage and refuelling station for DGR vehicles, unless all are designed in future to work on chargeable batteries or to be taken via shaft to be refuelled above ground. If an underground diesel storage fire occurs, fire safety measures will mitigate the spread of fire from the storage area and problems would arise from other health risks (such as smoke inhalation) and damage to the underground rooms than radiological reasons. Potential diesel storage in underground DGR would not be located next to UFC placement rooms. In considering battery operated vehicles and equipment, a hydrogen explosion initiated fire is possible. The risk of this is mitigated with use of an accepted supplier, good maintenance, timely battery changes and monitoring. In the battery storage area, the batteries are not kept with flammable materials; and the storage and loading areas are equipped with fire detection and suppression equipment.

Any spillage of oil and fuel is immediately cleaned, and not allowed to accumulate in places or on equipment. A fire due to this could only be caused by a vehicle accident that would, in addition to spilling, cause sparks for ignition. The vehicles within the UFPP travel at very slow speed and impacts would not initiate a fire. Mitigation of fires will include using hydraulic oils and fluids for vehicles with low flammability and on-board suppression system.

The following diesel vehicles are present in the UFPP and the underground DGR:

- UFTP transport vehicle; and
- Placement forklift in underground DGR.

Sparking can be induced with one hard object hitting another. This is possible in potential collisions in both the UFPP and underground DGR, especially if both objects are metal. Sparking alone does not cause fire, but combined with flammable material, as could be the case in vehicle collisions, if oil or diesel leak is considered, such accidents are possible. The materials and coatings can be selected to minimise sparking during collisions. Low speeds also decreases the potential for sparking.

Static discharge induced fire is not a realistic risk; in normal office and industrial work, its rarity allows this probability to be considered negligible. Static discharge can be diminished by material selection.

With DGR ventilation, a fresh air heating plant based on a direct-gas-fired heating system using burners placed directly into the airstream will accommodate winter temperatures. Direct fired heaters will consist of an intake section, burner section and air plenum. This system is located well away from the UFPP and its fire may cause ventilation failure in the underground DGR, but presents no direct radiological danger. In case of ventilation failure, all workers will be evacuated from the underground DGR.

In the underground DGR, a fire could ignite and spread due to same reasons as in the UFPP. Underground there is also potential for build-up of methane, which is discussed in Section 4.7. UFTP packages are designed to withstand fires. An assessment of a fire accident for a UFTP is provided in Appendix C of Batters et al. (2012). In tests, an empty half-scale model of the UFTP cask was dropped 9 m and exposed to one hour fire at 800°C temperature. UFTP shielding was not observed to fail in this test.

4.6.3 WIPP Vehicle Fire

In Waste Isolation Pilot Plant (WIPP) in Carlsbad, New Mexico (U.S.), a salt hauler vehicle fire occurred on February 2014 in the mine section of the facility. There were 86 people present at the onset of the fire, and all exited the mine safely. Six personnel were transported to the Carlsbad Medical Center for smoke inhalation and an additional seven personnel were treated on-site. The vehicle was the EIMCO Model 985, 15 ton haul truck, which is a diesel powered vehicle used to haul salt from the mine. It had an age of 29 years. After analysing the accident (U.S.DOE 2014), it was concluded that the fire ignited in the rear part of the vehicle, in section surrounded by steel framework, most probably by heating of accumulated grime that had not been removed in maintenance. Most significantly it was found that the safety culture of the mined section of the facility is not that of a nuclear facility, but resembles normal mining culture. The vehicle fluids were flammable; there were maintenance deficiencies and additional deficiencies in emergency and rescue training, fire extinguishing and evacuation. The burned salt hauler is shown in Figure 27.

The WIPP facility fire is a reminder of the importance of maintaining a good safety culture. As part of the detailed DGR design, it is expected that a thorough Fire Hazard Analysis will be completed to further ensure that the fire hazard is low.

Figure 27: Burned Salt Hauler Involved in the WIPP Fire

4.6.4 Potential Fires and Probabilities

In fire scenarios with impaired suppression and assumed fire spreading, the postulated event chains are long, but discussed here as illustrative examples of how a fire could spread close to used fuel. In other possible fire locations, such event chains were not postulated due to minimal fire load (e.g., hot cells and transfer and dispatch areas), but fire hazards will need to be further assessed as part of the future design development. The event chain described in Table 10 could result from problems in UFPP and underground DGR practices (extra fire load leading to unexpected spreading of fire and formation of more heat than should be possible), in quality control (vehicle and suppression device maintenance, e.g., accumulation of grime), and in emergency response training (mistakes in using equipment and/or slow response by on-site fire department).

With fires, it is possible that ventilation system or HEPA filters are damaged; but this is not considered as a separate fire incident. Ventilation failures are discussed in Section 4.2.

For the probability of a vehicle fire leading to UFTP damage (Fire1 in Table 10) and the probability of a fire leading to UFC damages (Fire2 in Table 10), the frequency has been derived from the data in U.S. DOE (2008). A scenario (nbr. 14) in U.S. DOE (2008) corresponds to a fire involving a truck transportation cask with light water reactor used fuel (with cask breach, fuel damage and radionuclide release) in the receipt area of the Wet Handling Facility. The mean number of occurrences of such a fire over the preclosure period is 2E-2 (Table E-1 in U.S. DOE 2008). Table A.1 of the same report shows that the number of truck transportation casks received at the Wet Handling Facility is about 2,650 during the whole preclosure period. With these data, a probability of 7.5E-6 fire (with cask breach, fuel damage and radionuclide release) per truck arriving to the Wet Handling Facility has been calculated. The calculation method is adapted for the UFTP transportation vehicle fire scenario (Fire1 accident scenario) and the UFC placement vehicle fire scenarios (Fire2 accident scenario).

Container damage due to a fire is considered to be far more probable for a bolted container, such as the transportation cask for Yucca Mountain and the UFTP, than for a welded container such as the Mark II UFC. As a consequence, a probability of 7.5E-6 fires (with radionuclide release) per transport is assumed for the UFTP, while for the UFC within the buffer box the adopted probability is 100 times lower, i.e., 7.5E-8 fire (with radionuclide release) per transport.

In the Mark II conceptual design, 630 UFTPs are assumed to be received annually at the UFPP. The resulting frequency of a fire with radionuclide release is estimated to be 4.7E-3 a^{-1} (Fire1 accident scenario). This scenario has been analyzed in depth in Batters et al. (2012).

Table 10: Illustrative Examples of Event Chain of Fire Scenarios Joined With Impaired Fire Suppression System and Fire Spreading

Nbr.	**Fire1 Accident Scenario**
Start description	UFTP transportation vehicle is in the UFPP receiving and shipping airlock with UFTP on board and radiation shield open.
Event 1	Vehicle catches fire (engine fire)
Event 2	Malfunction of automated fire suppression system
Event 3	Malfunction of manual fire extinguishers
Event 4	Spreading of fire from engine towards UFTP with substantial heat formation
Event 5	Burning of the impact limiter and engulfing fire around UFTP
Event 5	Fire leading to damage and release of radionuclides
Nbr.	**Fire2 Accident Scenario***
Start description	UFC within the buffer box is moved in the underground placement room using a remotely controlled forklift.
Event 1	Diesel-operated forklift catches fire in the placement room
Event 2	Malfunction of automated fire suppression system on the forklift
Event 3	Spreading of fire towards UFC with substantial heat formation
Event 4	Possible ignition of excess fire load in tunnel (materials stored in tunnel against regulations)
Event 5	Burning of the forklift and substantial heating of buffer box and UFC
Event 6	Fire leading to damage and release of radionuclides

*Assumed that no one would attempt to manually extinguish the fire in the placement room.

In the Mark II conceptual design, 2,520 UFCs per year are moved in the DGR using a diesel-operated forklift. The resulting frequency of a fire with radionuclide releases is estimated to be 1.9E-4 a^{-1} (Fire2 accident scenario).

4.7 EXPLOSION

Regarding explosions, nuclear power plant events have been included in the lessons learned study by IAEA (2004). The main initiating events are human errors. The probability of explosions can be lowered significantly by means of prevention and focusing on safety culture.

In the UFPP, Hybrid Laser Arc Welding has been selected as a reference welding system for the Mark II conceptual design, and is considered to be suitable for sealing the UFC. However, the technique is novel. There will also be minimal quantities of normal welding gases used in small welding operations in small maintenance workshop.

Gas-induced heating of inlet air into the underground DGR is in a dedicated ventilation building far off the UFPP, and though an explosion may be possible, it is not anticipated to damage the UFPP enough to induce radiological consequences.

Rechargeable batteries may present an explosion hazard for a battery-run vehicle, as a hydrogen explosion could occur due to thermal runaway and buildup of hydrogen. Mitigation of this hazard includes monitoring (possible for both temperature and hydrogen), monitored charging and replacement of aged batteries with fresh ones. The battery storage, reloading place and battery run vehicles will need to be located in rooms with ventilation and temperature monitoring. In case of ventilation failure, the room will need to constrain the temperature passively within set limits.

Diesel vehicles and diesel fuel storages, where sparking could cause more violent fires due to fumes (this would require substantial pressure and temperature in system), also present potential explosion hazards. These are discussed with potential fires in Section 4.6. The underground diesel storage and refuelling room will be designed to meet the national regulations and with sufficient ventilation and precautions to prevent buildup of explosive gases (or high flash point temperature required by diesel to ignite). The ventilation system and HEPA filters could be damaged by an explosion (or violent fume fire); failure of ventilation is discussed in Section 4.2. Explosion of a placement forklift for any given reason is not considered to cause damage to UFC both due to radiation shielding wall in the forklift (Figure 25) and the durability of the UFC.

The working assumption for this report is that no excavation occurs near the placement room and other underground spaces where operation takes place. Therefore, the storage of explosives for the excavation in the underground DGR is excluded from the current work as a potential cause of radiological release. When more detailed information is available, the hazards related to explosives will need to be evaluated.

Depending on the site, there may be gradual accumulation of explosive gases (primarily methane) from the host rock. During this time ventilation and monitoring of gas build-up is necessary. Probability of explosion due to build-up of natural gases is not considered further, as presence of hydrocarbon formations or leak of methane from surrounding rock formations into underground DGR through permeable sedimentary rock or fracture network in crystalline rock would be detected during site selection investigations and further investigations during construction, and explosion would be mitigated with monitoring and ventilation. Siting process would also screen off any site with significant hydrocarbon resource.

Explosion is also possible at battery charging stations that may be located underground. These stations are assumed to be located in such a way that the potential explosions will not cause radiological consequences to workers. Hydrogen explosion induced fires are discussed in Section 4.6.2.

4.8 INADVERTENT ENTRY SCENARIOS

Several delays in operation, which could cause longer exposure to personnel, were identified in the FMEA process. In addition, there are operation steps in both UFPP and DGR, where it is presumed that workers will not be present in a room during the operation step or that only workers assigned to the specific task are present. In rooms which are not locked, it is possible that a person could enter during an operation, should there be a malfunction in warning/locking system ("do not enter" light at door or similar) or due to operational mistake. Such accidental exposures are considered here as inadvertent entry scenarios.

Inadvertent entries are assumed to be possible only in rooms that are used by personnel in the facility. As a working assumption discussed in Section 3.3, inadvertent entries are not expected to occur in hot cells.

In the Mark II conceptual design, areas in the UFPP and underground DGR where inadvertent entry scenarios could occur are:

- UFTP shipping and receiving airlock and hall (basement);
- Intra-plant transfer hall (ground level);
- Dispatch hall in the buffer area (basement); and
- Underground DGR tunnel system when UFC is transferred from shaft/storage (less likely in placement room, since there is a shielding frame at the entrance during the placement operation).

See Figure 12. For workers in these areas, doses have been estimated for normal operation in Reijonen et al. (2014); however, additional personnel can also be exposed in these areas if they inadvertently walk into room. For these additional personnel, the doses would not exceed the dose rate calculated for workers normally in these areas. However, as this is an additional exposure that can be prevented, these inadvertent entries are considered here as abnormal operating events.

Table 11 presents the radiation sources and assumed distances and exposure times for such events for illustrative purposes. It is assumed that a worker becomes aware of the situation quickly, and stops when approaching the source of radiation. Ambient radiation is not considered in inadvertent entry scenarios, as it is assumed that all workers are aware of the places of ambient radiation and are prepared for receiving this dose when entering such area.

It is difficult to estimate a frequency for inadvertent entry accidents with the preliminary design and without detailed information on the safety equipment of the UFPP doors and access control. Therefore, this preliminary hazard identification assumes that inadvertent entry would occur more than once in 10 years.

It is expected that the additional individual doses incurred in these situations would be very small. However, inadvertent entry is kept as a potential hazard in the preliminary hazard identification, to emphasize that it is not acceptable to unnecessarily enter areas with even slightly elevated radiation doses.

Table 11: UFPP and Underground DGR Inadvertent Entry Scenarios as Illustrative Examples

No.	Inadvertent Entry Scenario	Source	Assumed Distance to Sources (m)	Assumed Exposure Time (min)
II-IE1	Entrance into UFTP shipping and receiving airlock, when radiation shield is open and UFTP is on vehicle or being lifted by OTC	UFTP	3	5
II-IE2	Entrance into UFTP shipping and receiving hall, when UFTP is being lifted by OTC in the hall near storage area	UFTP + UFTP storage	30 m to UFTP + 30 m to UFTP storage	5
II-IE3	Entrance into UFTP shipping and receiving hall, when UFTP is being lifted by OTC in the hall for impact limiter removal	UFTP + UFTP storage	30 m to UFTP + 30 m to UFTP storage	5
II-IE4	Entrance into transfer hall, at processing cell end, when UFC is in transfer flask	UFC in transfer flask	3	5
II-IE5	Entrance into transfer hall, near AGV parking, when UFC is in transfer flask	UFC in transfer cask	5	5
II-IE6	Entrance into dispatch hall, when the UFC buffer box is in transport cask	UFC buffer box in transport cask + UFC buffer box storage	20 m to UFC buffer box + 20 m to UFC buffer box storage	5
II-IE7	Tow vehicle driven by worker next to route to placement room	UFC buffer box in transport cask	2	5

4.9 FLOODING AND LEAKAGES (WATER AND GAS)

Water pipes can potentially leak resulting in internally initiated flooding. It is assumed that wet storage is not required because all fuel received at the UFPP will be sufficiently cool for dry storage (Section 3.2.1 of Heystee 2015). Use of gas in any of the processes could also lead to gas leakage.

Internal flooding can be caused by a fire suppression system failure (sprinkler system), water pipe rupture, and rupture of smaller scale water tanks, which may be utilised especially in underground DGR. As mentioned in Section 3.3, there will be no water pipes present that could break and cause flooding in the hot cells. The excavation will most likely be done as a step-wise process, panel by panel. Since the excavation would occur in any case far from the areas where placement operation is ongoing, water sources for tunnel excavation near the underground DGR operation can be excluded. However, this needs to be addressed in the future, when more detailed plans are available on the step-wise operation.

A sprinkler system will be designed to be installed in appropriate locations, away from any radiation source. Any water flooding from maintenance work or personnel rooms (e.g., kitchens, toilets) will have no impact on radiological safety, but may damage building components). In DGR radiation zones, the potential internally induced floods are relatively small. DGR will have safety monitoring factors (e.g., floor sumps, isolation valves in the water lines). Without details on how water will be brought into DGR, it is assumed that permanent water lines are not needed in the radiation zones.

These flooding accidents are mitigated by structural design and monitoring. Construction of the UFPP could include underground draining pipes to sump storage, which can help monitor any leaking water. Possible internal flooding is taken into consideration in design, so that any sprinkler or pipe water that could leak would not be near the radiation source.

Extended loss of power could lead to loss of sump pump capacity and eventual underground flooding. However, as the used fuel is within sealed containers and in most cases within sealed rooms, there would be no radiological consequence.

Externally initiated flooding is discussed in Section 5.6.

In the Mark II conceptual design, compressed gas is used in cold spray cell and is connected to a N_2 tank. Gas tanks are fitted with appropriate safety device, providing slow release of gas in the hot cells in case of line breakage (as discussed in Section 3.3). Controlled release of these gases is not assumed to lead to any hazard that would have radiological consequences.

4.10 COMBINATIONS OF INITIATING EVENTS (POSTULATED EVENT CHAINS)

In FMEA, the accident scenarios are identified by a single initiating event. However, a combination of initiating events is possible. Most combinations are not credible in terms of frequency, unless they have a common cause. The identified event chains include drop scenarios with impaired or deficient protection by the UFTP or UFC. General failures listed in Sections 4.2 to 4.9 are such that they can take place at the same time with any identified events in the FMEA process.

The drop scenarios with impaired or deficient protection by UFTP or UFC are considered with more severe consequences than what would follow if scenario would occur with intact and properly manufactured and closed UFTP or UFC. In these occasions, a drop that would otherwise not cause damage to an intact UFTP or UFC is assumed to cause radiological consequences due to an undetected major flaw in the package (UFTP, UFC, or UFC in transfer cask/transport cask), either due to wearing of UFTP or transfer flask/transport cask or a flaw in production . In the Mark II conceptual design, there are seven accident scenarios identified (Table 12).

Table 12: Event Chains of Dropping of Undetected Flawed UFTP or UFC

No.	Process Step in Appendix B	Failure Mode	Joined Flaw in Shielding	Consequence
II-DF1	Move UFTP from transport trailer into UFTP storage or on transfer pallet in the UFTP receiving and shipping hall with 40 tonnes OTC (Step 8)	OTC fails and UFTP is dropped (maximum 5 m)	UFTP is flawed and this has not been discovered in inspection and packing	UFTP is damaged and radiation is released
II-DF2	Move UFTP from storage to transfer pallet using OTC (Step 9-3)	OTC fails and UFTP is dropped (maximum 5 m)	UFTP is flawed and this has not been discovered in inspection and packing	Release of some radionuclides but no loss of shielding (fuel damage)
II-DF3	Grip loaded UFC using overhead transfer gantry to the rotary positioner in weld cell or copper application cell (Step 65-1 or 65-38)	Overhead transfer gantry fails and UFC is dropped (maximum 2 m)	UFC is flawed and this has not been discovered in inspection	Release of some radionuclides but no loss of shielding (fuel damage)
II-DF4	Grip loaded UFC using overhead transfer gantry from the rotary positioner in weld cell or copper application cell (Step 65-30 or 65-68)	Overhead transfer gantry fails and UFC is dropped (maximum 2 m)	UFC is flawed and this has not been discovered in inspection	Release of some radionuclides but no loss of shielding (fuel damage)
II-DF5	Place UFC on the bottom half of the buffer box using OTC (Step 75)	Lifting tool fails and UFC is dropped (maximum 2 m)	UFC is flawed and this has not been discovered in inspection	Release of some radionuclides but no loss of shielding (fuel damage)
II-DF6	Transfer buffer box to buffer box transfer area using OTC (Step 78)	OTC fails and buffer box is dropped on the floor, and buffer assembly is ruptured (maximum 2 m)	UFC is flawed and this has not been discovered in inspection	No loss of shielding, UFC in buffer box
II-DF7	Lift assembled buffer box by OTC to dispatch hall in the basement for transfer underground or stored in laydown area (Step 81)	OTC fails and buffer box is dropped on the floor or on the dispatch vehicle (maximum 5 m)	UFC is flawed and this has not been discovered in inspection	Damage to fuel, release of radionuclides, UFC in damaged buffer box

Note: DF = Drop/Fault

Considering UFC shielding failure, it is not considered possible that a UFC could be dispatched to the DGR with a defect that would result in constant leaking of radiation. It is considered, however, that there may have been a defect in a UFC and human error in non-destructive testing investigations where integrity is verified, and these flaws could result in radiological consequences joined with dropping scenario, as mentioned in the beginning of this section. The severity of the dropping scenarios depends on the maximum potential height of the drop. These are indicated for each accident scenario in Table 12.

For these combined scenarios, a probability is needed for:

- a UFTP/UFC with defect that has not been detected in the QA/QC controls; and
- the transfer cask will have had a flaw in preparation or a defect that has gone undetected in QA controls.

OPG (2001) concludes that about 2 out of every 10,000 UFCs can be expected to present undetected fabrication defects. Hence, the probability for a given UFC to be defective is 2E-4, and this value has been adopted in this report for the Mark II UFCs. Any drop of a flawed UFC could lead to UFC breach, fuel damage and radionuclide release. However, when the UFC dropped is inside a transfer flask/transport cask, it is assumed that the probability of breach of UFC and cask is reduced by a further factor of 1E-2. Probability of a defective UFTP is assumed to be 1E-3.

The frequency per lift of this class of accidents is obtained as the product of the drop frequency times the fraction of defective UFTPs/UFCs times the probability of transfer cask failure (if applicable). Since the estimated drop frequency is 5.0E-5 drop/lift (Section 4.1.2.4), the resulting frequency of drop with breach and radionuclide release is 1.0E-8 per lift for UFC and 5.0E-8 per lift for UFTP. In case of UFC being inside a transport cask, the frequency falls to 1.0E-10 per lift. These accident frequencies per lift seem very small, but the great number of lifts in the UFPP every year leads to relatively high annual frequencies. The potential event chains are presented in Table 12. These chains can be further combined to two combined failure modes describing the accidents and for assessing their probabilities. The two resulting combinations with estimated annual frequency are presented in Table 13.

Table 13: Combined Failure Modes of Event Chains (Fall of an Undetected Flawed UFTP or UFC) and Frequencies

Frequency of the Combined Failure Modes of Event Chains
EC1. Fall of an undetected flawed UFTP in the UFTP shipping and receiving hall
In the Mark II conceptual design, 630 UFTPs are received annually. Each UFTP is lifted twice, with full used fuel load (from the transport trailer to the storage and from the storage to the transfer pallet for processing) leading to 1,260 lifts a^{-1}. The frequency for UFTP fall with breach and radionuclide release is 6.3E-5 a^{-1}.
EC2. Fall of an undetected flawed UFC in a welding cell, a copper application cell or the UFC buffer box loading cell In the Mark II conceptual design, 2,520 UFCs will be produced annually. The FMEA table (Table 12) identifies 5 operations in which the UFC can be dropped, but operations II-DF3 and II-DF4 are performed twice (one in the weld cell and other in the copper application cell) and hence there are 17,640 lifts per year that could lead to UFC damage. Using the recommended frequency of 5E-5 drop/lift, the frequency of UFC drops is 8.8E-1 a^{-1}. Assuming that the probability of the UFC being flawed is 2E-4, the resulting frequency for this accident is 1.8E-4 a^{-1}.

Note: EC= Event Chain

4.11 SUMMARY OF INTERNAL INITIATING EVENTS AND ACCIDENT SCENARIOS

Several potential hazards were identified arising from both the operation process itself and from the facility design. For completeness, event chains considering flawed fuel packages combined with the potential drop scenarios were also postulated. To identify the meaning of these failure modes for the design and their role in possible design iteration, two aspects need further notice: the probabilities of the identified hazards and the potential radiological results of these hazards. The considerations of the probabilities have been included in Sections 4.1 - 4.10. Table 14 summarizes the postulated failure modes due to internal initiating events and associated accident scenarios, which can be taken forward from this identification phase to be binned as an Anticipated Operational Occurrence (AOO), Design Basis Accident (DBA) or a Beyond Design Basis Accident (BDBA).

