Canadian Nuclear Safety Commission
Commission canadienne de sûreté nucléaire

Severe Accident Progression Without Operator Action

Facility: Darlington
Classification: Unclassified

October 2015

Canada

Executive summary

After the Fukushima Daiichi accident in 2011, one of the many actions committed to by the Canadian Nuclear Safety Commission (CNSC) in its Integrated Action Plan was an assessment and video representation for the public of how a full station blackout could progress in a CANDU reactor in Canada. This video was posted online in January 2013. The CNSC has now followed up with this technical paper, which assesses the timing of a hypothetical blackout, using the Darlington Nuclear Generating Station for illustration.

For the assessment, it was necessary to make the extremely unrealistic assumption that operators take absolutely no action after a full station blackout. The assessment is not used to determine the effects of releases, but rather to assess the potential time and magnitude of releases to determine what operator action can be taken to prevent releases. The assessment identifies the multiple points when operator action becomes critical to stop the progression of an accident. Also, the assessment shows there is adequate time for operator action.

CNSC staff reviewed and agreed with the results of the Darlington Level 2 probabilistic safety assessment (PSA) performed by Ontario Power Generation (OPG), including the analysis of OPG's highly unlikely station blackout scenario which assumed no operator intervention took place. In this scenario, external electrical power sources, standby diesel generators and emergency power generators are unavailable.

CNSC staff's summary of OPG's data paid attention to how reactors currently operating in Canada offer multiple layers of defence-in-depth to prevent accidents. The postulated initiating event of a prolonged station blackout in itself is extremely unlikely and would require multiple failures of plant safety systems to occur. It also depends on the control room staff failing to perform the most basic control room actions in accordance with established safety procedures.

In such a hypothetical event, a release of radioactivity into the environment due to severe core melt can occur at around 11 hours (first stage of release) after this unmitigated station blackout begins. Twenty-three hours into the scenario, the containment integrity can be compromised due to structural failure, leading to a second stage of release at around 25 hours. Lastly, molten core–concrete interaction is expected to occur at around 58 hours, at this point releasing additional fission products into the containment and the environment.

The results of the MAAP4-CANDU severe accident analysis performed by OPG as part of its Level 2 PSA for Darlington indicate that a simple action carried out by the control room staff would provide approximately 8 to 10 hours of additional passive core cooling by supplying readily available water to the boilers. Based on operating procedures, control room staff are instructed to open safety relief valves to depressurize the boilers and allow gravity to feed the water into the boilers. This action could be accomplished from the main control room or secondary control area, and the control room staff would have over 1 hour to perform it. Following this action, field operators would have ample time to connect the portable emergency mitigating equipment and thus secure a continuous supply of coolant to the boilers. Successful connection of emergency mitigating equipment could fully halt progression of the accident. Such actions are regularly exercised and are highly likely to succeed in terminating accident progression and preventing releases of radioactive material to the environment.

The likelihood of such an accident described in this scenario is very low because of the multiple safety defences in place. Nonetheless, since the Fukushima accident, nuclear power plants in Canada have implemented numerous safety enhancements focusing on the prevention and mitigation of severe accidents. These safety enhancements would further reduce the likelihood of severe core damage resulting from a prolonged station blackout and the potential for radioactive releases.

Table of contents

1. Introduction

Using the results of the Level 2 probabilistic safety analysis (PSA) carried out by Ontario Power Generation (OPG), CNSC staff have verified the progression of a hypothetical prolonged station blackout scenario at the Darlington Nuclear Generating Station. This severe scenario pays important attention to how reactors currently operating in Canada offer multiple layers of defence-in-depth to prevent accidents leading to the core melting. This paper also addresses how control room and field operator actions can delay and lead to completely preventing core meltdown, as several cooling options are available to remove decay heat (maintain cooling) by using the plant water sources, even if the normal cooling is lost.

2. Methodology and basic scenario

The results of the MAAP4-CANDU (computer code) analysis that was produced to support the Darlington Level 2 PSA were used to verify the accident progression of a severe accident without operator actions. The specific accident described here is a prolonged station blackout scenario, where external AC electrical power sources, the standby diesel generators and emergency power generators are assumed unavailable. In addition, multiple plant safety systems are assumed to have failed, as outlined in annex A.