Table 14: Summary of Internal Initiating Events and Postulated Accident Scenarios

Internal Initiating Event	Failure Mode	Accident Scenario Leading to Radiation Exposure*	Accident Grouping
Operation derived accident leading to prolonged operation and additional radiation dose to personnel (Table 8)	1. Tie-down detachment problems	1. Tie-down detachment problems leading to prolonged operation	AOO (Table 8)
	2. Weather cover opening problems	2. Weather cover opening problems leading to prolonged operation	
	3. Smear test failure	3. Failed smear test leading to prolonged operation	
	4. Vent cell inspection equipment failure	4. Vent cell inspection equipment failure leading to prolonged operation	
	5. Overhead transfer crane/gantry failure	5. Overhead transfer crane/gantry failure leading to prolonged operation	
	6. Electrical door failure in process line	6. Electrical door failure leading to prolonged operation	
	7. Pallet on rail / rail cart / flask trolley on rails	7. Pallet on rail / rail cart / flask trolley on rails malfunctions causing prolonged operation	
	8. Tow vehicle	8. Tow vehicle / locomotive malfunction leading to prolonged operation	
	9. AGV system failure	9. AGV system malfunction leading to prolonged operation	
	10. Vent equipment malfunction	10. Vent cell equipment malfunction leading to prolonged operation	
	11. Attachment / detachment problems (UFTP lid)	11. Attachment or detachment problems with UFTP lid leading to prolonged operation	
	12. Attachment / detachment problems (UFTP, disposal process vehicles and equipment)	12. Attachment / detachment problems with UFTP, disposal process vehicles and equipment,leading to prolonged operation	

Internal Initiating Event	Failure Mode	Accident Scenario Leading to Radiation Exposure*	Accident Grouping
	13. Disposal process equipment failure (buffer box)	13. Problems or malfunctions with buffer box equipment or process leading to prolonged operation or renew operation	AOO (Table 8)
	14. Disposal process equipment failure (underground)	14. Problems with underground installation equipment leading to prolonged operation	
Operation derived accident leading to release of radionuclides (Table 9)	FMEA number II-16-1	15. Fall of the elevator while transferring an UFTP (without impact limiter and with loose lid) down to the basement	DBA (Table 9)
	FMEA number II-17.2	16. Dropping of an UFTP lid on UFTP when it is being lifted in the module handling cell	AOO (Table 9)
	FMEA number II-19-2.2	17. Fall of a module during transfer in the module handling cell, during transfer to dry storage, or during transfer from laydown area onto an inter-airlock trolley	
	FMEA number II-19-3.2		
	FMEA number II-19-6.2		
	FMEA number II-19-7.2		
	FMEA number II-31.2		
	FMEA number II-32.2		
	FMEA number II-33.2		
	FMEA number II-33.3		
	FMEA number II-35.2	18. Fall of a module in the distribution hall	
	FMEA number II-36.1	19. Fall of an empty module on full module during transfer to dry storage area	
	FMEA number II-38-1.2	20. Failure of scissor lift during alignment of a module tube for pushing, leading to falling of module/fuel bundles on floor	DBA (Table 9)
	FMEA number II-38-5.2	21. Forcing of fuel bundles to basket locations with fuel already in, leading to breaking of bundles	AOO (Table 9)
	FMEA number II-38-5.3	22. Mis-alignment of basket in fuel transfer machine, leading to pushing of the fuel bundles onto floor	
	FMEA number II-90.1	23. Fall of the shaft cage while transferring UFC underground (high fall scenario)	BDBA (Table 9)
Ventilation and filtration system failure (Section 4.2)	UFPP/DGR HEPA filter system failure	24. UFPP/DGR HEPA filter system failure	AOO** (Section 4.2)
Power failure (Section 4.3)	N/A	Non-credible to cause radiological results	-

Internal Initiating Event	Failure Mode	Accident Scenario Leading to Radiation Exposure*	Accident Grouping
Shielding failure (Section 4.4)	Failure of the connection of the UFC transfer flask with the weld or copper application cell	25. Gap in the connection of the UFC transfer flask with the weld or copper application cell, leading to additional worker dose	AOO (Section 4.4)
Criticality (Section 4.5)	N/A	Not credible	-
Fire (Table 10)	Fire1	26. UFTP transport vehicle fire leading to UFTP damages	DBA (Section 4.6.4)
	Fire2	27. UFC placement vehicle fire	
Explosion (Section 4.7)	N/A	Non-credible to cause radiological results	-
Inadvertent Entry (Table 11)	II-IE1 to II-IE7	28. Inadvertent entry to rooms with operation process, leading to additional worker dose	AOO (Section 4.8)
Flooding and leakages (water and gas) (Section 4.9)	N/A	No radiological consequence	-
Postulated event chains of flawed UFC/UFTP and a drop scenario (Table 13)	EC1. UFTP drop in the UFTP shipping and receiving hall	29. Fall of an undetected flawed UFTP in the UFTP shipping and receiving hall	DBA (Table 13)
	EC2. UFC drop in a welding cell, a copper application cell or the UFC buffer box loading cell	30. Fall of an undetected flawed UFC in the welding cell, or copper application cell or UFC buffer box loading cell	

* Accident scenarios are numbered together with accident scenario names.

** HEPA filter failure does not lead to release of radionuclides; but if it happens during accidents with radionuclide releases, it can increase the releases outside UFPP/DGR.

5. EXTERNAL INITIATING EVENTS

The NWMO Mark II conceptual design is currently in the development phase, and site selection is not completed. This hampers the possibility to conclusively include site-specific external events that could initiate an accident. In this report, the external events are derived taking into account operational safety assessment data from the following:

- OPG proposed DGR for LILW (Chapter 7 of OPG 2011)
- Used fuel DGR concept (Chapter 6 of OHN 1994)
- Western Waste Management Facility, Pickering Waste Management Facility and Darlington Waste Management Facility (OPG 2006a, OPG 2007, OPG 2006b)

Information from these documents is compared to external events considered in IAEA (2003) to confirm completeness (Table 15).

In consideration of external events, an emphasis is also on the current conceptual design, where the main shaft is separated from the UFPP. The rail system from the UFPP into the main shaft building is a tunnel-like reinforced concrete building itself, with adequate strength to meet potential stresses induced by the environment. It is referred to as the covered rail line in this preliminary hazard identification. Facility layout is in given in Figure 28, with area descriptions given in Table 16 (Heystee 2015).

Table 15: Comparison of the External Hazards Discussed in This Report to International IAEA Guidelines

NWMO (This Report)	IAEA 2003 (Corresponding Event)	Note
Severe rainfall (including thunderstorms)	Extreme meteorological conditions (temperature, snow, hail, frost, subsurface, freezing, drought)	See Section 5.1
Severe snow/ice (including adverse road conditions)	Extreme meteorological conditions (temperature, snow, hail, frost, subsurface, freezing, drought)	See Section 5.2
Severe wind	Extreme meteorological conditions (temperature, snow, hail, frost, subsurface, freezing, drought)	See Section 5.3
Lightning strike	Lightning	See Section 5.4
Tornado, tornado-generated missile	Cyclones (hurricanes, tornadoes and tropical typhoons)	See Section 5.5
Flooding	Floods (from tides, tsunamis, seiches, storm surges, precipitation, waterspouts, dam forming and dam failures, snow melt, landslides into water bodies, channel changes, work in the channel)	See Section 5.6
External fire	Fire generated from off-site sources (mainly for its potential for smoke and toxic gas production)	See Section 5.7
Aircraft crash	Aircraft crashes	See Section 5.8
Meteor impact	Excluded	See Section 5.9

NWMO (This Report)	IAEA 2003 (Corresponding Event)	Note
Earthquake	Earthquakes	See Section 5.10
Rail line blast or Toxic/Corrosive chemical rail line accident	-	See Section 5.11
Criticality due to flooding	-	See Section 5.12
Vault cave-in	-	See Section 5.13
-	Explosions with or without fire, originated from offsite sources and on-site (but external to safety related buildings), like storage of hazardous materials, transformers, high energy rotating equipment	See Section 4.7
-	Release of hazardous gas (asphyxiate, toxic) from off-site and on-site storage	Not relevant. No such storage on-site. Assumed no near-by off-site storages.
-	Release of corrosive gas and liquids from off-site and on-site storage	Not relevant. No such storage on-site. Assumed no near-by off-site storages.
-	Collision of ships and floating debris (ice, logs, etc.) with the water intakes	Not relevant.
-	Electromagnetic interference from off-site (e.g. from communication centers, portable phone antennas) and on-site (e.g. from the activation of high voltage electric switch gears)	Not relevant. Assumed that the selected site avoids these.
-	Combination	With very improbable events, combinations of external events are even more improbable. Events leading to other events have been identified in some cases (e.g. tornado leading to aircraft crash).
-	Landslides and avalanches	Not relevant. Site with potential landslides/ avalanches is not to be selected.
-	Volcanism	Not relevant. Site near volcano is not to be selected.

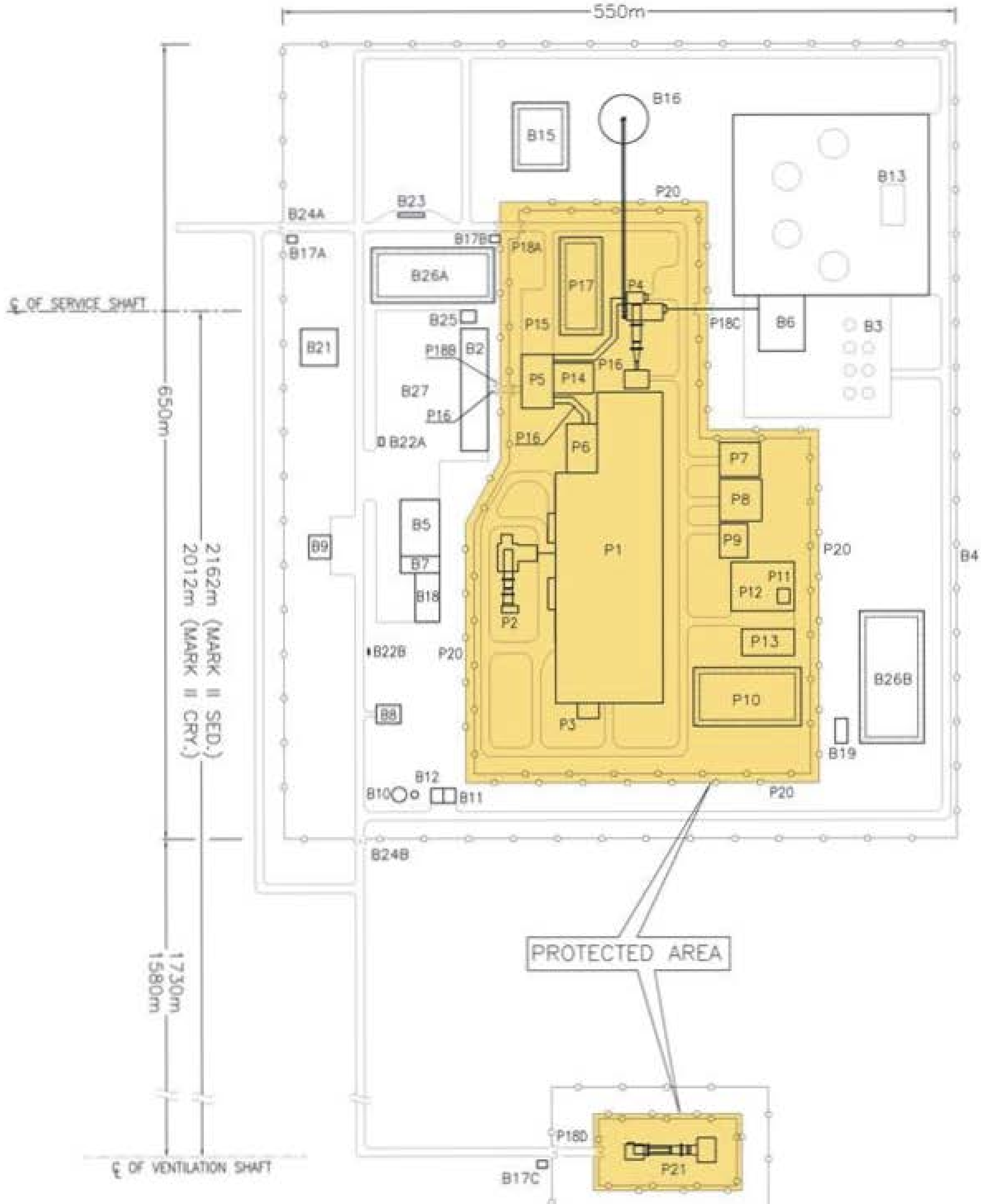


Figure 28: Layout of Facility Area

Table 16: Facility Area Description for Figure 28

Area	Protected Area	Area	Balance of Site
P1	Used Fuel Packaging Plant	B1	Waste Rock Management Area (WRMA)*
P2	Main Shaft Complex	B2	Administration Building including Fire Hall and Cafeteria
P3	Stack	B3	Sealing Material Storage Bins
P4	Service Shaft Complex	B4	Perimeter Fence
P5	Auxiliary Building	B5	Garage
P6	Active Solid Waste Handling Facility	B6	Sealing Materials Compaction Plant
P7	Waste Management Area	B7	Warehouse and Hazardous Materials Storage Building
P8	Active Liquid Waste Treatment Building	B8	Air Compressor Building
P9	Low-Level Liquid Waste Storage Area	B9	Fuel Storage Tanks
P10	Stormwater Management Pond	B10	Water Storage Tanks
P11	Switchyard	B11	Water Treatment Plant
P12	Transformer Area	B12	Pump House
P13	Emergency Generators	B13	Concrete Batch Plant
P14	Quality Control Offices and Laboratory	B14	Not Used
P15	Parking Area	B15	Process Water Settling Pond
P16	Covered Corridor / Pedestrian Routes	B16	Excavated Rock Stockpile
P17	Mine Dewatering Settling Pond	B17	Guardhouses (B17A, B17B & B17C)
P18	Security Checkpoints (P18A, P18B, P18C & P18D)	B18	Storage Yard
P19	Not Used	B19	Sewage Treatment Plant
P20	Double Security Fence	B20	WRMA Stormwater Management Pond*
P21	Ventilation Shaft Complex	B21	Helicopter Pad
		B22	Bus Shelters (B22A & B22B)
		B23	Weigh Scale
		B24	Security Checkpoints (B24A & B24B)
		B25	Security Monitoring Room
		B26	Stormwater Management Ponds (B26A & B26B)
		B27	Parking Area

*Refers to off-site facilities

5.1 SEVERE RAINFALL (INCLUDING THUNDERSTORMS)

Severe rainfall includes rainfall from storms, hurricanes, and constant enduring rain. The facility area will be designed to withstand extensive rainfall with potential soil erosion due to forming streams. The facility will be designed for the probable maximum flood, defined before detailed design stage. Storm waters are gathered in ponds on the premises and sediment settling is facilitated in the ponds. The ponds and flood control facilitate monitoring of retained water and controlled release observing the environmental aspects. The annual precipitation rate and local maximum precipitation depend on the selected site and cannot be estimated beforehand.

If the site is located in areas of large topographical variation, the possibility of rainfall in higher elevations could result in flash flooding at the lower elevation would be considered in the design of the facility. Possibility of DGR flooding due to severe rainfall and a hurricane is discussed in Section 5.6.

Severe rainfall in facility area is not considered to cause hazards leading to radiological consequences.

5.2 SEVERE SNOW/ICE

The potential for severe snow or ice to initiate an accident causing UFPP roof collapse is mitigated by structural design taking into account the maximum loads (with safety margins). Maintenance of the facility is imperative and substantial snow loads can be removed from roofs as normal winter maintenance. Severe snow or ice conditions may cause hazards to traffic entering the facility; but within the buildings, this is excluded as an unlikely initiating event (consideration of traffic into the facility is excluded from the scope of this study). Possibility of DGR flooding due to severe snow/ice is discussed in Section 5.6.

Severe snow or ice in facility area is therefore not considered to cause hazards leading to radiological consequences.

5.3 SEVERE WIND

Severe wind is caused by storms, hurricanes and tornadoes. Surface structures constructed at the site will meet all building code requirements including those for wind load. Wind speeds above the design basis may cause damage, but complete failure of the building is unlikely. The primary effects on the UFPP and main shaft building include local failure, e.g., window breakage, loss of roof panels, water penetration of the building, flying debris hitting buildings, and traffic stoppage into the facility during these weather conditions. However, the building design prevents severe damage to used fuel shielding structures within the building (thick shielding walls, durable UFTPs and UFCs).

Severe wind in facility area is, therefore, not considered to cause hazards leading to radiological consequences.

5.4 LIGHTNING STRIKE

Lightning strikes are common in thunderstorms. Lightning striking the facility is possible, especially the headframe structure. However, all surface structures will be designed with lightning protection with a grounding network.

Lightning strike damage to the UFPP, covered rail line and main shaft building is limited and potential effect would be power failure (discussed in Section 4.3). Possible fires would be suppressed by on-site fire detection and suppression system before radiological safety could be affected. See Section 4.6 for potential fire scenarios in UFPP.

5.5 TORNADO, TORNADO GENERATED MISSILE

Tornadoes are localized severe wind events. Therefore, it is difficult to estimate this potential risk before site selection process is completed.

Tornados can occur in southern Ontario (OPG 2011), though they are unlikely events; they are rare in all Canada. A typical southern Ontario tornado has ground touch of approximately 20 minutes and a width of 150-600 meters. For example, based on the UFPP and main shaft building footprint of approximately 0.02 km^2 (about 88 m x 254 m for UFPP and from Figure 28), and the annual frequency of approximately 1 tornado per 10,000 km^2 in Southern Ontario (OPG 2011), it is not likely for the UFPP and main shaft building to be hit by a tornado in southern Ontario.

As discussed with severe wind, projectiles present the greatest hazard. The shielding structures are very thick and can endure tornado wind force, but operation would cease and damage outside the facility may occur. It is not considered possible that a tornado would cause a radiological hazard within the UFPP, covered rail line and main shaft building. Building design is such that potential projectiles do not have a direct line from outside the UFPP through glass windows to lead glass windows of the hot cells. Some damage to building(s) may be caused by tornado generated missiles, but without radiological consequences. A tornado could cause damage to external infrastructure and power transfer, which could lead to loss of power, which is discussed in Section 4.3. IAEA (2003) notes also a possibility of tornado causing small air craft crash, which is discussed in more detail in Section 5.8.

Tornadoes in the facility area are, therefore, not considered to cause hazards leading to radiological consequences.

5.6 FLOODING

Flooding initiated by an external event could occur due to:

- Rainfall (including thunderstorms and hurricanes);
- Severe snow/ice;
- Flash flooding;
- Rise of sea/lake water;
- Disturbance in river flow;
- Tsunami;
- Increased groundwater inflow at DGR due to, e.g., earthquake; and
- Potential cracking of upper portions of the shaft liners (where there tends to be more permeable rock) due to major earthquake, causing groundwater to enter the shafts.

Frequency estimates concerning flooding should be site-specific. As site selection has not been completed, the discussion below derives mostly for facility design and general information concerning any environment specifically for Canada.

As discussed in Section 5.1, stormwater ponds are used to mitigate the effects of flooding. The drainage system of the facility is designed to guide the water away from the critical structures and DGR entrances/exits. Heavy rainfall caused by a hurricane could flood the DGR and erode clay materials from around UFCs; however, underground DGR and UFPP are designed for the probable maximum flood, which will be defined before detailed design stage.

Flooding that could cause radiological consequences by severe snow/ice is not considered possible. Gathered ice and snow can be removed from DGR entrance and critical buildings/structures.

Flash flooding caused by topographical differences next to the site can be caused by rain on an elevated location or melting of ice and snow higher on an elevation location. Geographical indicators for flash floods are clear and mitigating factors are, if necessary, included in surface water management system.

It is possible that the selected site is near a waterfront: lake or large river. Seafront locations are excluded in the Canadian program. With rivers, a possibility of a downstream hazard that could cause a dam to form could re-direct river flow and flood flat areas upstream. A hurricane induced temporary water rise is observed with tropical hurricanes. In addition, seiches are noted as potential causes of flooding around larger water bodies.

These flooding aspects are kept in mind during site selection and included in design of the facility area (common practice in design basis of locating safety relevant systems and components above the maximum flood level, see e.g., IAEA 2003).

Tsunamis are generated by earthquakes (Section 5.10). Potential locations of tsunami induced accidents are at coastal areas, and it is improbable (below BDBA threshold) to consider a tsunami in the Great Lakes. Even if lake conditions could form a tsunami due to improbable case of a large enough earthquake, the effect would be mitigated with design features. The stress tests of nuclear facilities such as done after the Fukushima accident in 2011 to mitigate similar incidents, could be included here prior to the start of operation. A major hazard in a potential tsunami would be, in addition to water flowing into site, debris; in the case of Fukushima tsunami this included ships, vehicles and building parts. Such a disaster would cause substantial harm to the facility infrastructure and smaller buildings, but UFPP, covered rail line and main shaft building should endure this with only some damage to the exterior parts. As discussed in the beginning of the paragraph a tsunami at Great Lakes is qualitatively considered to be below BDBA threshold.

Major earthquake could cause cracking of upper portions of the shaft liners where there tends to be more permeable rock, resulting in the groundwater entering the shafts. For these scenarios, the underground DGR could be completely flooded, potentially resulting in erosion of backfill and buffer material around the UFCs in their allocated placement rooms. In addition, workers who may have to go into rooms to possibly remove gap fill, retrieve buffer boxes, and to repack UFCs in new buffer boxes may be exposed.

Of the above, external events that could initiate flooding in the facility are massive hurricane, water level rise, tsunami, and possibly earthquake/cave-in. To give an example of how seismic movements can affect the inflow rates in underground spaces, the observations of the consequences of the 2011 Tohoku earthquake (in Pacific coast of Japan) on the local hydrology at Mizunami URL (MIU) in Central Japan are briefly discussed. Groundwater pressure changes were observed around MIU in 15 boreholes (Niwa et al. 2012). In boreholes further than 1 km away from MIU a drawdown was observed. In contrast, in boreholes within 500 m radius of MIU earthquake caused increase in heads. At MIU, soon after the Tohoku earthquake inflow volume of groundwater increased more than 10%. These observations show that the responses are related to tectonic setting and spatially variable contraction/dilation. The effects of the earthquakes on local groundwater inflows can be mitigated by site selection. MIU is an example of a location of very high inflow rates (not potential site for waste disposal).

Other events listed above can be mitigated. In cases when mitigation of potential damage to UFPP is effective, these events do not cause damage to DGR. Increase inflow due to earthquake or cave-in can also be mitigated by site selection and design.

For mitigation of large scale flooding events, the following are included:

- The site will be far enough inland to avoid any potential lake/sea flooding.
- Site is selected to have suitable hydrogeological conditions.
- Possible temporary water level rises will be included in stress test of the facility and flood control systems.

The only flooding event considered to have sufficient potential to cause radiological consequences is a hurricane, which could generate severe rain, flood underground rooms; the inflow water could potentially erode part of the backfill and buffer material off, leave UFCs exposed, and expose workers to increased radiation. Major earthquakes causing potential cracking of the shaft liners are considered under Section 5.10. Flooding of the facility area above ground level is not considered to cause hazards leading to radiological consequences for workers or public. These scenarios are considered very unlikely as the UFPP and underground DGR will be designed for probable maximum flood and to withstand a National Building Code of Canada seismic event, defined before detailed design stage.

5.7 EXTERNAL FIRE

External events that could cause a fire evolving to induce radiological impacts are scarce. Malevolent acts are excluded and considered with the security planning of the facility.

Forest fires were discussed in OPG (2011). With the used fuel disposal facility, the site selection process is not yet complete and the proximity of forest is not known. It is therefore considered possible, although with low probability, that a large scale forest fire could reach the facility. With a massively spreading forest fire, the facility perimeter may be affected and the fire could sweep across the facility area. DGR would remain mostly unaffected and suffer damage only to entrance equipment and structures, but buildings above ground could be severely damaged from the outside. The interior would be less affected and shielding structures would remain intact. Underground, the ventilation could fail. The forest fire scenario is mitigated by using concrete structures. It is possible to design the facility area, with minimum amounts of combustible materials such that fires would not spread. Nuclear facility areas are usually kept with limited vegetation and surrounding security area around perimeter fence has good visibility and clearance of vegetation (common practice, see e.g., IAEA 2003). Potential of forest fire is also limited due to precipitation rates in many parts of Canada. Small forest fires with limited duration are likely possible near the site; however, these are not anticipated to have any significant adverse impacts on the facility.

A vehicle crash within the disposal facility area is probable, but is most likely limited to accidents with personnel vehicles during normal commuting. The speed is limited in the facility area and a good safety culture allows no speeding. The area will have zero tolerance concerning alcohol and other intoxicant abuse, which lowers the probability of traffic accidents. A potential for a large-scale vehicle fire arise from diesel truck accidents. Due to low speed, this would only be possible due to poor maintenance or undetected flaw in the truck. Diesel truck accidents leading to fire are not common and the usual tanker truck accident leads to spilling of contents rather than explosion/fire. In case of fire, the consequences would not cause damage to interior of the UFPP, covered rail line and main shaft building. There are buildings (garage and storage building) between main shaft building and fuel tanks to provide cover in case of a fire (Figure 28).

External fire reaching the facility area is therefore not considered to cause hazards leading to radiological consequences for workers or the public.

5.8 AIRCRAFT CRASH

Since the site selection process is on-going, it is not yet known whether there is an airport, commercial or military, near the disposal facility. It can be assumed that there is at least several kilometers to the nearest airport. An accidental crash of a large airplane is unlikely. A small, privately owned aircraft crash is more probable.

As the distance to an airport(s) and local aviation rates are not known, the frequency of an aircraft crash is presented here according to OPG (2011) for OPG's DGR for low and intermediate level waste in the Bruce region. The aircraft crash frequency was estimated using DOE approach (2006) based on:

- Number of flight operations in area;
- Probability that an aircraft will crash during a flight operation; and
- Conditional probability that the aircraft crashes into the facility.

The annual frequency of aircraft crash was estimated to be around 4E-8 (OPG 2011). This is a preliminary value showing that the aircraft crash is improbable, but an appropriate value will need to be determined after site selection is completed.

5.9 METEORITE IMPACT

It is not credible that a large meteorite with capacity to damage concrete structures of the facility, would hit the UFPP, covered rail line or main shaft building, or hit ground with such force that underground room would collapse or be damaged. The approximate footprint of the UFPP and the main shaft building is relatively small (about 0.02 km^2). The likelihood of meteorite impact has been considered to be very low (upper annual limit is 1E-7) and IAEA (2003) excludes the event in its strategy design for surface nuclear facilities. It has been discussed in Posiva (2012) that regarding underground spaces, especially repository depths (several hundreds of meters) the likelihood is even smaller, since the meteorite causing damage would have to be so large that the consequences for the surrounding population would be greater concern from the meteorite impact than the damage to the underground repository.

Since meteorite impact has been screened out both considering surface facilities (operational) and underground DGR (even regarding long term safety), it is not considered here as a potential hazard.

5.10 MAJOR EARTHQUAKE

It is likely that the site selected will have very low seismic activity. For example, at the Bruce nuclear site, which is located within the tectonically stable interior of the North American continent, no earthquake exceeding magnitude 5 has been observed in the regional monitoring area in 180 years of record (NWMO 2011). Consideration of historical data, seismotectonics and overall geology of the site should provide enough information for site selection regarding the potential seismic hazard. Site selection criteria can diminish the potential for major earthquakes but it is probable that small seismic events will occur in the facility area during construction and operation. All buildings and structures will be designed to withstand a National Building Code of Canada (NBCC) seismic event, but major earthquake may cause some damage underground. (A major earthquake is defined here to be a seismic event larger than event specified in the NBCC). These events could cause rock fall/burst from vault, vault collapse, or cracking of the shaft liners resulting in groundwater entering the shafts. Vault cave-in is discussed in Section 5.13 and flooding in Section 5.6.

Posiva (2012) has discussed the impact of earthquakes on their repository. Both closed and open underground openings are discussed. As a general conclusion it is stated that backfilling of the underground spaces increase the stability of the host rock formation; however, the effectiveness depends of the definition of the step-wise operation for the APM concept. Open tunnels and boreholes have been studied in relation to earthquake induced damage. The data from Kamaishi underground research laboratory (fractured granite) (Shimizu et al. 1996) shows that the ground acceleration from earthquakes recorded in the underground research laboratory rapidly drop as a function of depth. Similar patterns have been observed also from Hosokura mine in sedimentary environment (JNC 2000) as well as in studies performed after Tohoku-Oki earthquake in 2011 (Ide et al. 2011 and NIED 2011). Despite this, the open spaces remain more prone to earthquake damage than backfilled spaces (see discussion in Posiva 2012). In addition to external earthquakes, it is also possible that the excavation operation itself can initiate earthquakes that lead to collapse. This has been studied in detail at 400 m deep Beaconsfield Gold Mine in northern Tasmania (Melick 2007), where in 2006 one miner died in such an event. However, regarding the APM concept, it is likely that earthquake induced events can be mitigated by good design and knowledge of local stresses in rock.

Based on the above discussion, the occurrence of an earthquake in facility neighbourhood is not considered to cause hazards leading to radiological consequences either in the UFPP or underground DGR. After site selection a more realistic estimate of the earthquake frequency can be estimated. In addition, the earthquake itself would not necessarily cause radiological consequences; it would have to be simultaneous to specific situation during operation (see vault cave-in in Section 5.13).

5.11 RAIL LINE BLAST OR TOXIC/CORROSIVE CHEMICAL RAIL LINE ACCIDENT

In the Mark II conceptual design assessed, the used fuel is delivered into the facility from the nuclear stations by road-travelling UFTP transport vehicles. The possibility of rails leading in the facility area is not excluded; however, rails leading into the facility area are not included in the current assessment.

It is not expected that the facility would be constructed close to a rail line. If the rail line is more than 1 kilometer from the DGR site perimeter fence, any potential blasts from rail line accidents would not cause effects to the facility operation. The same assumption goes for rail line accidents including toxic/corrosive chemicals.

Rail line blast or toxic/corrosive chemical rail line accident in the facility neighbourhood is therefore not considered to cause hazards leading to radiological consequences.

5.12 CRITICALITY DUE TO FLOODING

Criticality is discussed in Section 4.5. It is not credible that flooding would cause criticality with CANDU fuel. Flooding of DGR could potentially release radiation in water from defective UFC, as discussed in Section 5.6, but this is not credible.

Criticality due to flooding in the facility area is therefore not considered possible.

5.13 VAULT CAVE-IN

The working assumption for this report is that no excavation occurs near the placement room and other underground spaces where placement operations are taking place. When the design is more advanced, the effects of excavation should also be included in hazard identification in more detail. The entire volume being open at the same time and being backfilled slowly increases the potential of rock fall from the vault or walls in the facility due to aging of the facility during the entire operation sequence. However, despite the stepwise process, there will always be underground openings that need to stay open throughout the operational period of the facility.

As discussed above in relation to earthquakes, backfilling in general stabilises the rock conditions. Due to low probability of large scale earthquakes and good maintenance and monitoring of the facility, the frequency of rock fall in an active placement room during disposal operation should be very low. However, it cannot be ruled out that such an event would not occur.

Even a large scale vault cave-in has a very low probability to cause consequences affecting the radiological safety of the facility, because the UFC is protected by the buffer box in placement room, and is also covered by the transport cask in other spaces.

The probability of cave-in directly on the UFC being transferred to the placement room is extremely small. Actual probabilities for such a cave-in that would damage the UFC in the buffer box are difficult to define, but it is treated here as a beyond design basis accident (BDBA). No radiological consequences for workers would be expected from this, since all placement room operations are remotely controlled.

Offsite consequences would be similar to those obtained in chain events that lead to the drop of a defective UFC underground, its breach and release of radionuclides.

The Mark II containers are designed to withstand an isostatic pressure of 45 MPa (Heystee 2015). In practice, the maximum pressure before structural collapse is somewhat larger (see Nilsson et al. 2005 for KBS-3V type container). However, the isostatic load is different from abrupt loads that may be posed during rock movements. To look for an example for loads that are more abrupt, a special case of rock shear analysed in relation to long-term performance of the iron inserts and copper outer shell of containers can be examined. This rock shear case is the design basis case for the iron insert (e.g., see Raiko 2012). The copper is assumed to deform in the shear load case (base case 5 cm shear per 1 m/s movement), but no damage to integrity is expected (Posiva 2013). This is analysed in conditions where bentonite buffer provides additional protection (350 mm). The consequences of a vault cave-in for the container integrity are likely to be significantly less severe than the shear load case.

Depending on the bedrock properties, especially groundwater inflow rates, cave-in has potential also to increase inflows, which could lead to flooding of the tunnel(s) (see e.g., Alexander and Neall 2007). However, this is expected to be avoided largely by selecting low permeability host rock, where inflows are controllable and expected hydraulic changes due to seismic movements can be minimised.

5.14 SUMMARY OF EXTERNAL INITIATING EVENTS AND ACCIDENT SCENARIOS

A few accident scenarios with potential for radiological consequences were identified during the review of the externally initiating events. Two aspects on the identified hazards need further consideration in future design iterations: the event frequencies for the identified hazards and the potential radiological results of these hazards. The considerations of the probabilities have been included in Sections 5.1- 5.13.

Table 17 presents a summary of the postulated event scenarios with simplified explanation on how they can be taken forward from this identification phase to be binned as an Anticipated Operational Occurrence (AOO), Design Basis Accident (DBA) or a Beyond Design Basis Accident (BDBA).

Table 17: Summary of External Initiating Events and Postulated Accident Scenarios That Could Have Radiological Consequences

External Initiating Event	Frequency of External Initiating Event with Radiological Consequence	Accident Scenario and Consequences*
Severe rainfall (including thunderstorms)	Non-credible	-
Severe snow/ice	Non-credible	-
Severe wind	Non-credible	-
Lightning strike	Non-credible	-
Tornado, tornado generated missile	Non-credible	-
Flooding	Improbable (not quantified) Consider as a BDBA	31. Flooding of DGR due to hurricane, extreme rainfall, and major earthquake which could crack the shaft liners causing groundwater entering the shafts. This leads to the wetting of the buffer and backfill, potential erosion from around disposed UFCs, and potential exposure of workers to mediate the wetting.
External fire	Non-credible	-
Aircraft crash	Non-credible (estimated frequency of 4E-08 a^{-1} < BDBA limit)	-
Meteorite impact	Non-credible	-
Major earthquake	Improbable (not quantified) Consider as a BDBA	32. Major earthquake leading to potential vault cave-in and release of radionuclides, or cracking of the upper portions of the shaft liners causing groundwater entering the shafts and possible flooding of the repository.
Rail line blast or toxic/corrosive chemical rail line accident	Non-credible	-
Criticality due to flooding	N/A	-
Vault cave-in	Unlikely (not quantified) Consider as a BDBA	33. Vault collapse on UFCs while transferring UFCs into placement room, leading to release of radionuclides.

*Numbering of the accident scenarios continues from Table 14.

6. DIVISION OF SCENARIOS

Potential scenarios have been sorted into groups based on annual frequencies of initiating events. Initiating event frequencies are derived from limited data from the literature on DGR development, nuclear industry, and previous studies.

The accident scenarios were identified for internal initiating events in Section 4.11 and for external initiating events in Section 5.14. All together 33 scenarios were identified during this preliminary hazard assessment.

After the preliminary hazard identification presented here, the next stage in the hazard assessment process is the quantification of the potential radiological consequence of the identified accident scenarios. These calculations have not been carried out in this study.

6.1 ANTICIPATED OPERATIONAL OCCURRENCES

Anticipated Operational Occurrences (AOOs) are events that are expected to occur at least once per 100 years of operation. AOOs include a number of failure modes with very similar scenarios, consequences and frequencies such as failure mode 5 (overhead transfer crane/gantry failure leading to prolonged operation); therefore, they are binned in larger entities, as presented in Table 18. Failure modes with no other similar scenarios such as failure mode 21 (forcing of fuel bundles to basket locations with fuel already in, leading to breaking of bundles) are also presented in the table. The entire list of failure modes causing radiological consequences, postulated during the FMEA process (Section 4.1), is included in Appendix C.

Event frequencies and discussion of how the frequencies are selected are presented in Section 4.1. As AOOs, shielding system failure (gap in the connection of the transfer flask with the weld or copper application cell, leading to additional worker dose) and inadvertent entry scenarios are the postulated scenarios recognised separately from the FMEA process and these are discussed in Sections 4.4 and 4.8 respectively. In addition, UFPP/DGR HEPA filter failure, discussed in Sections 4.2, is also identified. HEPA filter failure by itself does not lead to release of radionuclides; but if the failure happens, it can increase the releases outside the UFPP/DGR during accident with radionuclide release in Table 18.

The results of AOOs lead either to increase in worker doses due to external radiation or to release of radionuclides. Increase in worker doses is either due to prolonged operation, additional worker exposure due to shielding system failure or additional dose due to released radionuclides. The severity of cases with release of radionuclides varies, as does also the effect of the hazard on shielding and exposed people. Appendix C includes the original FMEA table with failure modes leading to radiological consequences for a detailed view of each single failure mode. No external initiating events have been identified to cause AOOs.

Table 18: Anticipated Operational Occurrences (AOOs) for the Mark II Conceptual Design

Accident Scenario	Consequences	
	Increase in Worker Dose (W)	Release of Radionuclides (R)
1. Tie-down detachment problems leading to prolonged operation	W	
2. Weather cover opening problems leading to prolonged operation	W	
3. Failed smear test leading to prolonged operation	W	
4. Vent cell inspection equipment failure leading to prolonged operation	W	
5. Overhead transfer crane/gantry failure leading to prolonged operation	W	
6. Electrical door failure leading to prolonged operation	W	
7. Pallet on rail / rail cart / flask trolley on rails malfunctions causing prolonged operation	W	
8. Tow vehicle / locomotive malfunction leading to prolonged operation	W	
9. AGV system malfunction leading to prolonged operation	W	
10. Vent cell equipment malfunction leading to prolonged operation	W	
11. Attachment or detachment problems with UFTP lid leading to prolonged operation	W	
12. Attachment / detachment problems with UFTP, disposal process vehicles and equipment, leading to prolonged operation	W	
13. Problems or malfunctions with buffer box equipment or process leading to prolonged operation or renew operation	W	
14. Problems with underground installation equipment leading to prolonged operation	W	
16. Dropping of an UFTP lid on UFTP when it is being lifted in the module handling cell		R
17. Fall of a module during transfer in the module handling cell, during transfer to dry storage, or during transfer from laydown area onto an inter-airlock trolley		R
18. Fall of a module in the distribution hall		R
19. Fall of an empty module on full module during transfer to dry storage area		R
21. Forcing of fuel bundles to basket locations with fuel already in, leading to breaking of bundles		R
22. Mis-alignment of basket in the fuel transfer machine, leading to pushing of fuel bundles onto floor		R
24. UFPP/DGR HEPA filter system failure		R*
25. Gap in the connection of the UFC transfer flask with the weld or copper application cell, leading to additional worker dose	W	
28. Inadvertent entry to rooms with operation process, leading to additional worker dose	W	
Number of AOOs	**23**	

* HEPA filter failure by itself does not lead to release of radionuclides; but if the failure happens, it can increase the releases outside the UFPP/DGR during accident with radionuclide release.

6.2 DESIGN BASIS ACCIDENTS

Design Basis Accidents (DBAs) are events that are expected to occur with a frequency between once in one hundred years and once in one hundred thousand years (10^{-2} a^{-1} > DBA > 10^{-5} a^{-1}). They are presented in Table 19. The entire list of events causing radiological consequences, postulated during the FMEA process (Section 4.1), is included in Appendix C. Frequencies and discussion on how they are determined for operation derived failure modes are in Section 4.1.

The potential fire scenarios with impaired fire suppression system and fall scenarios of undetected flawed packages were identified separately from the FMEA process and these are discussed respectively in Sections 4.6 and 4.10. No external initiating events have been identified as causing DBAs. All of the identified DBAs could result in release of radionuclides.

Table 19: Design Basis Accidents (DBAs) for Mark II Conceptual Design

Accident Scenario	**Consequences**	
	Increase in Worker Dose (W)	**Release of Radionuclides* (R)**
15. Fall of the elevator while transferring an UFTP (without impact limiter and with loose lid) down to the basement		**R**
20. Failure of scissor lift during alignment of a module tube for pushing, leading to falling of module/fuel bundles on floor		**R**
26. UFTP transport vehicle fire leading to UFTP damages		**R**
27. UFC placement vehicle fire		**R**
29. Fall of an undetected flawed UFTP in the UFTP shipping and receiving hall		**R**
30. Fall of an undetected flawed UFC in the welding cell, copper application cell or UFC buffer box loading cell		**R**
Number of DBAs	**6**	

* HEPA filter failure is also considered. It does not lead to a release of radionuclides; but if it happens, it can increase the releases outside UFPP/DGR during accident with radionuclide release.

6.3 BEYOND DESIGN BASIS ACCIDENTS

Beyond Design Basis Accidents (BDBAs) are events that are expected to occur between a frequency of once in one hundred thousand years and once in ten million years (BDBA $< 10^{-5}\ a^{-1} - 10^{-7}\ a^{-1}$). In this report, potential accident scenarios with frequency less than $10^{-7}\ a^{-1}$ are considered non-credible and are not considered further.

Only a few hazards are identified as BDBAs and these are summarised in Table 20. They are shaft cage fall (Section 4.1.2.3), flooding in Section 5.6, major earthquake in Section 5.10, and vault cave-in in Section 5.13. Of external initiating events, most are considered non-credible and are excluded from further consideration based on separate discussion and justification in Chapter 5. Only three cases (flooding, major earthquake, and vault collapse) have been identified as BDBAs.

Table 20: Beyond Design Basis Accidents (BDBAs) for the Mark II Conceptual Design

Accident Scenario	Consequences	
	Increase in Worker Dose (W)	Release of Radionuclides (R)
23. Fall of the shaft cage while transferring UFC underground (high fall scenario)		R
31. Flooding of DGR due to hurricane, extreme rainfall, or major earthquake which could crack the shaft liners causing groundwater entering the shafts. These lead to wetting of buffer and backfill and potential erosion from around disposed UFCs	*	*
32. Major earthquake, leading to potential vault cave-in and release of radionuclides or cracking of the upper portions of the shaft liners causing groundwater entering the shafts and possible flooding of the repository.		R
33. Vault collapse on UFCs while transferring UFCs into placement room, leading to release of radionuclides		R
Number of BDBAs	4	

* It is possible that radiological consequences would remain negligible, because workers would not be at location and UFCs would remain intact. But the workers may be exposed during mediation of the wetting after the flooding.

7. DISCUSSION

This preliminary hazard identification results in twenty-three AOOs, six DBAs, and four BDBAs for the Mark II conceptual design (Sections 6.1, 6.2 and 6.3). They were identified by performing the FMEA process. There are 147 operation steps for the conceptual design as listed in Appendix B for annual processing of 630 UFTPs, 1,260 modules, 120,960 fuel bundles, and 2,520 UFCs. Of these, 115 steps lead to single failure modes with radiological consequences as given in Appendix C:

- 95 failure modes for UFPP operations; and
- 20 failure modes for shaft and underground operations.

The conceptual design has more single failure modes in UFPP operations than in shaft and underground operations. This is because UFPP has more electrically remote doors, and transfer operations using overhead transfer cranes/gantries, AGV, and tow vehicles/trolleys for UFTPs, modules, and UFCs. Most of these operations such as opening/closing of electrical doors and transfer operations are repeated frequently in many places in the UFPP. These equipment and vehicles may fail or malfunction. In contrast, there is no lifting by overhead transfer crane/gantry in underground DGR operations.

Most of the failure modes lead to prolonged operation and low dose consequence to workers (increased worker external radiation dose) rather than radionuclide release, as the UFTPs and UFCs are designed to withstand drop/fall and, with low travel speed, collision during traffic accident. In most cases, the radiological consequence to workers is limited due to safe practices of the nuclear facility operation, especially when the common practices follow the ALARA consideration in facility design and operation. Without quantification of consequence (i.e., calculation of additional doses), it is not possible to determine the effects of these accident scenarios on workers; but, when compared against the preliminary ALARA dose assessment in Reijonen et al. (2014), it is estimated that these events do not increase the worker doses significantly. Consequently, this allows a number of these similar low consequence failure modes to be grouped into fourteen accident scenarios as given in Table 8 and Table 14. As shown in Table 8, most of the failure modes occur frequently (>1E-2 a^{-1}) due to repeated operations. Examples are “electrical door failure”, “tow vehicle failure”, “overhead transfer crane/gantry failure”, and “failure of transfer pallet, rail cart and flask trolley”. There are also manual handling steps at the start of the processing of UFTPs, which could lead to human errors.

Some of the failure or equipment malfunction could lead to release of radionuclides due to potential damage to the UFTP (under elevator fall), modules, used fuel bundles (under fuel transfer of used fuel bundles to UFCs), and UFC (under cage fall) as listed in Table 9. These failure modes (16 in total) are grouped into nine accident scenarios (Table 14). The release of radionuclides could occur by damage of a few used fuel bundles as in modules, or by substantial breach of UFC and damage of all fuel bundles with significant release of radionuclides, for example, under shaft cage fall scenario. In this report, the consequences of release of radionuclides, i.e., whether radiation would spread and affect public or remain isolated, is not quantified.

In addition to operation-derived failures, ventilation HEPA filter system failure, shielding system failure (gap in the connection of the UFC transfer flask with the weld or copper application cell), fires involving UFTP transport vehicle and UFC placement vehicle, inadvertent entry to rooms with operation process, and drop of undetected flawed UFTP and UFC, are also identified (Table 14).

The initial list of external initiating events was based on literature (14 in total), which were further compared to those in IAEA (2004) consisting of 21 external events. Of these, only three (flooding of DGR due to hurricane, extreme rainfall or major earthquake causing potential cracking of the shaft liners, and major earthquake causing vault collapse/cave-in) were considered to cause potential hazard with radiological consequences (Table 17). The fact that site is not yet selected makes the event frequency estimation and discussion general in nature. After site selection, the external initiating events will need to be reconsidered.

In general, the hazard assessment is preliminary because of the preliminary stage of the Mark II conceptual design. Some steps may change and more steps may be included or excluded in the future as the design evolves. There are also certain process steps which do not have an international reference and, therefore, the hazards will need further assessment as design becomes more detailed (e.g., performance of the semi-circular headed UFC, UFC welding process, and installation of UFC in buffer box).

The estimation of event frequencies is also preliminary due to the preliminary design stage:

- The numerical failure frequencies were estimated for some failure modes (e.g., shaft cage fall, and overhead transfer crane/gantry failure) based on limited data from literature on the repository development studies as discussed in Chapter 4. Therefore, for example, the frequency of failures selected for prolonged operation due to equipment/vehicle failure or human errors is set as 5E-5 per operation (Section 4.1.2.6), the same as for crane drop. This is intended as a guide on how annual failure frequencies are formed and as an example of what kind of values would be reached with these failure modes due to their high occurrences in the facility operation. As discussed previously, even if this frequency per operation could be lowered in the future, the number of the repeated operations elevates the annual frequencies to quite high values (> 1E-2 a^{-1}).