3. Background information

CANDU reactors currently operating in Canada offer multiple layers of defence-in-depth to prevent accidents leading to the core melting. In a station blackout, the reactors would shut down automatically to stop the chain reaction, and only the decay heat from the fuel would need to be removed. CANDU reactors rely on human intervention to supply additional coolant and power, in case the normal and safety-grade backup cooling and power supplies are lost and unrecoverable. Many cooling options are available for control room staff or field operators to remove the decay heat using the plant water sources, including external sources of water pumped in by the portable emergency mitigating equipment that has been procured as part of the lessons learned from the Fukushima Daiichi nuclear accident.

The unmitigated scenario described in this report is not considered credible. The postulated initiating event in itself is extremely unlikely. A failure of the control room staff to perform straightforward, basic control room actions in accordance with procedures in the available time (several hours) is not believable. It is part of operational procedures to credit operator actions within 15 minutes for control room actions, and 30 minutes for field actions. The Level 2 Darlington PSA used to prepare this report was performed prior to the Fukushima event, and this progression of the accident does not take into account implementation of emergency mitigating equipment to delay or halt the accident progression.

4. Event progression

The station blackout accident progression has been simulated using the MAAP4-CANDU computer code. Annex A shows that most safety systems and components are assumed to be unavailable for this scenario. (Availability of even a small number of such systems would prevent core melt or calandria failure.) Annex B describes the station blackout accident progression in further detail.

Table 1 – Station blackout scenario progression

Significant events	Time (hr)	Potential key actions to stop or mitigate accident progression
All power lost – reactor is shut down but all active cooling systems' circulation is off	0	• Restore grid power to primary heat transport system and feedwater pumps to establish permanent heat sink • Restore standby generators to power primary heat transport system and feedwater pumps to establish permanent heat sink • Restore emergency power supply to power feedwater pumps and establish permanent heat sink • Depressurize boilers and open valves for emergency feedwater supply into boilers from the station sources • Use emergency mitigating equipment to pump external sources of water into boilers • *Note that restoring boilers as a heat sink must be done while the heat transport system coolant remains nearly full*
Boiler dryout	5.0	
Fuel channel dryout begins **Core damage state 1 (CDS 1)** [1]	6.4	• Use emergency mitigating equipment to pump external sources of water to the calandria • Restore cooling of containment or vent containment through filters • Bring in external generators to re-establish power to emergency coolant injection system pumps to maintain long-term core cooling
Calandria vessel rupture disks burst, relieving calandria vessel pressure and discharging moderator into containment **Core damage state 2 (CDS 2)** [1]	6.4	
Enhanced containment leakage [2]	6.4	
Core debris present in the calandria vessel	8.8	
Core collapses **First stage of release to the atmosphere**	10.7	
Water in calandria vessel completely boils off **Core damage state 3 (CDS 3)** [1]	16.0	• Use emergency mitigating equipment to pump external sources of water to
Catastrophic overpressure failure at the bottom	22.8	

Significant events	Time (hr)	Potential key actions to stop or mitigate accident progression
seam weld (worst scenario) of the shield tank occurs due to inadequate pressure relief		the shield tank • Restore cooling of containment or vent containment through filters
Containment failed (gross structural failure) [3]	22.9	
Calandria vessel fails **Core damage state 4 (CDS 4)** [1]	24.5	
Shield tank side wall melts through – corium relocates to the fuelling machine duct Limited core–concrete interaction occurs before the corium is quenched by water accumulated in the duct **Second stage of release to the atmosphere**	25.0	
Corium becomes uncovered in the fuelling machine duct Molten core–concrete interaction resumes **Third stage of release to the atmosphere**	58.3	• Use emergency mitigating equipment to pump external sources of water to submerge corium within containment • Restore cooling of containment or vent containment through filters • Mitigate effects of molten core–concrete interactions

[1] See annex B for a detailed description.

[2] Enhanced leakage is defined as leakage driven by the pressure above the design limit. Fission product release might not be significant at this time if radionuclides are still entrapped within the corium mass.

[3] Gross structural failure of the reactor building due to high pressure. This is modelled as an irreversible 1 m^2 hole.

Releases of iodine and cesium have been evaluated and presented in table 2; these two radionuclides are representative of short-lived (iodine) and long-lived (cesium) radioactive presence. The predominant chemical form inside containment is assumed to be cesium iodide (CsI) and the radionuclides of most concern are iodine-131 (I-131) and cesium-137 (Cs-137). Using initial core inventories described in the Darlington safety report, the releases of Cs-137 and I-131 can be estimated.