- Certain frequencies estimated for this preliminary hazard identification are conservative. An example of situations where the frequency may be reduced in future work is the drop of an empty module on a full module. In this report, the failure frequency per lift has been used for lifting full modules (Section 4.1.2.4). However, as the drop of an empty package onto the floor would not cause radiological results, the frequency of its falling on a full module is bound to be smaller. These generalizations have been kept for now due to the preliminary nature of the process design and iterations to follow. In final hazard assessment work, these will need further consideration.

- The accident frequencies in this report are for single failure modes. Combined failure modes that have common cause have not been considered except for the drop of an undetected flawed UFTP or UFC, and fire scenarios with impaired fire suppression system. For example, the annual failure frequency for the case with ventilation HEPA filter system failure during the cage fall or drop scenario has not been calculated. The annual frequency for this combined scenario would be lower than that for the cage fall or drop scenarios or for filter system failure. In this report, the HEPA filter system failure alone is listed as AOO, which by itself does not lead to radionuclide release.

The number of failure modes causing radionuclide release is reduced by the designed durability of the used fuel packages (UFTP and UFC) and low speed of transfer equipment/vehicles. These working assumptions to avoid drop and fall of UFTP/UFC and collision scenarios are listed in Section 3.3. These assumptions need to be validated.

Cage fall scenario, one of the most significant types of accidents regarding consequence, may be mitigated with further design (e.g., providing shock absorber at the bottom of the shaft). These may be based on different shock absorber materials considered by Posiva (e.g., Kukkola 2009) to help keep the shielding of the used fuel canister intact (although this may not prevent fuel damage inside).

7.1 DISCUSSION OF ANTICIPATED OPERATIONAL OCCURRENCES

Due to the large amount of failure modes within the AOO category, grouping of the occurrences is useful. Failure modes that have similar consequences and frequencies and occur in the same location have been binned in order to produce fewer cases that may need to be considered further. Table 18 presents the AOO accident scenarios and their consequences.

Most of the AOOs identified in this report result in low consequences, but dose calculations will be needed in future to affirm this. With design iterations, good facility practices (ALARA), personnel training and high standard equipment and their maintenance, the frequencies can be expected to be lowered before the operation starts.

Most AOOs were derived from steps with the FMEA process. However, HEPA filter system failure was estimated with such an annual frequency that it is also included, although the failure by itself would not lead to radionuclide release. Inadvertent entries, having very small increases in worker doses, are also AOOs.

7.2 DISCUSSION OF DESIGN BASIS ACCIDENTS

DBAs are discussed here by comparing the findings in this study to the information obtained in the literature (Appendix A.2).

Scissor lift failure is identified in this report as a DBA, same as in OHN (1994). In addition to scissor lift failure, a few other equipment malfunctions have also been found to cause dropping of the used fuel bundle(s), full module or UFC (with or without shielding package) as DBAs in e.g., OHN (1994) and Kukkola (2009). In this report, overhead transfer crane/gantry failure is identified as an AOO due to frequent repeated lifting operations in many places in UFPP. This type of failure leads to prolonged operation for durable UFTPs and Mark II UFCs and to potential release of radionuclides for modules (Table 18).

In the literature, the reported DBAs also include simultaneous failure of the ventilation HEPA system with a scissor lift, overhead carriage failure or shaft hoisting system as in OHN (1984), or ventilation HEPA system failure during a seismic event resulting in the collapse of a low level waste facility as in U.S. DOE (2009). In this report, ventilation system failure is discussed separately and the probability for a single HEPA filter system failure is determined according to literature as an AOO. However, future work should look into the combined effect of ventilation system failure with relevant accident scenarios.

In this report, drop scenarios combined with undetected flawed packages are also identified as DBAs. The probabilities for undetected flawed UFTP/UFC were determined here by expert judgement. With design proceeding, this estimation can be re-considered.

All fire scenarios were assessed to be DBAs in this study. In reference reports, fire is in most cases identified as a hazard with waste types other than used fuel, and in varying environments. OPG (2011) considered LILW, NDA (2010) ILW, U.S. DOE (2009) LLW, and WIPP (2013) TRU waste. In reference cases, the fire is induced by transportation accidents or lack of cooling leading to overheating or it is simply considered to occur without contemplation on how. Considering that the scope of work of this report excludes the road transport phase, only one clear reference for used fuel is found from SKB (2010) in which a large scale fire is included as a DBA. This case was not thoroughly discussed, and hence the ignition and burning mechanism cannot be compared to postulated events in this report. Due to the WIPP fire in 2014, fire is conservatively considered here to be a potential accident scenario.

7.3 DISCUSSION OF BEYOND DESIGN BASIS ACCIDENTS

BDBAs has been selected on the basis of dividing the initiating event frequencies as unlikely (BDBA) and non-credible (not considered further), using the annual frequency of 1.0E-7.

For most part, external initiating events were analysed based on very general considerations; when an actual site is selected, this analysis may need to be re-visited. Site selection criteria should also take account of the external initiating event list to avoid condition by reasonable screening in the site selection phase. Three of the four BDBAs identified in this report are due to natural phenomena for which frequencies are very difficult to estimate. Hence, they are based mostly on expert judgement.

Shaft cage fall is the only BDBA identified from the internal initiating events. This accident has qualitatively been estimated with the same probability as ANDRA (2005) has concluded. As the potential radiological consequence for the shaft cage fall is high, design actions should be taken to reduce both the probability of the cage fall and of radionuclide release.

Vault cave-in is also considered to have more potential to damage the Mark II UFC, because the UFCs (in buffer boxes) are outside their transfer packages in the underground facility. The probability of a major earthquake causing cave-in was qualitatively considered; because the earthquake damage would potentially affect larger areas of the underground facility, a single vault collapse would need to be specifically in certain place to damage an UFC. This hazard will be discussed further in future iterations of the hazard assessment when an actual site is selected.

7.4 COMPARISON WITH THE LITERATURE

Although there is some literature listing accidents identified for a deep geological repository, the fact remains that the concepts, waste types to be disposed of, and methodologies used vary depending on the studies. For the methodology development, literature review is very useful, and an appropriate methodology is defined for preliminary hazard assessment of the Mark II conceptual design.

Direct comparison among different studies is not considered to be fruitful, especially regarding internal initiating events. Only one study discusses the same fuel, CANDU, and a relatively similar design (OHN 1994). In this case, the assessed events are similar and no major gaps have been identified without reason (e.g., difference in design).

8. CONCLUSIONS AND RECOMMENDATIONS

This report presents potential hazards that were identified using the FMEA process for the Mark II conceptual design. Most of the identified failure modes lead to prolonged periods of operation and incremental low dose consequences to workers (i.e., increased worker external radiation dose) rather than radionuclide release. These failure modes are grouped into twenty-three AOOs, six DBAs, and four BDBAs according to estimated annual frequencies of the failure modes from which they were formulated. The accident scenarios presented in this report are the starting point for future dose calculations. The identified hazards can also be utilized in iterations of the Mark II conceptual design.

For internal initiating events, the risk priority number (see Appendix C) can be used to locate the cases with most severe consequences, and the severity number (Appendix C) can be used to group some of the identified cases to produce bounding scenarios.

For external initiating events, the fact that NWMO does not have a selected site, or reference sites for the design, leaves the discussion at a rather general level. When the site is selected, the external initiating event screening needs to be redone to account for the properties and environment of the site.

Ventilation filter system failure is recommended to be included in the dose calculations as an over-arching event, i.e., to be combined with other accident scenarios.

When the design is more detailed, a detailed Fire Hazard Analysis will need to be completed. Also each step of the operation process is recommended to be re-subjected to hazard identification (e.g., FMEA, HAZOP, event tree).

One of the main goals of the preliminary hazard identification is to identify processes or parts of them that may need some mitigating actions. FMEA table can be further developed by introducing mitigating actions and re-calculating the risk priority number. An example of the mitigating actions is cage fall in the shaft. Cage fall is one of the most significant types of accidents regarding severity. The consequences of the shaft cage fall can be mitigated using, e.g., shock absorbers at the bottom of the shaft.

REFERENCES

Alexander, W.R. and F. Neall. 2007. Assessment of Potential Perturbations to Posiva's SF Repository at Olkiluoto from the ONKALO Facility. Posiva Working Report 2007-35. Posiva Oy, Olkiluoto, Finland. (Also available at http://www.posiva.fi/files/362/WR2007-35web.pdf).

ANDRA. 2005. Dossier 2005 Argile. Architecture and Management of a Geological Repository. December 2005. Paris, France. (Also available at https://curie.ornl.gov/content/dossier-2005-argile-architecture-and-management-geological-repository).

Areva. 2012. NDA RWMD Operational Safety Assessment (ROSA) Toolkit Version 5.0 User Manual. Areva RMC Report Number R11-036(W). Warrington, U.K.

Batters, S., K. Tsang, and U. Stahmer. 2012. Generic Transportation Dose Assessment. Nuclear Waste Management Organization Report NWMO TR-2012-06. Toronto, Canada.

CNSC. 2008. Safety Analysis for Nuclear Power Plants. Canadian Nuclear Safety Commission, Regulatory Document RD–310 G-129. Ottawa, Canada.

Easton, E. 2014. Why the Nine Metre Drop Test Bounds the Impacts from Most Severe Accidents. Nuclear Waste Management Organization Report NWMO TR-2014-04. Toronto, Canada.

Garisto, N.C., W. Newmyer and A. Ho. 2014. Criticality Safety Computations for Spent CANDU Fuel in a Deep Geologic Repository. Nuclear Waste Management Organization Report NWMO TR-2014-08. Toronto, Canada.

Heystee, R.J. 2015. Deep Geological Repository Design Report, Crystalline/ Sedimentary Rock Environment, Mark II Used Fuel Container. NWMO Report APM-REP-00440-0015. Toronto, Canada.

Holmberg, J.E., P. Kuusela and Y. Malmén. 2012. Probabilistic Risk Assessment for encapsulation plant and underground repository (available only in Finnish: Kapselointi- ja loppusijoituslaitoksen PRA). VTT-R-00620-11. *Not in public distribution.*

IAEA 2003. Extreme External Events in the Design and Assessment of Nuclear Power Plants. International Atomic Energy Agency. IAEA-TECDOC-1341. Vienna, Austria.

IAEA 2004. Experience Gained from Fires in Nuclear Power Plants: Lessons learned. International Atomic Energy Agency. IAEA-TECDOC-1421. Vienna, Austria.

Ide, S., A. Baltay, and G.C. Beroza. 2011. Shallow Dynamic Overshoot and Energetic Deep Rupture in the 2011 Tohoku-Oki earthquake. Science 332, no. 6036, 1426-1429.

JNC. 2000. H12: Second Progress Report on R&D for the Geological Disposal of HLW in Japan. Supporting Report 1 – Geological Environment in Japan. Japan Atomic Energy Agency (JAEA). JNC TN1410 99-011. Tokai, Japan.

Kukkola, T. 2009. Olkiluoto Encapsulation and Disposal Plant; Determination of Normal Operation, Upset and Postulated Accident Conditions for Radioactive Release and Dose Assessment (in Finnish). Posiva Oy. Working Report 2008-71. Olkiluoto, Finland. (Also available at http://www.posiva.fi/files/981/TR_2008-71.web.pdf).

Melick, A.G. 2007. Beaconsfield Investigation Report. Prepared for the Coroner – at the Request of the Tasmanian Government. ALX.016.002.0002_001. Magistrates Court of Tasmania 2007. (Aslo available at http://www.magistratescourt.tas.gov.au/__data/assets/pdf_file/0005/120884/alx.016.002.0002_001.pdf).

NDA. 2010. Geologic Repository: Generic Operational Safety Case Main Report. Nuclear Decommissioning Authority Report no. NDA/RWMD/020. Didcot, U.K. (Also available at http://www.nda.gov.uk/publication/geological-disposal-generic-operational-safety-case-main-report-december-2010/).

NIED. 2011. Preliminary Evaluation of the Tohoku-Oki Earthquake Ground Acceleration Data. National Research Institute for Earth Science and Disaster Prevention. Tsukuba, Japan.

Nilsson K.F., F. Lofaj, M. Burström and C.G. Andersson. 2005. Pressure Tests of Two KBS-3 Canister Mock-ups. Swedish Nuclear Fuel and Waste Management Company Report SKB TR-05-18. Stockholm, Sweden. (Also available at http://www.skb.se/upload/publications/pdf/TR-05-18.pdf).

Niwa, M., R. Takeuchi, H. Onoe, K. Tsuyuguchi, K. Asamori, K. Umeda and K. Sugihara. 2012. Groundwater Pressure Changes in Central Japan Induced by the 2011 off the Pacific Coast of Tohoku Earthquake. Geochemistry, Geophysics, Geosystems 13, Q05020, doi:10.1029/2012GC004052.

NWMO. 2011. Geosynthesis. Nuclear Waste Management Organization Report NWMO DGR-TR-2011-11. Toronto, Canada. (Also available at http://dgr.nwmo.ca/uploads/DGR%20PDF/Geo/Geosynthesis.pdf).

OHN. 1994. The Disposal of Canada's Nuclear Fuel Waste: Preclosure Assessment of a Conceptual System. Ontario Hydro Nuclear Report N-03784-940010 (UFMED), COG-93-6. Toronto, Canada.

OPG. 2001. Early Failure Probability of Used-Fuel Containers in a Deep Geologic Repository. Ontario Power Generation Report 06819-REP-01300-10022-R00. August 2001. Toronto, Canada.

OPG. 2006a. Western Waste Management Facility Safety Report. Ontario Power Generation Report W-SR-01320-00001. R01. Toronto, Canada.

OPG. 2006b. Darlington Waste Management Facility Safety Report. Ontario Power Generation Report 00044-SR-01320-10002-R00. Toronto, Canada.

OPG. 2007. Pickering Waste Management Facility Safety Report. Ontario Power Generation Report 92896-SR-01320-10002-R003. Toronto, Canada.

OPG. 2011. OPG's Deep Geologic Repository Project for Low and Intermediate Level Waste – Preliminary Safety Report. Ontario Power Generation Report 00216-SR-01320-00001 R000. Toronto, Canada. (Also available at http://dgr.nwmo.ca/uploads/DGR%20PDF/Licensing/Preliminary-Safety-Report.pdf).

Posiva. 2012. Safety Case for the Disposal of Spent Nuclear Fuel at Olkiluoto – Complementary Considerations 2012. Posiva Report 2012-11. Posiva Oy, Eurajoki, Finland. (Also available at http://www.posiva.fi/files/2995/POSIVA_2012-11_web.pdf).

Posiva. 2013. Safety Case for the Disposal of Spent Nuclear Fuel at Olkiluoto – Performance Assessment 2012. Posiva Report 2012-04. Posiva Oy, Eurajoki, Finland. (Also available at http://www.posiva.fi/files/3010/Posiva_2012-04web.pdf).

Raiko, H. 2012. Canister Design 2012. Posiva Report 2012-13. Posiva Oy, Eurajoki, Finland. (Also available at http://www.posiva.fi/files/3093/POSIVA_2012-13.pdf).

Reijonen, H, T. Karvonen and J.L. Cormenzana. 2014. Preliminary ALARA Dose Assessment for Three APM DGR Concepts. Nuclear Waste Management Organization Report NWMO TR-2014-18. Toronto, Canada.

Rossi, J. and V. Suolanen. 2013. Operational Safety Analysis of the Olkiluoto Disposal Site (in Finnish). Posiva Oy Working Report 2013-51. Eurajoki, Finland. (Also available at http://www.posiva.fi/files/3457/TR_2013-51.pdf).

Rossi, J., H. Raiko and V. Suolanen. 2009. Assessment of Radiation Doses in Normal Operation, Upset and Accident Conditions at the Olkiluoto Nuclear Waste Facility. Posiva Oy Working Report 2009-106. Olkiluoto, Finland. (Also available at http://www.posiva.fi/files/1117/WR_2009-106web.pdf).

Shimizu, I., H. Osawa, T. Seo, S. Yasuike and S. Sasaki. 1996. Earthquake-related Ground Motion and Groundwater Pressure Change at the Kamaishi Mine. Engineering Geology 43, 107-118.

SKB. 2010. Fuel and Canister Process Report for the Safety Assessment SR-Site. Swedish Nuclear Fuel and Waste Management Company Technical Report SKB TR-10-46. Svensk Kärnbränslehantering AB, Stockholm, Sweden. (Also available at https://www.stralsakerhetsmyndigheten.se/Global/Slutf%C3%B6rvar/KTL/KTL%203/12_Fuel_and_canister_process_report.pdf).

Stamatis, D.H. 2003. Failure Mode and Effect Analysis: FMEA from Theory to Execution. ASQ Quality Press, 455pp.

STUK. 2013a. Regulatory Guides for Nuclear Safety; YVL D.3 Handling and storage of nuclear fuel. In Finnish. (Also available at http://plus.edilex.fi/stuklex/fi/lainsaadanto/saannosto/YVLD-3).

STUK. 2013b. Regulatory Guides for Nuclear Safety; YVL D.5 Radioactive Waste Management. In Finnish. (Also available at http://plus.edilex.fi/stuklex/fi/lainsaadanto/saannosto/YVLD-5).

U.S. DOE. 2006. Accident Analysis for Aircraft Crash into Hazardous Facilities. U.S. Department of Energy, DOE-STD-3014-2006. Washington, D.C., U.S. (Also available at http://energy.gov/sites/prod/files/2013/06/f2/std3014.pdf).

U.S. DOE. 2008. Supplemental Environmental Impact Assessment for the Disposal of Spent Nuclear Fuel and High-Level Radioactive Waste at Yucca Mountain, Nye County, Nevada, Volume II, Appendices A through J. U.S. Department of Energy. Office of Civilian Radioactive Waste Management. DOE/EIS-0250F-S1. U.S.

U.S. DOE. 2009. Yucca Mountain Repository License Application Safety Analysis Report. Sections 1.6-1.8. DOE/RW-0573 Rev.1. Las Vegas, U.S. (Also available at http://pbadupws.nrc.gov/docs/ML0907/ML090700894.pdf; the whole report is available from the U.S. NRC web site http://www.nrc.gov/waste/hlw-disposal/yucca-lic-app/yucca-lic-app-safety-report.html).

U.S. DOE. 2014. Accident Investigation Report, Underground Salt Haul Truck Fire at the Waste Isolation Pilot Plant, February 5, 2014. U.S. Department of Energy. Office of Civilian Radioactive Waste Management. DOE, March 2014. U.S. (Also available at http://www.wipp.energy.gov/Special/AIB%20Report.pdf).

U.S. NRC. 1987. NUREG/CR-4846 U.S. Nuclear Regulatory Commission (USNRC). High-Level Waste Pre-closure Systems Safety Analysis. Phase 2, Final Report. 1987. Washington, D.C., U.S.

U.S. NUREG. 1980. Control of Heavy Loads at Nuclear Power Plants. U.S. Nuclear Regulatory Commission Office of Nuclear Reactor Regulation. NUREG-0612. Washington, D.C., U.S. (Also available at http://pbadupws.nrc.gov/docs/ML0702/ML070250180.pdf).

U.S. NUREG. 2003. A Survey of Crane Operating Experience at U.S. Nuclear Power Plants from 1968 through 2002. U.S. Nuclear Regulatory Commission Office of Nuclear Regulatory Research. NUREG-1774. Washington, D.C., U.S. (Also available at http://pbadupws.nrc.gov/docs/ML0320/ML032060160.pdf).

WIPP. 2013. Waste Isolation Pilot Plant Documented Safety Analysis. DOE/WIPP 07-3372, REV. 4. Carlsbad, U.S. (Also available at http://www.wipp.energy.gov/library/DSA/DOE_WIPP_07-3372_Rev_4_DSA.pdf).

APPENDIX A: HAZARD CATEGORIZATION FROM INTERNATIONAL REFERENCES

CONTENTS

Page

A.1 ANTICIPATED OPERATIONAL OCCURRENCES IDENTIFIED IN REVIEWED LITERATURE

In this appendix the Anticipated Operational Occurrences (AOOs) compiled from Kukkola (2009), Rossi et al. (2009), SKB (2010) and OPG (2011) are presented. Because the terminology varies among different countries, local terminology of each document is used for describing the scenario. Operational failures, upsets and other similar expressions in the provided table refer to what is in this report (Preliminary hazard assessment) referred to as AOOs.

The following abbreviations are used in the table:

T1	Refers to incorrect handling of fuels transport cask resulting in leak of radionuclides
T2	Refers to incorrect handling of fuel element resulting in breaking elements
T3	Refers to exposure to direct radiation due to entering areas of high radiation levels
A	Radiological occurrence resulting in emission
B	Effect on barriers (occurrences with only B not listed in this report)
D	Radiological accident leading to increase in doses for people
L1 – L10	Identification markings

AOOs identified by Posiva (Finland)					
Operational Failures					
Place	**Event**	**Consequence**	**Kukkola (2009, Table 2 in Appendix)**	**Rossi et al. (2009)**	**Upset Code (Rossi et al. 2009)**
Transport cask's transfer corridor	Incorrectly connected sampling tubes	Radioactive gas leakage	x	x	T1
Transport cask's transfer corridor	Incorrectly connected pressure balancing tubes	Radioactive gas leakage		x	T1
Transport cask's transfer corridor	Incorrect connection in washing the transport cask	Radioactive gas leakage	x		
Handling chamber	Damage to fuel rods (e.g., two fuel rods forced in a single position)	Radioactive gas leakage, dispatching of crud	x	x	T2
Handling chamber	Entering when fuel is in the handling chamber	Exposure to direct radiation	x	x	T3
Handling chamber	Entering when there is radiation in the handling chamber	Exposure through ventilation		x	T3
Handling chamber	Bundle/rod is stuck	Exposure through ventilation	x		
Canister transfer corridor	Entering when fuel is in the transfer corridor	Exposure to direct radiation	x	x	T3
Buffer storage	Entering when fuel is in the buffer storage	Exposure to direct radiation	x	x	T3
Canister lift	Entering when fuel is in the canister lift (both entry levels)	Exposure to direct radiation	x	x	T3
Repository	Loading of a canister at an awkward angle	Exposure to external radiation	x	x	T4
Repository	Entering disposal site before buffer is installed but fuel is loaded already	External exposure	x	x	T3

Device Malfunctions						
Place	**Event**	**Consequence**	**Kukkola (2009, Table 2 in Appendix)**	**Rossi et al. (2009)**	**Upset Code (Rossi et al. 2009)**	**Notes**
Reception area and transfer corridor	Breakage to the transport cask's washing equipment	Radioactive water leakage	x	x	L2	Not included in further assessments
Handling chamber	Damage to fuel rods (e.g. two fuel rods forced in a single position)	Radioactive gas leakage, dispatching of crud	x	x	L3	
Handling chamber	Malfunctions of the drying system	Cannot lead to radiation release		x	L4	Not included in further assessments
Handling chamber	Damage to the negative pressure system	Radioactive gas leakage	x	x	L5	Not included in further assessments
Handling chamber	Damage to the cooling and filtering system	Radioactive gaseous release in the controlled area	x	x	L6	Not included in further assessments
Handling chamber	Damage to the crud vacuuming system	Spreading of crud	x			
Encapsula-tion	Tightness of the handling chambers docking station is lost (if seals are damaged)	Release to controlled area		x	L7	Not included in further assessments
Encapsula-tion	Damage to the vacuum and decontamination systems	Release of radioactive particles or water	x	x	L8	Not included in further assessments
Encapsula-tion	Unsuccessful alignment of the electron beam	Not discussed		x	L9	Not included in further assessments
Repository	Loading of a canister at an awkward angle	Exposure to external radiation	x	x	L10	
Repository	Malfunction in placing buffer blocks	Exposure to external radiation	x			

Other Upset Situations (Kukkola 2009, Section 3.2)
(For these situations, no radioactive consequence was given)

Place	Event	Correcting Procedure
Handling chamber	Lid elevator for transport cask is stuck	Moving of lid elevator in the maintenance area with a maintenance crane
Handling chamber	Fuel transfer manipulator is stuck	Moving of the manipulator in the maintenance area, after fuel bundle is removed with another manipulator
Handling chamber	Failure in attachment of the inner lid	Detachment of lid and replacement with new
Transport cask's transfer corridor	Canister elevating mechanism gets stuck below the handling chamber	Re-docking and emptying the canister of the fuel bundles
Transport cask's transfer corridor	Canister transfer trolleys moving mechanism gets stuck	Pulling with cable wire below the elevator and lifting into the buffer storage
Transport cask's transfer corridor	Canister lifting mechanism gets stuck below the welding chamber	Re-docking and emptying the canister of the fuel bundles
Encapsulation	Malfunction of the automated guided vehicle in the buffer storage	Replacement of the vehicle with another
Repository	Malfunction of the canister transfer and installation vehicle	Repairing the vehicle
Repository	Loading of a canister at an awkward angle	Pulling the canister back up in the radiation shield. Replacement of lineation (buffer) and re-installation of canister.
Repository	Failure in placing buffer blocks on top of a canister	Buffer is replaced

Other Mentioned Occurrences (Kukkola 2009, Section 3.2)

Place	Event	Consequence
Encapsulation process	Damaged fuel rod (due to upset/accident)	Contamination of the encapsulation process
Encapsulation plant/disposal facility	Power loss for a limited time	Replacing power supply, no releases or elevated doses
Encapsulation plant/disposal facility	Fires (fuel transport vehicle, diesel aggregate, electrical systems, cranes, lifts, gearing, cables due to shortcuts, canister moving and installation vehicle in the repository)	Fire load is small, no releases or elevated doses
Flooding and leakage	Flooding and leakage	Premature swelling of bentonite, no releases or elevated doses

AOOs Identified by SKB (2010) (Sweden)				
Expected Occurrences				
Place	**Event**	**Considered Consequence**		
		A	**B**	**D**
Collision				
Terminal building	Collision to rock wall or other vehicle, canister in transport cask (in terminal vehicle)	x	x	x
Ramp				
Reloading hall				
Reloading hall	Collision to rock wall or other vehicle, canister outside transport cask (in deposition machine)	x	x	x
Transport tunnel				
Main tunnel				
Deposition tunnel				
Lifting or handling perturbance, which can result in injury of the copper canister				
Terminal building	Swinging load (canister in transportation cask)	x	x	x
Reloading place				
Ramp	Objects from other equipment (canister in transportation cask)	x	x	x
Reloading hall	Objects from other equipment (canister outside transportation cask)	x	x	x
Reloading hall	Objects from other equipment (canister in deposition machine)	x	x	x
Deposition tunnel		x	x	x
Reloading place	Too high lowering speed of canister (canister in transport cask)	x	x	x
Reloading place	Too high lowering speed of canister (canister outside transport cask)	x	x	x
Deposition hole	Too high lowering speed of canister (canister outside transport cask)	x	x	x
Internal occurrences				
All	Limited fire	x	x	x
All	Ventilation failure			x
Reloading hall	Canister placed without radiation shielding (unmonitored)			x
Deposition hole				
Transportation cask	Radiation shield opening failure			x
Reloading hall				
Deposition machine				
External occurrences				
Terminal building	Occurrence resulting in failure of overlying system (flooding, ventilation, power loss, cooling)		x	x
Reloading hall				
Deposition machine				

AOOs identified by OPG (2011) (Canada)	
Event	**Considered Consequence**
Mechanical/equipment failure (ventilation system)	The ventilation system could fail due to fan or damper electrical or mechanical problems. This would not affect the package integrity, but could allow the local build-up of flammable gases or radioactive gases. However, these gases would take days (radioactive gases) to months (flammable gases) to build up to hazardous levels. Since the ventilation flow is driven through the tunnels and rooms by a simple negative pressure maintained by fans at the ventilation shaft, and since the underground area is monitored for flammable gases and radioactivity, it is not credible that they would build up to hazardous levels before being detected. Nonetheless, ventilation system failure is considered as an unlikely initiating event.
Human error causing package drop/hit	An examination of the Western Waste Management Facility station condition records from 1998 to 2006 identified various human error related incidents, including several cases with minor damage to packages during handling. None of these cases led to package drop or breach. Over the deep geological repository operating life, the largest risk of package drop is with the low level waste packages due to their large number. Package drop is considered as a possible initiating event for low level waste and an unlikely initiating event for intermediate level waste.

A.2 DESIGN BASIS ACCIDENTS IDENTIFIED IN REVIEWED LITERATURE

In this appendix the DBAs compiled from U.S. DOE (2009), NDA (2010), OPG (2011), WIPP (2013), Kukkola (2009), Rossi and Suolanen (2013), SKB (2010) and OHN (1994) are presented. Because the terminology varies among different countries, local terminology of each document is used for describing the scenario. Bounding event implies that the event was selected from binned scenarios of the similar incidents, the selected ones having the most significant results.

The following abbreviations are used in the table:

BWR	Boiling Water Reactor
DBA	Design Basis Accident
DBF	Design Basis Fault
DOE	Department of Energy (U.S.)
HEPA	High-efficiency particulate air
HLW	High Level Waste
H3/H4	Accident rating in SKB (2010)
ILW	Intermediate Level Waste
L&ILW	Low and Intermediate Level Waste
LLW	Low Level Waste
NDA	Nuclear Decommissioning Authority (UK)
OHN	Ontario Hydro Nuclear
OPG	Ontario Power Generation
PWR	Pressurised Water Reactor
SKB	Swedish Nuclear Fuel and Waste Management
SNF	Spent Nuclear Fuel
TRU	Transuranic
UF	Used Fuel
WIPP	Waste Isolation Pilot Plant (U.S.)

Accident Type	Design Basis Accidents	Waste	Reference
DBA	Forklift with tines collides and punctures waste array, resulting in a fire	TRU	WIPP (2013), Section 3.4.2.1
DBA	Loaded transporter collides with the waste array, resulting in a fire	TRU	WIPP (2013), Section 3.4.2.1
DBA	Electric cart or electric man lift collides with waste array, resulting in a fire	TRU	WIPP (2013), Section 3.4.2.1
DBA	Collision at the waste face with mining equipment results in a fire	TRU	WIPP (2013), Section 3.4.2.1
DBA	Non-waste handling equipment collides with waste array, resulting in a fire	TRU	WIPP (2013), Section 3.4.2.1
DBA	Fuel-pool fire occurs at the waste face with mining equipment	TRU	WIPP (2013), Section 3.4.2.1
DBA	Fuel-pool fire occurs at the waste face with the contact-handled waste forklift	TRU	WIPP (2013), Section 3.4.2.1
DBA	Fuel-pool fire occurs at the waste face with the contact-handled waste transporter	TRU	WIPP (2013), Section 3.4.2.1
DBF	Inadvertent exposure of maintenance worker to unshielded package	Unshielded ILW	NDA (2010), Section 5.4.4
DBF	Impacts underground involving a single unshielded package; these faults are only potentially significant in terms of worker	Unshielded ILW	NDA (2010), Section 5.4.4

Accident Type	Design Basis Accidents	Waste	Reference
	exposure; results for the public are fully compliant with dose targets		
DBF	Severe impacts underground involving multiple unshielded packages	Unshielded ILW	NDA (2010), Section 5.4.4
DBF	Fires underground involving unshielded packages	Unshielded ILW	NDA (2010a), Section 5.4.4
DBF	Impacts at the surface involving shielded packages	Shielded ILW	NDA (2010), Section 5.4.4
DBF	Sustained fires (including those following an impact event) at the surface	Shielded ILW	NDA (2010), Section 5.4.4
DBF	Severe impacts underground involving multiple shielded packages; these faults are only potentially significant in terms of worker exposure; public exposure from these faults is negligible and fully compliant with dose targets	Shielded ILW	NDA (2010), Section 5.4.4
DBF	Sustained fires (including those following an impact event) occurring underground	Shielded ILW	NDA (2010), Section 5.4.4
Potential Accident, Bounding Scenario	Outdoor waste package fire (above ground)	L&ILW	OPG (2011), Table 7-27
Potential Accident, Bounding Scenario	Indoor waste package fire (above ground)	L&ILW	OPG (2011), Table 7-27
Potential Accident, Bounding Scenario	Outdoor waste package breach (above ground)	L&ILW	OPG (2011), Table 7-27
Potential Accident, Bounding Scenario	Indoor waste package breach (above ground)	L&ILW	OPG (2011), Table 7-27
Potential Accident, Bounding Scenario	Inadequate shielding (above ground)	Moderator resin	OPG (2011), Table 7-27
Potential Accident, Bounding Scenario	Waste package fire during transport (underground operations)	L&ILW	OPG (2011), Table 7-28
Potential Accident, Bounding Scenario	In room waste package fire (underground operations)	L&ILW	OPG (2011), Table 7-28
Potential Accident, Bounding Scenario	Waste package breach during transfer (underground operations)	L&ILW	OPG (2011), Table 7-28
Potential Accident, Bounding Scenario	In room waste package breach (underground operations)	L&ILW	OPG (2011), Table 7-28
Potential Accident, Bounding Scenario	Cage fall with waste package breach (underground operations)	L&ILW	OPG (2011), Table 7-28
Potential Accident, Bounding Scenario	Ventilation system failure (underground operations)	All (L&ILW)	OPG (2011), Table 7-28
High impact accident scenario	Breach accidents	Ash containers	OPG (2011), p. 468
High impact accident scenario	Fire accidents	Box compacted and non-processible wastes	OPG (2011), p. 468
High impact accident scenario	Fire accidents	Multiple packages in an emplacement room	OPG (2011), p. 468
Bounding Category 2 event sequence	Seismic event resulting in low level waste facility collapse and failure of HEPA filters and ductwork in other facilities	HEPA filters and low level waste facility inventory	U.S. DOE (2009), Table 1.8-26
Bounding Category 2 event sequence	Breach of sealed HLW canisters in a sealed transportation cask	5 HLW canisters	U.S. DOE (2009), Table 1.8-26
Bounding Category 2 event sequence	Breach of sealed HLW canisters in an unsealed waste package	5 HLW canisters	U.S. DOE (2009), Table 1.8-26
Bounding Category 2 event sequence	Breach of sealed HLW canister during transfer (one drops onto another)	2 HLW canisters	U.S. DOE (2009), Table 1.8-26
Bounding Category 2 event sequence	Breach of un-canistered commercial SNF in a sealed truck transportation cask in air	4 PWR or 9 BWR commercial SNF	U.S. DOE (2009), Table 1.8-26

Accident Type	Design Basis Accidents	Waste	Reference
Bounding Category 2 event sequence	Breach of un-canistered commercial SNF in an unsealed truck transportation cask in pool	4 PWR or 9 BWR commercial SNF	U.S. DOE (2009), Table 1.8-26
Bounding Category 2 event sequence	Breach of a sealed dual-purpose canister in air	36 PWR or 74 BWR commercial SNF	U.S. DOE (2009), Table 1.8-26
Bounding Category 2 event sequence	Breach of commercial SNF in unsealed dual-purpose canister in pool	36 PWR or 74 BWR commercial SNF	U.S. DOE (2009), Table 1.8-26
Bounding Category 2 event sequence	Breach of a sealed TAD canister in air within facility	21 PWR or 44 BWR commercial SNF	U.S. DOE (2009), Table 1.8-26
Bounding Category 2 event sequence	Breach of commercial SNF in unsealed TAD canister in pool	21 PWR or 44 BWR commercial SNF	U.S. DOE (2009), Table 1.8-26
Bounding Category 2 event sequence	Breach of un-canistered commercial SNF assembly in pool (one drops onto another)	2 PWR or 2 BWR commercial SNF	U.S. DOE (2009), Table 1.8-26
Bounding Category 2 event sequence	Breach of un-canistered commercial SNF in pool	1 PWR or 1 BWR commercial SNF	U.S. DOE (2009), Table 1.8-26
Bounding Category 2 event sequence	Fire involving low level waste facility inventory	Combustible inventory	U.S. DOE (2009), Table 1.8-26
Bounding Category 2 event sequence	Breach of a sealed truck transportation cask due to a fire	4 PWR or 9 BWR commercial SNF	U.S. DOE (2009), Table 1.8-26
Accident scenario	Fall of the transport cask in transport space (translated)	SNF	Posiva, Kukkola (2009), Table 5. Rossi and Suolanen 2013, Section 2.5
Accident scenario	Fall of the transport cask lid in handling cell on top of transport cask (translated)	SNF	Posiva, Kukkola (2009), Table 5. Rossi and Suolanen 2013, Section 2.5
Accident scenario	Fall of the fuel bundles in handling cell (translated)	SNF	Posiva, Kukkola (2009), Table 5. Rossi and Suolanen 2013, Section 2.5
Accident scenario	Fall of the spent fuel canister in the transport shaft (translated)	SNF	Posiva, Kukkola (2009), Table 5. Rossi and Suolanen 2013, Section 2.5
Accident scenario	Fall of the spent fuel canister to deposition hole (translated)	SNF	Posiva, Kukkola (2009), Table 5. Rossi and Suolanen 2013, Section 2.5
Accident scenario	Rock fall in the deposition tunnel while spent fuel canister is being installed (translated)	SNF	Posiva, Kukkola (2009), Table 5. Rossi and Suolanen 2013, Section 2.5
Accident scenario[2]	Rock fall in the deposition tunnel while spent fuel canister is being installed (translated)	SNF	Posiva, Kukkola (2009), Table 5. Rossi and Suolanen 2013, Section 2.6.4
H3/H4	Large scale fire	SNF	SKB (2010), Kapitel 8, Chapter 3
H3/H4	Missile with large consequences	SNF	SKB (2010), Kapitel 8, Chapter 3
H3/H4	Dropping lifting device on canister	SNF	SKB (2010), Kapitel 8, Chapter 3

---

[2] Unclear whether this was a DBA, BDBA or upset.

Accident Type	Design Basis Accidents	Waste	Reference
H3/H4	Prohibited chemical substances	SNF	SKB (2010), Kapitel 8, Chapter 3
H3/H4	Uncontrolled amount of inflowing water	SNF	SKB (2010), Kapitel 8, Chapter 3
H3/H4	Defects in canister or buffer	SNF	SKB (2010), Kapitel 8, Chapter 3
H3/H4	Defects in rock	SNF	SKB (2010), Kapitel 8, Chapter 3
H3/H4	Malfunctioning concrete plug	SNF	SKB (2010), Kapitel 8, Chapter 3
H3/H4	Deficient bentonite quality and installation of backfill	SNF	SKB (2010), Kapitel 8, Chapter 3
H3/H4	Flooding	SNF	SKB (2010), Kapitel 8, Chapter 3
H3/H4	Extreme flooding causing canister moving vehicle or radiation shielding to get stuck in connection to moving and disposal activities	SNF	SKB (2010), Kapitel 8, Chapter 3
H3/H4	Detonation around the capsule (excavation)	SNF	SKB (2010), Kapitel 8, Chapter 3
H3/H4	Earthquake	SNF	SKB (2010), Kapitel 8, Chapter 3
H3/H4	Extreme weather conditions	SNF	SKB (2010), Kapitel 8, Chapter 3
H3/H4	Extreme weather conditions, causing effects underground	SNF	SKB (2010), Kapitel 8, Chapter 3
S1*	Scissor lift failure: The open road/rail transportation cask is dropped before transfer of the fuel modules to the Module Handling Cell	UF	OHN (1994), Section 6.1.2.3
S2*	Scissor lift and ventilation failure: Same as S1, plus a failure in the ventilation system so that the airborne effluent by-passes the HEPA filters	UF	OHN (1994), Section 6.1.2.3
S3*	Overhead carriage failure: A loaded fuel module is dropped on top of another loaded fuel module in the Module Handling Cell	UF	OHN (1994), Section 6.1.2.3
S4*	Overhead carriage and ventilation failure: Same as S3, plus a failure in the ventilation system so that the airborne effluent by-passes the HEPA filters	UF	OHN (1994), Section 6.1.2.3
V1**	Failure in the shaft and hoisting facilities: An used fuel container is dropped down the shaft	UF	OHN (1994), Section 6.1.2.3
V2**	Failure in the shaft and hoisting facilities plus ventilation failure: Same as V1, plus a failure in the ventilation system so that the airborne effluent by-passes the HEPA filters	UF	OHN (1994), Section 6.1.2.3

* S = Surface event; ** V= Vault event

A.3 BEYOND DESIGN BASIS ACCIDENTS IDENTIFIED IN REVIEWED LITERATURE

In this appendix the DBAs compiled from NDA (2010), OPG (2011), WIPP (2013), Rossi and Suolanen (2013), SKB (2010), and OHN (1994) are presented. Because the terminology in different countries varies, local terminology of each document is used for describing the scenario. Bounding event implies that the event was selected from binned scenarios of the similar incidents, the selected having the most significant results.

The following abbreviations are used in the table:

L&ILW	Low and Intermediate Level Waste
MIX	Mixture of waste types, see reference for details
OHN	Ontario Hydro Nuclear
OPG	Ontario Power Generation
SNF	Spent Nuclear Fuel
TRU	Transuranic
UF	Used Fuel

Accident type	Beyond Design Basis Accidents	Waste	Organization/ Reference
BDBA	Wind events (high wind or tornado) that result in a WHB collapse	TRU	WIPP (2013), Section 3.4.3
BDBA	Snow load event that results in roof collapse	TRU	WIPP (2013), Section 3.4.3
BDBA	Seismic event that results in a building collapse with a subsequent fire	TRU	WIPP (2013), Section 3.4.3
BDBA	NPH events that lead to waste shaft tower collapse	TRU	WIPP (2013), Section 3.4.3
SA	Aircraft crash on site (not considered as severe accident but assessed)	MIX	NDA (2010), Section 5.6.2
BDBA	Roof collapse due to major earthquake (moved to be considered as a bounding accident scenario)	L&ILW	OPG (2011)
Event recognised, not considered further	Dropping of a fuel module in the receiving pool, due to failure of the module handling tool	UF	OHN (1994), Section 6.1.2.3
Event recognised, not considered further	Release of radioactivity due to loss of cooling	UF	OHN (1994), Section 6.1.2.3
Event recognised, not considered further	Several possible failure modes during the fuel packaging procedure	UF	OHN (1994), Section 6.1.2.3
Event recognised, not considered further	Failure of the airlocks between the Fuel Packaging Cell and the Head frame building	UF	OHN (1994), Section 6.1.2.3
Event recognised, not considered further	Abnormal conditions that could occur during the transfer of the casks from the Fuel Packaging Cell to the waste shaft	UF	OHN (1994), Section 6.1.2.3
Event recognised, not considered further	Transportation equipment failures in the facility	UF	OHN (1994), Section 6.1.2.3
Event recognised, not considered further	Container emplacement accidents	UF	OHN (1994), Section 6.1.2.3
Considered in post-closure assessment	Emplacement of a Defective Disposal Container in the Vault	UF	OHN (1994), Section 6.1.2.3

Accident type	Beyond Design Basis Accidents	Waste	Organization/ Reference
Event recognised, not considered further	Internal fires	UF	OHN (1994), Section 6.1.2.3
Event recognised, not considered further	Criticality due to flooding	UF	OHN (1994), Section 6.1.2.3
Event recognised, not considered further	Cave-in serious enough to result in fuel container damage	UF	OHN (1994), Section 6.1.2.3
Event recognised, not considered further	Aircraft crash	UF	OHN (1994), Section 6.1.2.3
Event recognised, not considered further	Earthquake	UF	OHN (1994), Section 6.1.2.3
Event recognised, not considered further	Forest fire	UF	OHN (1994), Section 6.1.2.3
External threat, analysed to some point, not further	Small aircraft impact	SNF	Posiva: Rossi and Suolanen (2013) Chapter 10
External threat, analysed to some point, not further	Earthquake	SNF	Posiva: Rossi and Suolanen (2013) Chapter 10
External threat, analysed to some point, not further	Extreme weather conditions	SNF	Posiva: Rossi and Suolanen (2013) Chapter 10, flooding discussed also in section 2.6.5
External threat, analysed to some point, not further	Extreme weather conditions	SNF	Posiva: Rossi and Suolanen (2013) Chapter 10, flooding discussed also in section 2.6.5
External threat, analysed to some point, not further	Forest fire	SNF	Posiva: Rossi and Suolanen (2013) Chapter 10
Internal threat, analysed to some point, not further	Breaking of pipes or canisters causing leakage of radioactive water	SNF	Posiva: Rossi and Suolanen (2013), Section 2.6
Internal threat, analysed to some point, not further	Loss of SNF cooling, overheating and fire	SNF	Posiva: Rossi and Suolanen (2013), Section 2.6
Internal threat, analysed to some point, not further	Accidents concerning explosives in the repository	SNF	Posiva: Rossi and Suolanen (2013), Section 2.6

APPENDIX B: PROCESS STEPS FOR THE MARK II CONCEPTUAL DESIGN

STEP NO.	DESCRIPTION OF PROCESS STEP
-	**Used Fuel Packaging Plant activities (Figure 14)**
-	**Receiving and handling UFTP in the basement (Figure 14)**
1	Drive transport trailer to airlock
2	Inspect UFTP transport vehicle
3	Open weather cover on UFTP transport vehicle
4	Perform smear test
5	Perform pre-lifting inspection
6	Detach tie-downs of loaded UFTP
7	Attach UFTP to OTC lifting device
-	**UFTP activities, UFTP Receiving and Shipping Hall in the basement (Figure 14)**
8	Move UFTP from transport trailer into storage or on transfer pallet in UFTP receiving and shipping hall with 40 tonne OTC (from airlock)
9-1	Detach UFTP from OTC in UFTP storage
9-2	Attach OTC on UFTP in UFTP storage
9-3	Move UFTP from storage to transfer pallet using OTC
10	Manually remove impact limiter with assistance of OTC
11	Manually transfer impact limiter to storage area with assistance of OTC
-	**UFTP activities, vent cell in the basement (Figure 14)**
12	Move transfer pallet into UFTP vent cell
13	Inspect UFTP
14	Vent UFTP
15	Remove UFTP lid bolts by Master Slave Manipulator
16-1	Lift UFTP on open top elevator from basement to airlock from above to UFTP at ground level
16-2	Open module handling cell door on ground level
17	Remove UFTP lid using OTC
18	Replace UFTP lid using OTC
-	**Dry module storage operations (alternative to normal process) (Figure 14)**
19-1	Open dry storage room door
19-2	Transfer full module in module handling cell using OTC
19-3	Transfer full module to dry storage using OTC
19-4	Close dry storage room door
19-5	Open dry storage room door
19-6	Transfer full module to module handling cell using OTC
19-7	Lift full module to module lay down area using OTC
19-8	Close dry storage room door
-	**Empty UFTP activities (Figure 14)**
20	Close access to module handling cell and move empty UFTP to vent cell in the basement via elevator
21	Measure contamination of empty UFTP, decontaminate if required, and attach lid bolts on empty UFTP
22	Transfer empty UFTP from vent cell on transfer pallet through airlock to UFTP shipping and receiving hall in the basement
23	Transfer impact limiter from storage back to empty UFTP
24	Attach impact limiter on empty UFTP
25	Attach OTC lifting device on empty UFTP