These two radionuclides are also representative of the different radiological hazards: radioactive iodine, if absorbed by a human body in significant quantities, accumulates in the thyroid and may lead to latent thyroid cancers.

The analysis predicts three major stages of radioactivity release occurring at the moments of substantial changes in the state of core melt, as shown in tables 1 and 2 and in figure 1. The results of these simulations show that fission products are released into the environment as early as 10.7 hours into the scenario due to severe core melt combined with increased leakage from containment.

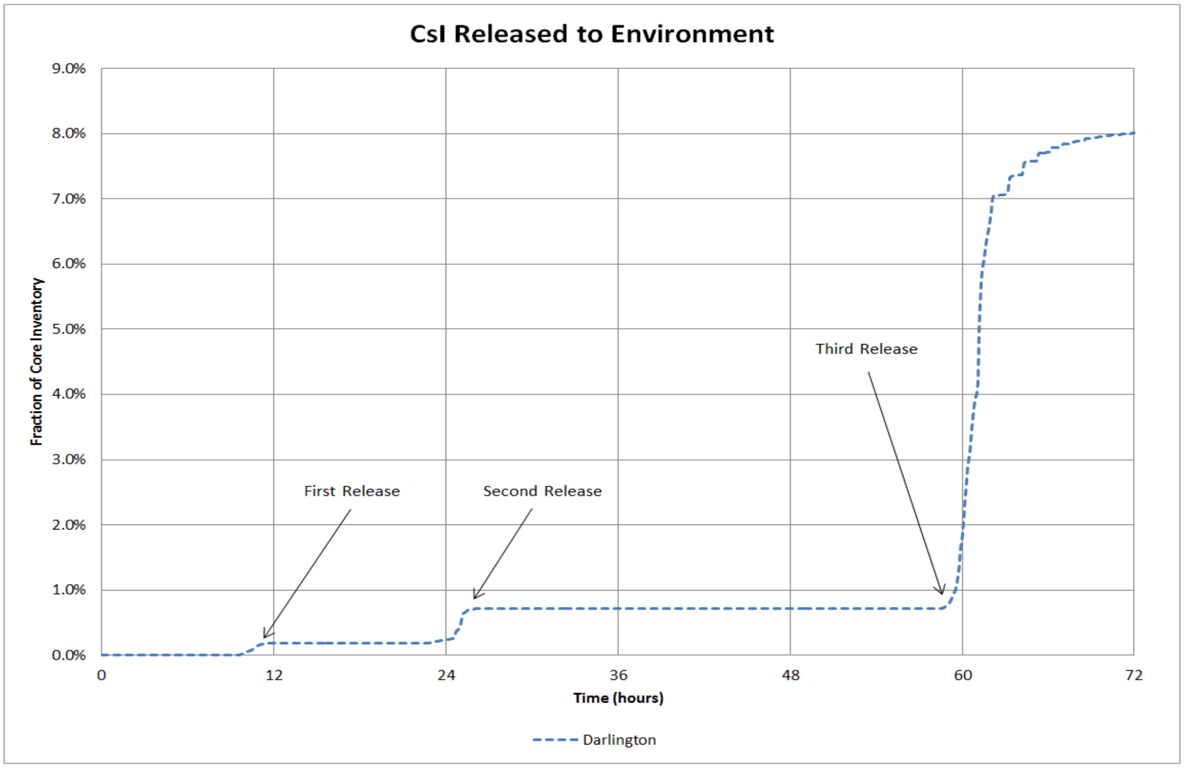
The containment response analysis shows that the containment pressure can cause gross structural failure due to high containment pressure at around 23 hours. However, the second stage of significant radioactive release is not expected until around 2 hours later, when the shield tank fails at the bottom due to overpressure. At that time, the shield tank water inventory and the molten corium mass spill onto the fuelling machine duct floor.

The majority of the fission products released into containment in the Darlington scenario are caused by molten core–concrete interaction, which occurs immediately after the molten fuel relocates to the fuelling machine duct and again when the corium is uncovered. By that time, the containment is expected to lose its integrity and thus allow large releases into the environment. At 58 hours, the amount of water in contact with the corium is insufficient to remove all the decay heat. At that time, molten core–concrete interaction is the main contributor to radioactive releases into the environment.