STEP NO.	DESCRIPTION OF PROCESS STEP
26	Transfer empty UFTP to storage area or transport trailer
27	Attach tie-downs of (empty) UFTP on trailer in airlock
28	Close weather cover on UFTP transport trailer
29	Inspect UFTP transport trailer in airlock
30	Drive transport trailer through port to UFTP shipping and receiving hall airlock
-	**Module handling cell and module distribution activities (Figure 15)**
31	Unload upper module using OTC to lay down area in module handling cell
32	Unload lower module using OTC to lay down area in module handling cell
33	Transfer module from lay down area using OTC onto inter-airlock trolley
34	Move inter-airlock trolley from module handling cell to fuel module distribution hall
35	Exchange module in distribution hall (full module / empty module)
36	Return empty module from distribution hall to dry storage area using OTC
-	**Fuel from modules to baskets handling activities (Figure 16)**
37	Receive full module on inter-airlock trolley from fuel module distribution hall via airlock onto module positioning worktable (with scissor lift) in fuel handling cell
38-1	Align module tube to push location
38-2	Fuel push to inspection
38-3	Retract ram clear
38-4	Undergo fuel inspection
38-5	Fuel push (2 bundles at a time) through shielding wall and basket interface sleeve into UFC basket tube
38-6	Retract ram full
	Repeat steps 38-1 to 38-6 23 times
39-1	Transfer empty fuel module from worktable to module transfer position
39-2	Transfer empty fuel module to fuel module distribution hall
40	Transfer UFC to UFC head installation position
41	Advance and engage UFC head installation tooling
42	Release head and retract installation tooling
43	Transfer loaded UFC on flask trolley to transfer flask
44	Exchange flasks
45	Repeat steps 38 and 44
-	**Receiving empty UFC for loading with fuel bundles (Figure 16)**
46-1	Transfer empty UFC on flask trolley from transfer flask to fuel loading cell
46-2	Extract empty UFC on flask trolley from transfer flask
46-3	Position trolley to UFC head removal position
46-4	Advance and engage head removal tooling
47	Retract head removal tooling
48-1	Transfer open UFC to positioning worktable
48-2	Transfer open UFC from transfer position to UFC basket orientation vision system
48-3	Get UFC basket orientation image by vision system
48-4	Advance UFC to UFC fuel load position
48-5	Align UFC basket tubes (using feedback from vision system) to transfer port and shroud position
48-6	Load 4 bundles to each basket tube
49-1	Disengage shroud and transfer UFC to UFC transfer position
49-2	Transfer UFC to head installation position
49-3	Advance and engage head installation tooling

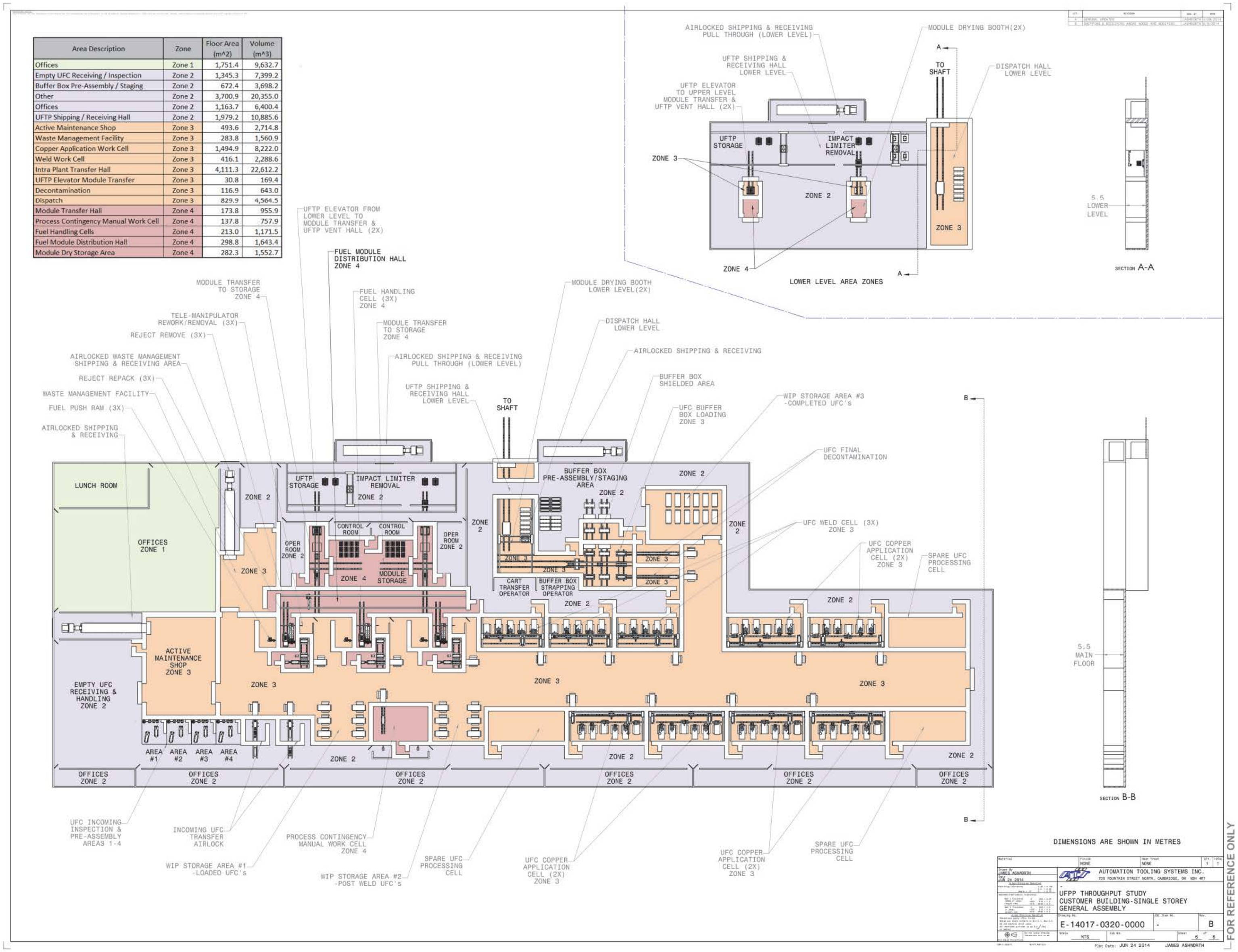
STEP NO.	DESCRIPTION OF PROCESS STEP
50-1	Install hemispherical head
50-2	Release head and retract installation tooling
51	Transfer loaded UFC on flask trolley to transfer flask
52	Exchange flasks
-	**Empty UFC activities**
53	Receive empty UFC in empty UFC receiving and handling area
54	Move UFC components to pre-assembly and inspection area
55	Inspect, assemble components manually to kit with assistance of cell jib crane and kit cart, and mark qualified empty UFC with unique ID
56	Transfer marked and qualified UFC kits on their carts to processing area loading station
57	With UFC transfer flask already docked to loading site and empty flask trolley extracted, open shielding door to UFC load cell
58	Grip UFC kit using OTC from cart and transfer into loading area
59	Lower UFC kit onto flask trolley and retract trolley
60	Close shielding door and open UFC processing shielding door
61	Retract flask trolley to transfer flask and close UFC processing shielding door
62	Transfer UFC kit to fuel handling cell for fuel loading
-	**UCF Processing cell activities**
63	Transfer loaded UFC on flask trolley in transfer flask to processing cell door
64	Extract loaded UFC on flask trolley from transfer flask through processing cell door
-	**UFC Welding process (Welding cell) (Figure 17)**
-	**UFC Welding process**
65-1	Grip loaded UFC on flask trolley using overhead transfer gantry to rotary positioner
65-2	Advance UFC to weld worktable position
65-3	Advance weld worktable and engage joint line inspection tooling
65-4	Inspect joint line
65-5	Retract weld worktable and disengage joint line inspection tooling
65-6	Advance UFC to pre-heat worktable position
65-7	Advance pre-heat induction coil
65-8	Pre-heat weld area to 450°C
65-9	Retract pre-heat induction coil
65-10	Advance UFC to weld worktable position
65-11	Advance weld worktable and engage weld tooling
65-12	Engage Hybrid Laser Arc Welding (HLAW) tack weld
65-13	Engage HLAW circumferential weld
65-14	Retract weld worktable and disengage weld tooling
65-15	Advance UFC to forced air cooling worktable position
65-16	Undergo forced air cooling
65-17	Retract forced air cooling tooling worktable
-	**UFC Weld machining**
65-18	Advance UFC to weld machining worktable position
65-19	Advance weld machining worktable and engage tooling
65-20	Engage weld machining
65-21	Use air blast to remove any remaining chips
65-22	Retract weld machining worktable and disengage tooling
65-23	Cool down welded UFC

STEP NO.	DESCRIPTION OF PROCESS STEP
-	**UFC Weld NDE inspection**
65-24	Advance UFC to weld NDE worktable position
65-25	Advance NDE tooling worktable and engage tooling
65-26	Undergo NDE inspection scan
65-27	Retract weld NDE tooling and worktable
65-28	Evaluate NDE results
65-29	Advance UFC rotary positioner to unload position
65-30	Grip loaded UFC using overhead transfer gantry from the rotary positioner onto flask trolley
-	**Transfer from welding cell to copper application cell (same procedure also for transfer from copper application cell to dispatch)**
65-31	Dock UFC transfer flask and open weld cell door
65-32	Retract welded UFC on flask trolley
65-33	Undock UFC transfer flask and close weld cell door
65-34	Transfer UFC on flask trolley in transfer flask to copper application cell
65-35	Dock UFC transfer flask and open copper application cell door
65-36	Extract flask trolley from transfer flask
65-37	Undock UFC transfer flask and close copper application cell door
-	**UFC Copper application process (Figure 18)**
-	**Copper application**
65-38	Grip loaded UFC on flask trolley using overhead transfer gantry to rotary positioner
65-39	Advance UFC to grit blast/air blast worktable position
65-40	Advance grit blast/air blast worktable and engage tooling
65-41	Undergo grit blast
65-42	Undergo air blast
65-43	Retract grit/air blast worktable and disengage tooling
65-44	Advance UFC to copper application worktable
65-45	Advance copper application worktable and engage tooling
65-46	Apply copper spray
65-47	Retract copper application worktable and disengage tooling
-	**Copper machining**
65-48	Advance UFC to copper machining worktable position
65-49	Advance copper machining worktable and engage tooling
65-50	Engage copper machining
65-51	Undergo post machine clean-up
65-52	Retract copper machining worktable and disengage tooling
-	**Copper annealing**
65-53	Advance UFC to copper annealing worktable position
65-54	Advance copper annealing worktable
65-55	Ramp up anneal temperature to 350 °C
65-56	Soak copper annealing at 350°C
65-57	Retract annealing worktable
65-58	Advance UFC to forced air cooling worktable position
65-59	Advance forced air cooling worktable
65-60	Undergo forced air cooling
65-61	Retract forced air cooling worktable

STEP NO.	DESCRIPTION OF PROCESS STEP
-	**Copper NDE inspection**
65-62	Advance UFC to copper NDE worktable position
65-63	Advance copper NDE worktable and engage tooling
65-64	Undergo NDE inspection scan
65-65	Retract copper NDE worktable and disengage tooling
65-66	Evaluate NDE results
65-67	Advance UFC rotary positioner to unload position
65-68	Grip loaded UFC using overhead transfer gantry from the rotary positioner onto flask trolley
66-1	Dock UFC transfer flask and open copper application cell door
66-2	Retract flask trolley from transfer flask
66-3	Undock UFC transfer flask and close copper application cell door
67	Transfer processed UFC in transfer flask to decontamination cell
-	**Decontamination cell activities (Figure 19)**
68-1	Dock UFC transfer flask and open decontamination cell door
68-2	Extract flask trolley from transfer flask
68-3	Undock UFC transfer flask and close decontamination cell door
69	Survey UFC and disposition results
70	Decontaminate UFC
-	**Disposing of empty modules**
71	Inspect empty module visually in fuel handling cell
72	Transfer empty module for decontamination and then dispatch for compaction in off-site metals recycling facility
-	**Buffer box loading**
73	Transfer UFC on flask trolley through airlock to buffer box loading area
74	Pre-install buffer box bottom half on removable pallet
75	Place UFC on bottom half of buffer box using OTC
76	Assemble upper buffer block using OTC
77	Install steel cover
78	Transfer buffer box to buffer box transfer area using OTC
79	Perform final preparation operations
80	Transfer buffer box to assembled buffer box transfer position on rail
81	Lift assembled buffer box by another OTC to dispatch hall in the basement for transfer underground or stored in lay down area
-	**Bringing in the empty transport flask in the basement**
82	Move empty UFC transport cask with trolley
83	Inspect transport cask
84	Move trolley and cask next to buffer box installation station
85	Open transport cask lid
-	**Loading the UFC and buffer box into transport cask in the basement**
86	Move UFC and buffer box remotely into transport cask
-	**Shaft operation activities in the basement (from UFPP to underground DGR) (Figure 21)**
87	Connect tow vehicle to loaded UFC transport cask and trolley at UFPP
88	Dispatch transport cask from UFPP and move to main shaft
89	Secure transport cask in shaft
90	Lower transport cask and loaded UFC to repository

STEP NO.	DESCRIPTION OF PROCESS STEP
-	**Underground operation activities**
-	**Preparation of placement room and shielding canopy**
91	Install bentonite levelling layer
92	Place floor plates with ventilation ducts
93	Connect tow vehicle to shielding canopy trolley in underground storage
94	Move tow vehicle with shielding canopy trolley to shielding canopy
95	Connect shielding canopy trolley to shielding canopy
96	Move shielding canopy to next placement room entrance
97	Disconnect shielding canopy trolley from shielding canopy
98	Connect shielding canopy to ventilation and services
99	Move tow vehicle with shielding canopy trolley to underground storage
100	Move placement vehicle to shielding canopy
101	Move placement vehicle inside shielding canopy
102	Close and secure shielding canopy doors
-	**Buffer box and bentonite spacer placement operation**
103	Unsecure load and move trolley with loaded UFC transport cask off shaft cage using tow vehicle
104	Move trolley with loaded UFC transport cask to shielding canopy at placement room entrance
105	Secure UFC transport cask to shielding canopy transfer window
106	Verify alignment of placement vehicle wedge tray and UFC transport cask
107	Connect tow vehicle to hydraulic cylinder cart in underground storage
108	Move hydraulic cylinder cart to UFC transport cask trolley
109	Connect hydraulic cylinder cart to UFC transport cask trolley
110	Connect hydraulic cart to services
111	Install coupling between cylinder and ram on UFC transport cask
112	Open UFC transport cask shielding door
113	Push buffer box from UFC transport cask
114	Verify position of buffer box on placement vehicle wedge tray
115	Retract ram through UFC transport cask
116	Close UFC transport cask door
117	Move placement vehicle remotely to placement position
118	Disconnect hydraulic cylinder cart from services
119	Position placement vehicle wedge tray and eject buffer box
120	Position wedge tray and move placement vehicle remotely back to shielding canopy
121	Move trolley with empty UFC transport cask to underground storage
122	Connect tow vehicle to trolley with bentonite spacer block in underground storage
123	Move trolley with bentonite spacer block to shielding barrier
124	Secure trolley with bentonite spacer block to shielding canopy transfer window
125	Verify alignment of placement vehicle wedge tray and bentonite spacer block
126	Connect trolley for bentonite spacer block to services
127	Move bentonite spacer block from trolley to placement vehicle
128	Verify position of bentonite spacer block on the placement vehicle and retract cylinder
129	Move placement vehicle remotely to placement position
130	Disconnect trolley for bentonite spacer block from services
131	Disconnect trolley for bentonite spacer block from shielding canopy
132	Move trolley for bentonite spacer block to underground storage
133	Position placement vehicle wedge tray and eject bentonite spacer block

STEP NO.	DESCRIPTION OF PROCESS STEP
134	Position wedge tray and move placement vehicle remotely back to shielding canopy
-	**Bentonite pellet placement operation**
135	Move bentonite pellet placement system vehicle to the shielding canopy
136	Move bentonite pellet placement vehicle remotely to last placed buffer box
137	Blow in bentonite pellets
138	Move bentonite pellet placement vehicle out of placement room
139	Move bentonite pellet placement vehicle to underground storage
-	**Floor plate/ventilation duct removal**
140	Connect tow vehicle to trolley with floor plate handling system in underground storage
141	Move trolley with floor plate handling system to shielding canopy
142	Attach floor plate handling system to placement vehicle
143	Move placement vehicle to the floor plate removal position in placement room
144	Pick up floor plate remotely
145	Move placement vehicle out of placement room
146	Detach floor plate handling system and floor plate from placement vehicle
147	Return floor plate system with floor plate to underground storage



Area Description	Zone	Floor Area (m^2)	Volume (m^3)
Offices	Zone 1	1,751.4	9,632.7
Empty UFC Receiving / Inspection	Zone 2	1,345.3	7,399.2
Buffer Box Pre-Assembly / Staging	Zone 2	672.4	3,698.2
Other	Zone 2	3,700.9	20,355.0
Offices	Zone 2	1,163.7	6,400.4
UFTP Shipping / Receiving Hall	Zone 2	1,979.2	10,885.6
Active Maintenance Shop	Zone 3	493.6	2,714.8
Waste Management Facility	Zone 3	283.8	1,560.9
Copper Application Work Cell	Zone 3	1,494.9	8,222.0
Weld Work Cell	Zone 3	416.1	2,288.6
Intra Plant Transfer Hall	Zone 3	4,111.3	22,612.2
UFTP Elevator Module Transfer	Zone 3	30.8	169.4
Decontamination	Zone 3	116.9	643.0
Dispatch	Zone 3	829.9	4,564.5
Module Transfer Hall	Zone 4	173.8	955.9
Process Contingency Manual Work Cell	Zone 4	137.8	757.9
Fuel Handling Cells	Zone 4	213.0	1,171.5
Fuel Module Distribution Hall	Zone 4	298.8	1,643.4
Module Dry Storage Area	Zone 4	282.3	1,552.7

Figure 29: UFPP Conceptual Layout

APPENDIX C: FAILURE MODES IDENTIFIED IN THE FMEA PROCESS

FMEA No.	Step in process	Zone/ Cell /Station	Assembly	Potential Failure Mode	Potential effect(s) of failure	Causes of Failure	Radiological consequence	Affected people	Severity	Occurrence	Detection	RPN	Grouping Number When Appropriate and Note*
II-3.1	Open weather cover on UFTP transport vehicle	Airlock, UFTP receiving and shipping hall	UFTP, weather cover	Jamming of the weather cover	Weather cover opening takes longer than expected	Equipment malfunction	Longer exposure to UFTP radiation	Technician (3) UFTP receiving and shipping hall	3	5	1	15	2 (Weather cover opening problems)
II-4.1	Perform smear test	Airlock, UFTP receiving and shipping hall	Test equipment	Test equipment malfunction, mismatch between equipment	Testing takes longer than expected	Test equipment malfunction	Longer exposure to UFTP radiation (if done only with one device, not probable)	Technician (3) UFTP receiving and shipping hall	4	5	2	40	3 (Smear test failure) Assume no checking equipment at the beginning of shift; mismatch between equipment; equipment is not calibrated
II-4.2	Perform smear test	Airlock, UFTP receiving and shipping hall	UFTP	Does not pass smear test, contamination of UFTP	Evacuation of NEWs, Removal of decontamination	Mistake in packing process	Higher exposure	Technician (3) UFTP receiving and shipping hall	6	1	2	12	3 (Smear test failure) Q/C at sending
II-6.1	Detach tie-downs of loaded UFTP	Airlock, UFTP receiving and shipping hall	Tie-downs	Stuck tie-downs	Tie-downs do not open	Equipment failure	Longer exposure to UFTP radiation	Technician (2) , 40 tonne OTC operator, UFTP receiving and shipping hall	4	4	1	16	1 (Tie down detachment problems)

FMEA No.	Step in process	Zone/ Cell /Station	Assembly	Potential Failure Mode	Potential effect(s) of failure	Causes of Failure	Radiological consequence	Affected people	Severity	Occurrence	Detection	RPN	Grouping Number When Appropriate and Note*
II-6.2	Detach tie-downs of loaded UFTP	Airlock, UFTP receiving and shipping hall	Tie-downs	Jammed tie-downs	Longer to open tie-downs	Equipment failure	Longer exposure to UFTP radiation	Technician (2) , 40 tonne OTC operator, UFTP receiving and shipping hall	4	4	1	16	1 (Tie down detachment problems)
II-7.1	Attach UFTP to OTC lifting device	Airlock, UFTP receiving and shipping hall	40 tonne OTC	OTC does not move to location above UFTP	Longer operation time	Equipment failure / loss of power	Longer exposure to UFTP radiation	Technician (2) , 40 tonne OTC operator, UFTP receiving and shipping hall	3	4	1	12	5 (Drop, slow operation / jamming, failure to grip, stop, unexpected location, collision)
II-7.2	Attach UFTP to OTC lifting device	Airlock, UFTP receiving and shipping hall	OTC attachment pieces	OTC does not get hold of the UFTP	Longer operation time	Equipment failure	Longer exposure to UFTP radiation	Technician (2) , 40 tonne OTC operator, UFTP receiving and shipping hall	4	4	1	16	12 (Does not attach/ detach or takes longer than expected)
II-8.1	Move UFTP from transport trailer into storage or on transfer pallet in UFTP receiving and shipping hall with 40 tonne OTC (from airlock)	UFTP shipping and receiving hall	UFTP/OTC	Does not lift	Longer operation time	Equipment malfunction	Longer exposure	UFTP personnel	4	4	1	16	5 (Drop, slow operation / jamming, failure to grip, stop, unexpected location, collision)
II-8.2	Move UFTP from transport trailer into storage or on transfer pallet in UFTP receiving and shipping hall with 40 tonne OTC (from airlock)	UFTP shipping and receiving hall	UFTP/OTC	Jamming	Longer operation time	Equipment malfunction	Longer exposure	UFTP personnel	4	4	1	16	5 (Drop, slow operation / jamming, failure to grip, stop, unexpected location, collision)

FMEA No.	Step in process	Zone/ Cell /Station	Assembly	Potential Failure Mode	Potential effect(s) of failure	Causes of Failure	Radiological consequence	Affected people	Severity	Occurrence	Detection	RPN	Grouping Number When Appropriate and Note*
II-8.3	Move UFTP from transport trailer into storage or on transfer pallet in UFTP receiving and shipping hall with 40 tonne OTC (from airlock)	UFTP shipping and receiving hall	UFTP/OTC	Falling	UFTP falls on the floor but not damaged	Equipment malfunction	Longer exposure	UFTP personnel	4	4	1	16	5 (Drop, slow operation / jamming, failure to grip, stop, unexpected location, collision) UFTP is designed to withstand drop; assumed that UFTPs are not lifted over each other
II-8.4	Move UFTP from transport trailer into storage or on transfer pallet in UFTP receiving and shipping hall with 40 tonne OTC (from airlock)	UFTP shipping and receiving hall	UFTP/ OTC	OTC guiding failure	UFTP hits another UFTP, but both UFTPs are not damaged	Mechanical/ human error	Longer exposure to UFTP radiation	UFTP personnel	4	4	1	16	5 (Drop, slow operation / jamming, failure to grip, stop, unexpected location, collision) UFTP is designed to withstand drop; assumed that UFTPs are not lifted over each other
II-9-1.1	Detach UFTP from OTC in UFTP storage	UFTP storage	40 tonne OTC	OTC does not detach	Longer operation time	Equipment failure	Longer exposure to UFTP radiation	Technician (2) , 40 tonne OTC operator, UFTP receiving and shipping hall	4	4	1	16	12 (Does not attach/ detach or takes longer than expected)