Table 2 – Station blackout releases

Significant events	Time (hr)	% of initial core inventory release	Cs-137 release (becquerels)	I-131 release (becquerels)
Core collapses. **First stage of release to the atmosphere**	10.7	0.2%	$5.2x10^{14}$	$2.3x10^{16}$
Shield tank side wall melts through. Corium relocates to the fuelling machine duct. Limited core–concrete interaction occurs before the corium is quenched. **Second stage of release to the atmosphere**	25.0	0.7%	$1.8x10^{15}$	$8.2x10^{16}$
Corium becomes uncovered in the fuelling machine duct. Molten core–concrete interaction resumes. **Third stage of release to the atmosphere**	58.3	8.0%	$2.1x10^{16}$	$9.3x10^{17}$

Figure 1 – Amount of CsI released from containment to environment



5. Discussion on the event frequency and fission product releases

5.1 Frequency of event

Station blackout events leading to severe core damage are the dominant contributors to the release category of very large releases (Release Category 1, or RC1), in which the majority of releases occurs after 24 hours. The accident sequence frequencies that are included in the RC1 category are in the order of 1E-7/year range (that is, one in every 10 million years). The Level 2 Darlington PSA used to prepare this report was performed prior to the Fukushima event and does not take into account implementation of emergency mitigating equipment to delay or halt the accident progression.

In the most recent Darlington Level 2 PSA, which was done in 2015, the inclusion of emergency mitigating equipment and removal of overly conservative assumptions represents a more realistic model of the accident scenario. In light of such changes, the event sequences leading to RC1 show a one order of magnitude decrease in the event frequency – that is, one in every 100 million years (1E-8/year).

5.2 Effects of boiler (steam generator) inventory

Darlington's limiting case of a severe accident involving a prolonged station blackout scenario shows that fission product releases are predicted to happen as early as 11 hours after the initiating event. The steam generator water inventories play a very important role in the timing of the initial release. The steam generators act as large heat sinks in the early hours of the accident to remove heat from the heat transport system and thus prevent fuel dryout and damage.

During an accident scenario, the steam generator safety relief valves would automatically open to maintain heat removal from the steam generators. The steam generators would vent non-radioactive steam into the atmosphere, which would remove heat from the steam generators and heat transport system.

If operator actions were credited, a simple action performed by control room staff could greatly delay accident progression. In that scenario, once the steam generators are depressurized, the control room staff are able to initiate the steam generator emergency cooling system to supply water to the steam generators through gravity-fed injection. This action could provide 8 to 10 hours of additional core cooling with the water available at the plant. Due to the reduction of decay heat, the additional core cooling would have a secondary effect of making the water inventories at later stages of the scenario last longer. Field operators employing the emergency mitigating equipment to replenish the source of water supplied to the steam generators prior to boiler dryout (5 hours from the initiating event) would terminate the accident.

6.0 Conclusion

The postulated initiating event of a prolonged station blackout in itself is extremely unlikely and would require multiple failures of plant safety systems to occur. In the scenario described in this report, it is assumed that the control room staff fail to perform straightforward, most basic control room actions in accordance with established safety procedures in the available time; such inaction is not credible. Additionally, the emergency mitigating equipment and severe accident management guidance are not credited in the analysis. Even with these conservative assumptions, the likelihood of a large radioactive release due to a station blackout is well below the established safety goals.

The results of the analytical simulation indicate that a release of fission products, radioactive cesium in particular, could occur as early as 10.7 hours for Darlington. Subsequent releases would be expected to occur at around 25 hours when corium relocates onto the containment floor, and 58 hours when molten core–concrete interaction begins.

It should be noted that a simple control room staff action would provide several hours of core cooling by supplying readily available water to the boilers (approximately 8 to 10 hours, depending on the exact volume of water available for addition to boilers and the reactor power level prior to shutdown). The action is to open the safety relief valves to depressurize boilers and open valves to gravity-feed water into the boilers. This action can be accomplished from the main control room or secondary control area, and the control room staff would have over 1 hour to perform it. The additional hours of passive cooling would give ample time for field operators to connect the portable emergency mitigating equipment and thus secure a continuous supply of coolant.