FMEA No.	Step in process	Zone/ Cell /Station	Assembly	Potential Failure Mode	Potential effect(s) of failure	Causes of Failure	Radiological consequence	Affected people	Severity	Occurrence	Detection	RPN	Grouping Number When Appropriate and Note*
II-9-2.1	Attach OTC on UFTP in UFTP storage	UFTP storage	40 tonne OTC	OTC does not attach	Longer operation time	Equipment failure	Longer exposure to UFTP radiation	Technician (2) , 40 tonne OTC operator, UFTP receiving and shipping hall	4	4	1	16	12 (Does not attach/ detach or takes longer than expected)
II-9-3.1	Move UFTP from storage to transfer pallet using OTC	UFTP shipping and receiving hall	UFTP/ OTC	Falling	UFTP falls on the floor but not damaged	Equipment malfunction	Longer exposure to UFTP radiation	UFTP personnel	4	4	1	16	5 (Drop, slow operation / jamming, failure to grip, stop, unexpected location, collision) UFTP designed to withstand drop; low height operation
II-9-3.2	Move UFTP from storage to transfer pallet using OTC	UFTP shipping and receiving hall	UFTP/ OTC	Does not lift	Longer operation time	Equipment malfunction	Longer exposure to UFTP radiation	UFTP personnel	4	4	1	16	5 (Drop, slow operation / jamming, failure to grip, stop, unexpected location, collision)
II-9-3.3	Move UFTP from storage to transfer pallet using OTC	UFTP shipping and receiving hall	UFTP/ OTC	Jamming	Longer operation time	Equipment malfunction	Longer exposure to UFTP radiation	UFTP personnel	4	4	1	16	5 (Drop, slow operation / jamming, failure to grip, stop, unexpected location, collision)
II-9-3.4	Move UFTP from storage to transfer pallet using OTC	UFTP shipping and receiving hall	UFTP/ OTC	OTC guiding failure	UFTP hits transfer pallet but is not damaged	Mechanical/ human error	Longer exposure to UFTP radiation	UFTP personnel	4	4	1	16	5 (Drop, slow operation / jamming, failure to grip, stop, unexpected

FMEA No.	Step in process	Zone/ Cell /Station	Assembly	Potential Failure Mode	Potential effect(s) of failure	Causes of Failure	Radiological consequence	Affected people	Severity	Occurrence	Detection	RPN	Grouping Number When Appropriate and Note*
													location, collision) UFTP is designed to withstand drop; NEWs can leave immediately after spotting the problem
II-9-3.5	Move UFTP from storage to transfer pallet using OTC	UFTP shipping and receiving hall	UFTP/ OTC	UFTP ends up elsewhere than on the pallet	Longer operation time (corrective action)	Equipment failure	Longer exposure to UFTP radiation	UFTP personnel	4	4	1	16	5 (Drop, slow operation / jamming, failure to grip, stop, unexpected location, collision)
II-9-3.6	Move UFTP from storage to transfer pallet using OTC	UFTP shipping and receiving hall	UFTP/ OTC	UFTP is dropped	UFTP remains intact but delay of operation; fuel inside may be damaged, so processing will need considerations	Equipment failure/ operator mistakes	Longer exposure to UFTP radiation	UFTP personnel	4	4	1	16	5 (Drop, slow operation / jamming, failure to grip, stop, unexpected location, collision) UFTP is designed to withstand drop
II-9-3.7	Move UFTP from storage to transfer pallet using OTC	UFTP shipping and receiving hall	UFTP/ OTC	UFTP positioned wrong (not centered)	Longer operation time	Operator error / mechanical failure	Longer exposure to UFTP radiation	UFTP personnel	4	4	1	16	5 (Drop, slow operation / jamming, failure to grip, stop, unexpected location, collision) Presumed guided action with guides also in pallet

FMEA No.	Step in process	Zone/ Cell /Station	Assembly	Potential Failure Mode	Potential effect(s) of failure	Causes of Failure	Radiological consequence	Affected people	Severity	Occurrence	Detection	RPN	Grouping Number When Appropriate and Note*
II-10	Manually remove impact limiter with assistance of OTC	UFTP shipping and receiving hall	OTC	OTC does not get hold of the impact limiter	Longer operation time	Equipment failure	Longer exposure to UFTP radiation	UFTP personnel	4	4	3	48	12 (Does not attach/ detach or takes longer than expected)
II-11.1	Manually transfer impact limiter to storage area with assistance of OTC	UFTP shipping and receiving hall	OTC	OTC does not get hold of the impact limiter	Longer operation time	Equipment failure	Longer exposure to UFTP radiation	UFTP personnel	4	4	2	32	12 (Does not attach/ detach or takes longer than expected)
II-11.2	Manually transfer impact limiter to storage area with assistance of OTC	UFTP shipping and receiving hall	OTC	Crane does not lift the impact limiter	Longer operation time	Equipment failure / power loss (see 8.2)	Longer exposure to UFTP radiation	UFTP personnel	4	4	1	16	5 (Drop, slow operation / jamming, failure to grip, stop, unexpected location, collision) NEWs can leave immediately after spotting the problem
II-11.3	Manually transfer impact limiter to storage area with assistance of OTC	UFTP shipping and receiving hall	OTC	Crane moves too slow	Longer operation time	Equipment failure / operator mistake	Longer exposure to ambient radiation from UFTP storage	UFTP personnel	4	4	1	16	5 (Drop, slow operation / jamming, failure to grip, stop, unexpected location, collision)
II-11.4	Manually transfer impact limiter to storage area with assistance of OTC	UFTP shipping and receiving hall	OTC	Crane stops	Longer operation time	Equipment failure / power loss (see 8.2)	Longer exposure to ambient radiation from UFTP storage	UFTP personnel	4	4	1	16	5 (Drop, slow operation / jamming, failure to grip, stop, unexpected location, collision)
II-11.5	Manually transfer impact limiter to storage	UFTP shipping and	OTC	Impact limiter is dropped	Longer operation time	Equipment failure	Longer exposure to ambient	UFTP personnel	4	4	1	16	5 (Drop, slow operation /

FMEA No.	Step in process	Zone/ Cell /Station	Assembly	Potential Failure Mode	Potential effect(s) of failure	Causes of Failure	Radiological consequence	Affected people	Severity	Occurrence	Detection	RPN	Grouping Number When Appropriate and Note*
	area with assistance of OTC	receiving hall					radiation from UFTP storage						jamming, failure to grip, stop, unexpected location, collision)
II-12.1	Move transfer pallet into UFTP vent cell	Vent cell	UFTP on transfer pallet	Vent cell door does not open	Longer operation time as UFTP is moved away to make room for repairs	Equipment failure	Longer exposure to UFTP radiation and to ambient radiation from UFTP storage	UFTP personnel	4	4	1	16	6 (Door does not open, opens half way, does not close)
II-12.2	Move transfer pallet into UFTP vent cell	Vent cell	UFTP on transfer pallet	Transfer pallet does not move	Longer operation time as UFTP is moved away to make room for repairs	Equipment failure	Longer exposure to UFTP radiation and to ambient radiation from UFTP storage	UFTP personnel	4	4	1	16	7 (Does not move, moves too slow, only part of the way, too fast, collides)
II-12.3	Move transfer pallet into UFTP vent cell	Vent cell	UFTP on transfer pallet	Stop in doorway	Longer processing time	Equipment failure	Exposure to UFTP	UFTP personnel	4	2	1	8	7 (Does not move, moves too slow, only part of the way, too fast, collides)
II-13	Inspect UFTP	Vent cell	UFTP on transfer pallet / inspection device	Inspection equipment malfunction	Delay	Equipment malfunction/ power loss	Longer exposure time	Operation rooms #1 and #2	3	5	1	15	4 (Vent cell inspection equipment failure)
II-14	Vent UFTP	Vent cell	UFTP on transfer pallet / venting system	Venting system does not function	Delay	Equipment malfunction	Longer exposure time	Operation rooms #1 and #2	3	5	1	15	10 (Does not operate, takes longer than expected)
II-15	Remove UFTP lid bolts by Master Slave Manipulator	Vent cell	UFTP on transfer pallet /bolt removing system	Bolt removing system does not work	Delay	Equipment malfunction	Longer exposure time	Operation rooms #1 and #2	3	5	1	15	11 (Does not attach / detach or takes longer than expected)

FMEA No.	Step in process	Zone/ Cell /Station	Assembly	Potential Failure Mode	Potential effect(s) of failure	Causes of Failure	Radiological consequence	Affected people	Severity	Occurrence	Detection	RPN	Grouping Number When Appropriate and Note*
II-16-1	Lift loaded UFTP on open top elevator from basement to airlock from above to UFTP at ground level	Elevator in vent cell	Elevator	Elevator breaks down	Elevator with UFTP falls down and lid and upper module fall over releasing some radionuclides	Equipment malfunction	Damage to UFTP, release of radionuclides (used fuel damage)	Operation rooms #1 and #2???	7	1	1	7	- UFTP without impact limiter and with loose lid Assume no or malfunction of double- proofed mechanism
II-16-2	Open module handling cell door	Elevator in vent cell	Access door	Access door does not open	Module cannot be moved	Equipment malfunction	Longer exposure time	Operation rooms #1 and #2	3	4	1	12	6 (Door does not open, opens half way, does not close)
II-17.1	Remove UFTP lid using OTC	Vent cell	UFTP on transfer pallet /lid removal system	Lifting system does not function	Delay	Equipment malfunction	Longer exposure time	Operation rooms #1 and #2	3	4	1	12	5 (Drop, slow operation / jamming, failure to grip, stop, unexpected location, collision)
II-17.2	Remove UFTP lid using OTC	Vent cell	UFTP on transfer pallet / lid removal system	Lid is dropped on open UFTP	Lid breaks modules	Equipment malfunction	Damage to used fuel, release of radionuclides	Operation rooms #1 and #2	7	2	1	14	-
II-18	Replace UFTP lid using OTC	Vent cell	UFTP on transfer pallet / lid removal system	Lifting system does not function	Delay	Equipment malfunction	Longer exposure time	Operation rooms #1 and #2	3	4	1	12	5 (Drop, slow operation / jamming, failure to grip, stop, unexpected location, collision)
II-19-1	Open dry storage room door	Module handling cell	Door	Does not open	Module cannot be moved	Equipment malfunction	Longer exposure	Operation rooms #1 and #2	3	4	1	12	6 (Door does not open, opens half way, does not close)

FMEA No.	Step in process	Zone/ Cell /Station	Assembly	Potential Failure Mode	Potential effect(s) of failure	Causes of Failure	Radiological consequence	Affected people	Severity	Occurrence	Detection	RPN	Grouping Number When Appropriate and Note*
II-19-2.1	Transfer full module in module handling cell using OTC	Module handling cell	OTC	Does not move or moves too slowly	Delay	Equipment malfunction	Longer exposure	Operation rooms #1 and #2	3	4	1	12	5 (Drop, slow operation / jamming, failure to grip, stop, unexpected location, collision) Speed limiters (cannot hit walls)
II-19-2.2	Transfer full module in module handling cell using OTC	Module handling cell	OTC	Module is tilted or drops and bundles fall out or fall with module	Bundles potentially break	Equipment malfunction	Release of some radionuclides but no loss of shielding (used fuel damage)	Operation rooms #1 and #2	7	5	1	35	- Assumed no stoppers in modules
II-19-3.2	Transfer full module to dry storage using OTC	Dry storage	OTC	Module drops and bundles fall out of module (can be caused by tilting of the module)	Bundles potentially break	Equipment malfunction	Release of some radionuclides but no loss of shielding (used fuel damage)	Operation rooms #1 and #2	7	5	1	35	- Assumed no stoppers in modules
II-19-5	Open dry storage room door	Dry storage	Door	Does not open	Module cannot be moved	Equipment malfunction	Longer exposure	Operation rooms #1 and #2	3	4	1	12	6 (Door does not open, opens half way, does not close)
II-19-6.2	Transfer full module to module handling cell using OTC	Dry storage	OTC	Module drops and bundles fall out of module (can be caused by tilting of the module)	Bundles potentially break	Equipment malfunction	Release of some radionuclides but no loss of shielding (used fuel damage)	Operation rooms #1 and #2	7	5	1	35	- Assume no or malfunction of double-proofed lifting mechanism; assumed no stoppers in modules

FMEA No.	Step in process	Zone/ Cell /Station	Assembly	Potential Failure Mode	Potential effect(s) of failure	Causes of Failure	Radiological consequence	Affected people	Severity	Occurrence	Detection	RPN	Grouping Number When Appropriate and Note*
II-19-7.1	Lift full module to module lay down area using OTC	Module handling cell	OTC	Does not move or moves too slowly	Delay	Equipment malfunction	Longer exposure	Operation rooms #1 and #2	3	4	1	12	5 (Drop, slow operation / jamming, failure to grip, stop, unexpected location, collision)
II-19-7.2	Lift full module to module lay down area using OTC	Module handling cell	OTC	OTC fails	Module drops on other modules (estimated maximum 4 of 5) in the cell	Equipment failure	Damage to fuel, release of radionuclides	Public, workers in the facility	7	3	1	21	- Assume no or malfunction of double-proofed lifting mechanism
II-23	Transfer impact limiter from storage back to empty UFTP	UFTP shipping and receiving hall	OTC	OTC does not transfer	Delay	Equipment malfunction	Longer exposure	UFTP personnel	2	4	1	8	5 (Drop, slow operation / jamming, failure to grip, stop, unexpected location, collision)
II-24	Attach impact limiter on empty UFTP	UFTP shipping and receiving hall	Impact limiter	Problem in attaching	Delay	Equipment malfunction	Longer exposure	UFTP personnel	2	4	1	8	12 (Does not attach/ detach or takes longer than expected)
II-25	Attach OTC lifting device on empty UFTP	UFTP shipping and receiving hall	OTC	Problem in attaching	Delay	Equipment failure	Longer exposure	UFTP personnel	2	4	1	8	12 (Does not attach/ detach or takes longer than expected)
II-26.1	Transfer empty UFTP to storage area or transport trailer	UFTP shipping and receiving hall	UFTP/ OTC	Does not lift	Longer operation time	Equipment malfunction	Longer exposure	UFTP personnel	2	4	1	8	5 (Drop, slow operation / jamming, failure to grip, stop, unexpected location, collision)

FMEA No.	Step in process	Zone/ Cell /Station	Assembly	Potential Failure Mode	Potential effect(s) of failure	Causes of Failure	Radiological consequence	Affected people	Severity	Occurrence	Detection	RPN	Grouping Number When Appropriate and Note*
II-26.2	Transfer empty UFTP to storage area or transport trailer	UFTP shipping and receiving hall	UFTP/ OTC	Jamming	Longer operation time	Equipment malfunction	Longer exposure	UFTP personnel	2	4	1	8	5 (Drop, slow operation / jamming, failure to grip, stop, unexpected location, collision)
II-26.3	Transfer empty UFTP to storage area or transport trailer	UFTP shipping and receiving hall	UFTP/ OTC	Falling	UFTP falls on floor and potentially breaks	Equipment malfunction	Longer exposure	UFTP personnel	2	1	1	2	5 (Drop, slow operation / jamming, failure to grip, stop, unexpected location, collision) UFTP is designed to withstand drop; assumed that UFTPs are not lifted over each other
II-26.4	Transfer empty UFTP to storage area or transport trailer	UFTP shipping and receiving hall	UFTP/ OTC	OTC guiding failure	UFTP hits another full UFTP, but both UFTPs are not damaged	Mechanical/ human error	Longer exposure	UFTP personnel	4	4	1	16	5 (Drop, slow operation / jamming, failure to grip, stop, unexpected location, collision) UFTP designed to withstand drop; assumed that UFTPs are not lifted over each other; slow speed operation

FMEA No.	Step in process	Zone/ Cell /Station	Assembly	Potential Failure Mode	Potential effect(s) of failure	Causes of Failure	Radiological consequence	Affected people	Severity	Occurrence	Detection	RPN	Grouping Number When Appropriate and Note*
II-31.2	Unload upper module using OTC to lay down area in module handling cell	Module handling cell	Module/ OTC	OTC grip fails	Module drops on lower module	Equipment failure	Damage to used fuel, release of radionuclides	Public, workers in the facility	7	3	1	21	- Assume no or malfunction of double-proofed mechanism
II-32.2	Unload lower module using OTC to lay down area in module handling cell	Module handling cell	Module/ OTC	OTC grip fails	Module drops on open empty UFTP or floor	Equipment failure	Damage to used fuel, release of radionuclides	Public, workers in the facility	7	3	1	21	- Assume no or malfunction of double-proofed mechanism
II-33.2	Transfer module from lay down area using OTC onto inter-airlock trolley	Module handling cell	Module/ OTC	OTC fails	Module drops on other modules (estimated maximum 4 of 5) in the cell	Equipment failure	Damage to used fuel, release of radionuclides	Public, workers in the facility	7	3	1	21	- Assume no or malfunction of double-proofed lifting mechanism
II-33.3	Transfer module from lay down area using OTC onto inter-airlock trolley	Module handling cell	Module/ OTC	OTC fails	Module drops on inter- airlock trolley or floor	Equipment failure	Damage to used fuel, release of radionuclides	Public, workers in the facility	7	3	1	21	- Assume no or malfunction of double-proofed lifting mechanism
II-35.2	Exchange module in distribution hall (full module / empty module)	Fuel module distribution hall	OTC	OTC fails	Module and inter-airlock trolley drop on floor	Equipment failure	Damage to used fuel, release of radionuclides	Public, workers in the facility	7	3	1	21	- Assume no or malfunction of double-proofed lifting mechanism
II-36.1	Return empty module from distribution hall to dry storage area using OTC	Module handling cell	OTC	OTC fails	Empty module drops on other modules (estimated maximum 4 of 5) in the cell	Equipment failure	Damage to used fuel, release of radionuclides	Public, workers in the facility	7	3	1	21	- Assume no or malfunction of double-proofed lifting mechanism
II-38-1.2	Align module tube to push location	Fuel handling cell	Module positioning worktable	Module positioning worktable scissor lift fails	Module drops on scissor lift or slides from scissor lift	Equipment failure	Damage to used fuel, release of radionuclides	Public, workers in the facility	7	1	1	7	-

FMEA No.	Step in process	Zone/ Cell /Station	Assembly	Potential Failure Mode	Potential effect(s) of failure	Causes of Failure	Radiological consequence	Affected people	Severity	Occurrence	Detection	RPN	Grouping Number When Appropriate and Note*
II-38-5.2	Fuel push (2 bundles at a time) through shielding wall and basket interface sleeve into UFC basket tube	Fuel handling cell	Fuel push system	Bundle is inserted on full bundle location in basket	Fuel bundles pushed against each other	Equipment failure	Damage to used fuel, release of radionuclides	Public, workers in the facility	7	1	1	7	- Assume no or malfunction of automatic stopping when counterforce is met ; sensor does not work
II-38-5.3	Fuel push (2 bundles at a time) through shielding wall and basket interface sleeve into UFC basket tube	Fuel handling cell	Fuel push system	Malfunction of chaining of events (basket is not in place when bundle is pushed in, or transfer machine is not in place when bundle is pushed from module)	Falling of bundles	Equipment failure	Damage to used fuel, release of radionuclides	Public, workers in the facility	7	1	1	7	- Assume malfunction of automatic chaining of events
II-51.2	Transfer loaded UFC on flask trolley to transfer flask	Fuel loading cell / transfer hall	Full UFC flask trolley on rails and UFC transfer flask	Trolley does not move or stops	Longer operation time	Equipment failure	Longer exposure	UFC processing	3	5	1	15	7 (Does not move, moves too slow, only part of the way, too fast, collides)
II-51.4	Transfer loaded UFC on flask trolley to transfer flask	Fuel loading cell / transfer hall	UFC transfer flask door	Transfer flask door does not close	Longer operation time	Equipment failure	Longer exposure	UFC processing	3	5	1	15	6 (Door does not open, opens half way, does not close) Assumed no additional scatter if door is left half open
II-52	Exchange transfer flasks	Transfer hall	UFC transfer flask on AGV	AGV system malfunction	Longer operation time	Equipment failure	Longer exposure	UFC processing	3	5	1	15	9 (AGV failure, stop and delay)

FMEA No.	Step in process	Zone/ Cell /Station	Assembly	Potential Failure Mode	Potential effect(s) of failure	Causes of Failure	Radiological consequence	Affected people	Severity	Occurrence	Detection	RPN	Grouping Number When Appropriate and Note*
II-63	Transfer loaded UFC on flask trolley in transfer flask to processing cell door	Transfer hall	Transfer flask on AGV transfer system	AGV system malfunction	Longer operation time	Equipment failure	Longer exposure	UFC processing	3	5	1	15	9 (AGV failure, stop and delay)
II-64.1	Extract loaded UFC on flask trolley from transfer flask through processing cell door	Transfer hall/ processing cell	Door/ transfer flask and UFC flask trolley	Shielding door does not open or opens half way	Longer operation time, potential longer exposure from UFC	Equipment failure	Longer exposure	UFC processing	3	5	1	15	6 (Door does not open, opens half way, does not close) Assumed no additional scatter if door is left half open
II-64.2	Extract loaded UFC on flask trolley from transfer flask through processing cell door	Transfer hall/ processing cells	Transfer flask and UFC flask trolley	UFC flask trolley does not move or stops	Longer operation time	Equipment failure	Longer exposure	UFC processing	3	5	1	15	7 (Does not move, moves too slow, only part of the way, too fast, collides)
II-64.4	Extract loaded UFC on flask trolley from transfer flask through processing cell door	Transfer hall/ processing cells	Transfer flask and UFC flask trolley	Connection failure	Additional exposure, gap is left between transfer flask and processing cell wall	Mismatch in the alignment	Additional exposure	UFC processing	5	3	2	30	Considered in "Shielding Failure" in Section 4.4; excluded from "Operation derived failures) in Section 4.1
II-65-31.2	Dock UFC transfer flask and open weld cell door	Transfer hall/ weld cell	Transfer flask and UFC flask trolley	Connection failure	Additional exposure, gap is left between transfer flask and processing cell wall	Mismatch in the alignment	Additional exposure	UFC processing	5	3	2	30	Considered in "Shielding Failure" in Section 4.4; excluded from "Operation derived failures) in Section 4.1
II-65-32.1	Retract welded UFC on flask trolley	Transfer hall/ weld cell	Transfer flask and UFC flask trolley	UFC flask trolley does not move or stops	Delay of operation/longer exposure	Equipment failure	Longer exposure	UFC processing	3	5	1	15	7 (Does not move, moves too slow, only part of the

FMEA No.	Step in process	Zone/ Cell /Station	Assembly	Potential Failure Mode	Potential effect(s) of failure	Causes of Failure	Radiological consequence	Affected people	Severity	Occurrence	Detection	RPN	Grouping Number When Appropriate and Note*
													way, too fast, collides)
II-65-33	Undock UFC transfer flask and close weld cell door	Transfer hall/ weld cell	Door	Door does not close	Door stays half open causing potential increased radiation from UFC	Equipment failure	Longer exposure	UFC processing	3	5	1	15	6 (Door does not open, opens half way, does not close) Assumed no additional scatter if door is left half open
II-65-34	Transfer UFC on flask trolley in transfer flask to copper application cell	Transfer hall	UFC transfer flask on AGV	AGV system malfunction	Delay	Equipment failure	Longer exposure	UFC processing	3	5	1	15	9 (AGV failure, stop and delay)
II-65-35.1	Dock UFC transfer flask and open copper application cell door	Transfer hall/ copper application cell	UFC transfer flask and door	Does not dock; shielding door does not open or opens half way	Longer operation time	Equipment failure	Longer exposure	UFC processing	3	5	1	15	6 (Door does not open, opens half way, does not close) Assumed no additional scatter if door is left half open
II-65-35.2	Dock UFC transfer flask and open copper application cell door	Transfer hall/ copper application cell	Transfer flask and UFC flask trolley	Connection failure	Additional exposure (gap is left between transfer flask and copper application cell wall)	Mismatch in the alignment	Additional exposure	UFC processing	5	3	2	30	Considered in "Shielding Failure" in Section 4.4; excluded from "Operation derived failures" in Section 4.1
II-65-36.1	Extract flask trolley from transfer flask	Transfer hall/ copper application cell	Transfer flask and UFC flask trolley	UFC flask trolley does not move or stops	Longer operation time	Equipment failure	Longer exposure	UFC processing	3	5	1	15	7 (Does not move, moves too slow, only part of the way, too fast, collides)

FMEA No.	Step in process	Zone/ Cell /Station	Assembly	Potential Failure Mode	Potential effect(s) of failure	Causes of Failure	Radiological consequence	Affected people	Severity	Occurrence	Detection	RPN	Grouping Number When Appropriate and Note*
II-66-1.2	Dock UFC transfer flask and open copper application cell door	Transfer hall/ copper application cell	Transfer flask and UFC flask trolley	Connection failure	Additional exposure (gap is left between transfer flask and copper application cell wall)	Mismatch in the alignment	Additional exposure	UFC processing	5	3	2	30	Considered in "Shielding Failure" in Section 4.4; excluded from "Operation derived failures" in Section 4.1
II-66-2.1	Retract UFC flask trolley from transfer flask	Transfer hall/ copper application cell	Transfer flask and UFC flask trolley	UFC flask trolley does not move or stops	Delay of operation or longer exposure	Equipment failure	Longer exposure	UFC processing	3	5	1	15	7 (Does not move, moves too slow, only part of the way, too fast, collides)
II-66-3	Undock UFC transfer flask and close copper application cell door	Transfer hall/ copper application cell	Door	Door does not close	Door stays half open causing potential increased radiation from UFC	Equipment failure	Longer exposure	UFC processing	3	5	1	15	6 (Door does not open, opens half way, does not close)
II-67	Transfer processed UFC in transfer flask to decontamination cell	Transfer hall	UFC transfer flask on AGV	AGV system malfunction	Delay	Equipment failure	Longer exposure	UFC processing	3	5	1	15	9 (AGV failure, stop and delay)
II-68-1.1	Dock UFC transfer flask and open decontamination cell door	Transfer hall/ decontamination cell	UFC transfer flask and door	Does not dock; shielding door does not open or opens half way	Longer operation time	Equipment failure	Longer exposure	UFC dispatch	3	5	1	15	6 (Door does not open, opens half way, does not close)
II-68-1.2	Dock UFC transfer flask and open decontamination cell door	Transfer hall/ decontamination cell	Transfer flask and UFC flask trolley	Connection failure	Additional exposure, (gap is left between transfer flask and decontamination cell wall)	Mismatch in the alignment	Additional exposure	UFC dispatch	5	3	2	30	Considered in "Shielding Failure" in Section 4.4; excluded from "Operation derived failures)"in Section 4.1

FMEA No.	Step in process	Zone/ Cell /Station	Assembly	Potential Failure Mode	Potential effect(s) of failure	Causes of Failure	Radiological consequence	Affected people	Severity	Occurrence	Detection	RPN	Grouping Number When Appropriate and Note*
II-68-2.1	Extract flask trolley from transfer flask	Transfer hall/ decontamination cell	Transfer flask and UFC flask trolley	UFC flask trolley does not move or stops	Longer operation time	Equipment failure	Longer exposure	UFC dispatch	3	5	1	15	7 (Does not move, moves too slow, only part of the way, too fast, collides)
II-73	Transfer UFC on flask trolley through airlock to buffer box loading area	Decontamination cell	UFC transfer flask on AGV	AGV system malfunction	Delay	Equipment failure	Longer exposure	Buffer box loading	4	5	1	20	9 (AGV failure, stop and delay)
II-74	Re-install buffer box bottom half on removable pallet	Buffer box pre assembly area	Bottom half of buffer box and installation machinery	Machinery does not work	Delay	Equipment failure	Longer exposure	Buffer box loading	4	5	1	20	13 (Does not operate, stops, takes longer than expected)
II-75.1	Place UFC on bottom half of buffer box using OTC	UFC buffer box loading cell	UFC, buffer box bottom half, installation equipment	Problems in transferring UFC to buffer box loading area	Delay	Transfer system malfunction	Longer exposure	Buffer box loading	4	5	1	20	13 (Does not operate, stops, takes longer than expected)
II-75.2	Place UFC on bottom half of buffer box using OTC	UFC buffer box loading cell	UFC, buffer box bottom half, installation equipment	Installation fails	Delay	Installation equipment failure	Longer exposure	Buffer box loading	4	5	1	20	13 (Does not operate, stops, take longer than expected)
II-75.3	Place UFC on bottom half of buffer box using OTC	UFC buffer box loading cell	UFC, buffer box bottom half, installation equipment	Installation fails	UFC is mis-located	Installation equipment failure	Longer exposure	Buffer box loading	4	5	1	20	13 (Does not operate, stops, takes longer than expected) Assumed that UFC cannot drop at this stage, or very low energy dropping causes no damage

FMEA No.	Step in process	Zone/ Cell /Station	Assembly	Potential Failure Mode	Potential effect(s) of failure	Causes of Failure	Radiological consequence	Affected people	Severity	Occurrence	Detection	RPN	Grouping Number When Appropriate and Note*
II-76.1	Assemble upper buffer block using OTC	UFC buffer box loading cell	Equipment to install upper buffer blocks	Installation process slows down or stops	Delay	Equipment failure	Longer exposure	Buffer box loading	4	5	1	20	13 (Does not operate, stops, takes longer than expected)
II-76.2	Assemble upper buffer block	UFC buffer box loading cell	Equipment to install upper buffer blocks	Buffer blocks are dropped on UFC	Delay	Equipment failure	Longer exposure	Buffer box loading	4	5	1	20	13 (Does not operate, stops, takes longer than expected) Assumed that UFC is not harmed by this drop, as UFC is designed to withstand drop
II-77	Install steel cover	UFC buffer box loading cell	Steel strapping equipment	Malfunction	Delay	Equipment failure	Longer exposure	Buffer box loading	4	5	1	20	13 (Does not operate, stops, takes longer than expected)
II-78.1	Transfer buffer box to buffer box area using OTC	UFC buffer box loading cell	OTC / buffer box assembly	OTC does not get grip, moves too slow, stops or jams	Delay	Equipment malfunction	Longer exposure	Buffer box loading	4	5	1	20	13 (Does not operate, stops, takes longer than expected) Assumed limited speed and stoppers (cannot hit wall)
II-78.2	Transfer buffer box to buffer box area using OTC	UFC buffer box loading cell	OTC / buffer box assembly	OTC fails and buffer box is dropped on the floor, but UFC is not damaged	Delay	Equipment malfunction	Longer exposure	Buffer box loading	4	5	1	20	5 (Drop, slow operation / jamming, failure to grip, stop, unexpected location, collision) Assumed that UFC is not harmed by this drop, as UFC is

FMEA No.	Step in process	Zone/ Cell /Station	Assembly	Potential Failure Mode	Potential effect(s) of failure	Causes of Failure	Radiological consequence	Affected people	Severity	Occurrence	Detection	RPN	Grouping Number When Appropriate and Note*
													designed to withstand drop
II-80	Transfer buffer box to assembled buffer box transfer position on rail	UFC buffer box loading cell	Buffer box assembly on rail	Buffer box assembly moves too slow, stops or too fast	Delay	Equipment failure	Longer exposure	Buffer box loading	4	5	1	20	13 (Does not operate, stops, takes longer than expected) Assumed limited speed and stopper (cannot hit walls)
II-81.1	Lift assembled buffer box by another OTC to dispatch hall in the basement for transfer underground or stored in a lay down area	Dispatch hall/ buffer box lay down area	OTC, remotely operated	OTC does not get grip, moves too slow, stops or jams	Delay	Equipment malfunction	Longer exposure	Dispatch hall / buffer box lay down area	3	4	1	12	5 (Drop, slow operation / jamming, failure to grip, stop, unexpected location, collision)
II-81.2	Lift assembled buffer box by another OTC to dispatch hall in the basement for transfer underground or stored in lay down area	Dispatch hall/ buffer box lay down area	OTC, remotely operated	OTC fails and buffer box is dropped from ground level on basement floor or transport cask, but UFC is not damaged	Buffer box is dropped, potentially breaks	Equipment malfunction	Longer exposure / additional exposure	Dispatch hall / buffer box lay down area	4	4	1	16	5 (Drop, slow operation / jamming, failure to grip, stop, unexpected location, collision) Assumed that UFC is not harmed by this drop, as UFC is designed to withstand drop

FMEA No.	Step in process	Zone/ Cell /Station	Assembly	Potential Failure Mode	Potential effect(s) of failure	Causes of Failure	Radiological consequence	Affected people	Severity	Occurrence	Detection	RPN	Grouping Number When Appropriate and Note*
II-87.1	Connect tow vehicle to loaded UFC transport cask and trolley at UFPP	Main shaft hoist area, shaft hoist	Tow vehicle and trolley with transport cask	Tow vehicle does not operate	Delay in operation	Equipment failure	Longer exposure time	Tow vehicle driver and shaft hoist operator	3	4	1	12	8 (Does not move, moves too slow, only part of the way, too fast and de-rails, collides)
II-87.2	Connect tow vehicle to loaded UFC transport cask and trolley at UFPP	Main shaft hoist area, shaft hoist	Tow vehicle and trolley with transport cask	Collision	Delay in operation	Equipment failure, tow vehicle diver mistake	Longer exposure time	Tow vehicle driver and shaft hoist operator	3	4	1	12	8 (Does not move, moves too slow, only part of the way, too fast and de-rails, collides) Assumed that transport cask cannot break due to slow speed collision
II-88.1	Dispatch transport cask from UFPP and move to main shaft	Main shaft hoist area, shaft hoist	Tow vehicle and trolley with transport cask	Tow vehicle does not operate	Delay in operation	Equipment failure	Longer exposure time	Tow vehicle driver and shaft hoist operator	3	4	1	12	8 (Does not move, moves too slow, only part of the way, too fast and de-rails, collides)
II-88.2	Dispatch transport cask from UFPP and move to main shaft	Main shaft hoist area, shaft hoist	Tow vehicle and trolley with transport cask	Collision	Delay in operation	Equipment failure, tow vehicle diver mistake	Longer exposure time	Tow vehicle driver and shaft hoist operator	3	4	1	12	8 (Does not move, moves too slow, only part of the way, too fast and de-rails, collides) Assumed that transport cask cannot break due to slow speed collision
II-89	Secure transport cask in shaft	Main shaft hoist area, shaft hoist	Trolley with transport cask	Problem in securing	Delay	Mechanical/ operational malfunction	Longer exposure time	Shaft operator	4	5	1	20	12 (Does not attach/ detach or

FMEA No.	Step in process	Zone/ Cell /Station	Assembly	Potential Failure Mode	Potential effect(s) of failure	Causes of Failure	Radiological consequence	Affected people	Severity	Occurrence	Detection	RPN	Grouping Number When Appropriate and Note*
													takes longer than expected)
II-90.1	Lower transport cask and loaded UFC to repository	Main shaft hoist	Trolley with transport cask	Breaking of equipment	Entire cage falls with loaded UFC in transport cask	Failure of shaft hoist system	Damage to used fuel, release of radionuclides	Public, workers in the facility	7	1	1	7	- Assume no or malfunction of double-proofing in lifting mechanism and braking system
II-103.1	Unsecure load and move trolley with loaded UFC transport cask off shaft hoist using tow vehicle	DGR, shaft area	Tow vehicle and trolley with transport cask	Tow vehicle does not operate	Delay in operation	Equipment failure	Longer exposure time	Tow vehicle driver	3	4	1	12	8 (Does not move, moves too slow, only part of the way, too fast and de-rails, collides)
II-103.2	Unsecure load and move trolley with loaded UFC transport cask off shaft hoist using tow vehicle	DGR, shaft area	Tow vehicle and trolley with transport cask	Collision	Delay in operation	Equipment failure or tow vehicle diver mistake	Longer exposure time	Tow vehicle driver	3	4	1	12	8 (Does not move, moves too slow, only part of the way, too fast and de-rails, collides) Assumed that transport cask cannot break due to slow speed collision
II-104.1	Move trolley with loaded UFC transport cask to shielding canopy at placement room entrance	Access tunnel	Tow vehicle and trolley with transport cask	Tow vehicle does not operate	Delay in operation	Equipment failure	Longer exposure time	Tow vehicle driver	3	4	1	12	8 (Does not move, moves too slow, only part of the way, too fast and de-rails, collides)
II-104.2	Move trolley with loaded UFC transport cask to shielding canopy at placement room entrance	Access tunnel	Tow vehicle and trolley with transport cask	Collision	Delay in operation	Equipment failure or tow vehicle driver mistake	Longer exposure time	Tow vehicle driver	3	4	1	12	8 (Does not move, moves too slow, only part of the way, too fast and de-rails, collides)

FMEA No.	Step in process	Zone/ Cell /Station	Assembly	Potential Failure Mode	Potential effect(s) of failure	Causes of Failure	Radiological consequence	Affected people	Severity	Occurrence	Detection	RPN	Grouping Number When Appropriate and Note*
													Assumed that transport cask cannot break due to slow speed collision
II-105	Secure UFC transport cask to shielding canopy transfer window	Access tunnel	Tow vehicle and trolley with transport cask, shielding canopy	Does not operate as designed	Delay	Equipment failure or driver mistake	Longer exposure time	Tow vehicle driver	3	4	1	12	12 (Does not attach/ detach or takes longer than expected) Adjusting accounted
II-108	Move hydraulic cylinder cart to UFC transport cask trolley	Access tunnel	Hydraulic cylinder cart and transport cask trolley	Collision	Potential damage to shielding canopy or transport cask	Delay	Longer exposure time	Tow vehicle driver	3	4	1	12	14 (Does not operate, stops, takes longer than expected) Assumed that transfer cask cannot break due to slow speed collision
II-109	Connect hydraulic cylinder cart to UFC transport cask trolley	Access tunnel	Hydraulic cylinder cart and transport cask trolley	Process takes longer than expected	Delay	Equipment malfunction	Longer exposure time	Tow vehicle driver	3	5	1	15	12 (Does not attach/ detach or takes longer than expected)
II-110	Connect hydraulic cart to services	Access tunnel	Hydraulic cylinder cart and transport cask trolley	Process takes longer than expected	Delay	Equipment malfunction	Longer exposure time	Tow vehicle driver	3	5	3	45	12 (Does not attach/ detach or takes longer than expected)
II-111	Install coupling between cylinder and ram on UFC transport cask	Access tunnel	Hydraulic cylinder cart and transport cask trolley	Process takes longer than expected	Delay	Equipment malfunction	Longer exposure time	Tow vehicle driver	3	5	1	15	12 (Does not attach/ detach or takes longer than expected)

FMEA No.	Step in process	Zone/ Cell /Station	Assembly	Potential Failure Mode	Potential effect(s) of failure	Causes of Failure	Radiological consequence	Affected people	Severity	Occurrence	Detection	RPN	Grouping Number When Appropriate and Note*
II-112	Open UFC transport cask shielding door	Access tunnel	Transport cask trolley	Door does not operate	Delay	Equipment malfunction	Longer exposure time	Tow vehicle driver	3	5	1	15	6 (Door does not open, opens half way, does not close)
II-113	Push buffer box from UFC transport cask	Access tunnel	Hydraulic cylinder cart and transport cask trolley	Does not operate as designed	Delay	Equipment malfunction	Longer exposure time	Tow vehicle driver	3	5	1	15	14 (Does not operate, stops, takes longer than expected)
II-114	Verify position of buffer box on placement vehicle wedge tray	Access tunnel	Placement vehicle	Does not operate as designed	Delay	Equipment malfunction	Longer exposure time	Tow vehicle driver	3	5	1	15	14 (Does not operate, stops, takes longer than expected)
II-115	Retract ram through UFC transport cask	Access tunnel	Hydraulic cylinder cart	Does not operate as designed	Delay	Equipment malfunction	Longer exposure time	Tow vehicle driver	3	5	1	15	14 (Does not operate, stops, takes longer than expected)
II-116	Close UFC transport cask door	Access tunnel	Transport cask trolley	Door does not operate	Delay	Equipment malfunction	Longer exposure time	Tow vehicle driver	3	5	1	15	6 (Door does not open, opens half way, does not close)

* Grouping was used to combine similar operations leading to longer or higher worker exposure. This number was used in calculating annual frequencies for failure modes. The number refers to the numeral used in the second column (Failure Model Specification) of Table 8. Dash means potential scenarios causing release of radionuclides in Table 9.

APPENDIX D: VALUES USED IN FREQUENCY CALCULATIONS

CONTENTS

D.1 VALUES USED IN FREQUENCY CALCULATIONS

Initiating Event	**Frequency**	**Section of the Report**
Elevator malfunction leading to elevator fall with loaded UFTP (loose lid without impact limiter)	1.2E-06 per operation	4.1.2.1
Scissor lift failure leading to module drop from positioning table	1.6E-06 per operation	4.1.2.2
Shaft hoist system failure leading to cage fall with loaded UFC	5E-7 a^{-1} (5,000 hours)	4.1.2.3
Overhead transfer crane/gantry failure leading to drop of a suspended load	5.0E-5 per operation	4.1.2.4
Used Fuel transfer machine failure	5.0E-5 per operation	4.1.2.5
Equipment/ vehicle failure or human errors leading longer or additional worker exposure	5.0E-5 per operation	4.1.2.6
Failure modes leading to significant loss of shielding	5.0E-5 per operation	4.4
Fire leading to UFTP (bolted) damage and radionuclide release	7.5E-6 per diesel truck operation	4.6.4
Fire leading to UFC (welded) damage and radionuclide release	7.5E-8 per diesel truck operation	4.6.4
Inadvertent entry scenarios	$>10^{-1}$ a^{-1}	4.8
Condition Failure	**Probability**	**Section of the Report**
Flawed UFTP	1.0E-3	4.10
Flawed UFC	2.0E-4	4.10
Flawed transfer flask/transport cask	1.0E-2	4.10
HEPA filtration unavailable	7.6E-2 a^{-1}	4.2

Annual Package Quantities for the Mark II Conceptual Design	
UFTP	630
Modules	1,260
Fuel bundles	120,960 (In the fuel push operations, two bundles are pushed at the same time)
Mark II UFCs	2,520

D.2 VALUES USED IN FREQUENCY CALCULATIONS – OPERATION DERIVED FAILURES

Operation Derived Failures in Section 4.1.2 (Values used in the calculations for Table 9)

FMEA No.	Failure Mode	Scenario Specification	Failure Frequency per Event	Quantity of Potential Occurrence per Year	Affected Component	Frequency per Year
II-16-1	When an UFTP is lifted on elevator from the basement to the ground level, the elevator fails and drops to the basement with the loaded UFTP (loose lid without impact limiter)	The elevator with UFTP falls down to the basement and the UFTP lid and the upper module fall over releasing some radionuclides (used fuel damage)	1.20E-06	630	UFTP	**7.56E-04**
II-17.2	When the UFTP lid is raised using OTC in the module handling cell, the OTC drops the lid on modules in the open UFTP	The UFTP lid falls (corner first) and breaks top part of The upper module damaging uppermost fuel bundles	5.00E-05	630	UFTP	**3.15E-02**
II-19-2.2	When a full module is transferred using OTC from the open UFTP in the module handling cell, the OTC fails dropping the module	The module is tilted or dropped and the fuel bundles fall out or fall with the module, resulting in the release of some radionuclides but no loss of shielding (used fuel damage)	5.00E-05	1,260	Module	**6.30E-02**
II-19-3.2	When a full module is transferred using OTC from the module handling cell to the dry storage, the OTC fails dropping the module	The module is tilted or dropped and the fuel bundles fall out or fall with the module, resulting in the release of some radionuclides but no loss of shielding (used fuel damage)	5.00E-05	1,260	Module	**6.30E-02**
II-19-6.2	When a full module is transferred using OTC from the dry storage to the module handling cell, the OTC fails dropping the module	The module is tilted or dropped and the fuel bundles fall out or fall with module, resulting in the release of some radionuclides but no loss of shielding (fuel damage)	5.00E-05	1,260	Module	**6.30E-02**

FMEA No.	Failure Mode	Scenario Specification	Failure Frequency per Event	Quantity of Potential Occurrence per Year	Affected Component	Frequency per Year
II-19.7.2	When a full module is lifted using OTC to the lay down area in the module handling cell, the OTC fails dropping the module	The module is tilted or dropped and the fuel bundles fall out or fall with module, release of some radionuclides but no loss of shielding (used fuel damage)	5.00E-05	1,260	Module	**6.30E-02**
II-31.2	When the upper module is loaded from the open UFTP using OTC to the lay down area in the module handling cell, the OTC fails dropping the module	The module is dropped (on lower module) and the used fuel is damaged	5.00E-05	630	Module	**3.15E-02**
II-32.2	When the lower module is loaded from the open UFTP using OTC to the lay down area in the module handling cell, the OTC fails dropping the module	The module is dropped on open empty UFTP or floor and the used fuel is damaged	5.00E-05	630	Module	**3.15E-02**
II-33.2	When a module is transferred using OTC from the lay down area in the module handling cell onto an inter-airlock trolley, the OTC fails dropping the module	The module drops on other modules (estimated maximum 4 of 5) in the module handling cell and the used fuel is damaged	5.00E-05	1,260	Module	**6.30E-02**
II-33.3	When a module is transferred using OTC from the lay down area in the module handling cell onto an inter-airlock trolley, the OTC fails dropping the module	The module drops on the inter-airlock trolley or floor and the used fuel is damaged	5.00E-05	1,260	Module	**6.30E-02**
II-35.2	When the full module and empty module are exchanged using OTC in the fuel module distribution hall, the OTC fails dropping the full module	The module and air- interlock trolley drop on floor and the used fuel is damaged	5.00E-05	1,260	Module	**6.30E-02**

FMEA No.	Failure Mode	Scenario Specification	Failure Frequency per Event	Quantity of Potential Occurrence per Year	Affected Component	Frequency per Year
II-36.1	When an empty module is returned from the fuel module distribution hall and transferred to the lay down area in the module handling cell, the OTC fails dropping the empty module	An empty module drops on other modules (estimated maximum 4 of 5) in the module handling cell and the used fuel is damaged	5.00E-05	1,260	Module	**6.30E-02**
II-38-1.2	When the module tube on the position table is aligned to the push location, the position table scissor lift fails dropping the module	The module is dropped (on scissor lift or slides from scissor lift) and the used fuel is damaged	1.60E-06	1,260	Module	**2.02E-03**
II-38-5.2	When the used fuel bundle is pushed (2 bundles at a time) to the UFC basket tube, the bundle is forced to the already filled places in basket tube	The used fuel bundles break	5.00E-05	60,480	Bundles (two at a time)	**3.02E+00**
II-38-5.3	When the used fuel bundle is pushed (2 bundles at a time) to the UFC basket tube, the basket is not in place due to malfunction of chaining of events	The used fuel bundles fall on floor, damage of the used fuel	5.00E-05	60,480	Bundles (two at a time)	**3.02E+00**
II-90.1	When the transport cask with the loaded UFC is lowered to the repository, the main shaft hoist fails dropping the cage with loaded UFC	The shaft cage falls and the loaded UFC is severely damaged and all fuel bundles are damaged	Discussed in Section 4.1.2.3		UFC	**5.00E-07**