Successful connection of emergency mitigating equipment can fully halt progression of the accident. Such actions are regularly exercised and have a high likelihood of success in preventing accident progression and releases of radioactivity to the environment. However, such human interventions are not credited in this paper.

Annex A: Availability of systems assumed in MAAP4 CANDU simulation of the station blackout scenario

Plant systems	**Availability**	**System main function**
AC and DC power	Unavailable	Provides power to pumps and instrumentation
Battery power	Available	Provides power to key systems and instrumentation for limited duration
Instrument air	Unavailable	Operates pneumatic valves
Primary side		
Reactor shutdown systems (SDS1/SDS2)	Available	Stop chain reaction
Heat transport pumps	Off	Assure continuous circulation in the primary heat transport system
Moderator cooling	Unavailable	Cools the moderator (calandria) water
Emergency coolant injection system	Unavailable	Adds coolant to the primary heat transport system
Shutdown cooling system (auxiliary cooling system)	Unavailable	Removes the reactor heat when reactor in shutdown mode
Endshield cooling	Unavailable	Removes heat from the endshields of calandria assembly
Deuterium oxide (D_2O – heavy water) feed	Unavailable	Supplies heavy water to reactor systems
Pressurizer heater	Unavailable	Allows pressure to be raised in the pressurizer and thus the primary heat transport system
Secondary side		
Main feedwater	Unavailable	Adds water to boilers from condensers
Auxiliary feedwater	Unavailable	Adds water to boilers
Boiler safety relief valves (SRVs)	Auto	Allow pressure to be quickly reduced on the secondary side of boilers
Atmospheric steam discharge valves	Unavailable	Allow steam to be vented into the atmosphere without actuation of SRVs
Containment systems		
Air cooling units	Unavailable	Cool containment atmosphere
Emergency filtered air discharge system	Unavailable	Allows filtering of atmospheric discharges

Annex B: Description of event progression for a station blackout without operator action

The description below explains how an accident progresses from core damage states 1 to 5.

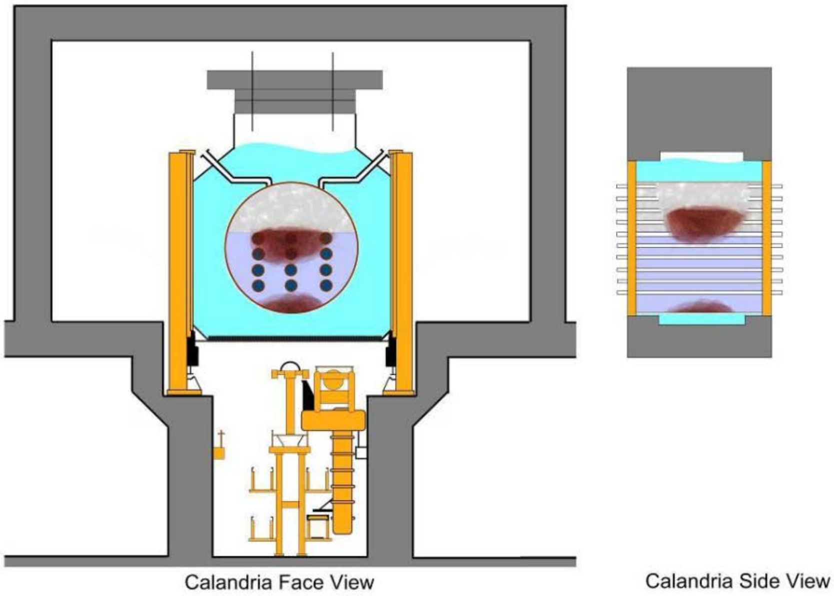
Core damage state 1 (CDS 1): Moderator heat-up and boil-off

After reactor shutdown, the decay heat being generated in the core is transferred through the heat transport system (HTS) to the secondary side water in the steam generators by means of natural circulation flow (thermosyphoning), given that the HTS pumps are tripped. Without feedwater, the pressure in the steam generators increases rapidly, which triggers opening of the boiler safety relief valves shortly after the reactor trip. The escaping steam serves as a temporary means of heat rejection. The steam generators dry out at approximately 5 hours. HTS boil-off depletes the primary side inventory and fuel channel dryout occurs. This event causes bursting of the calandria vessel rupture discs that rapidly depletes the moderator inventory. The first fuel channel (pressure tube and calandria tube) failure is predicted at 8.8 hours.

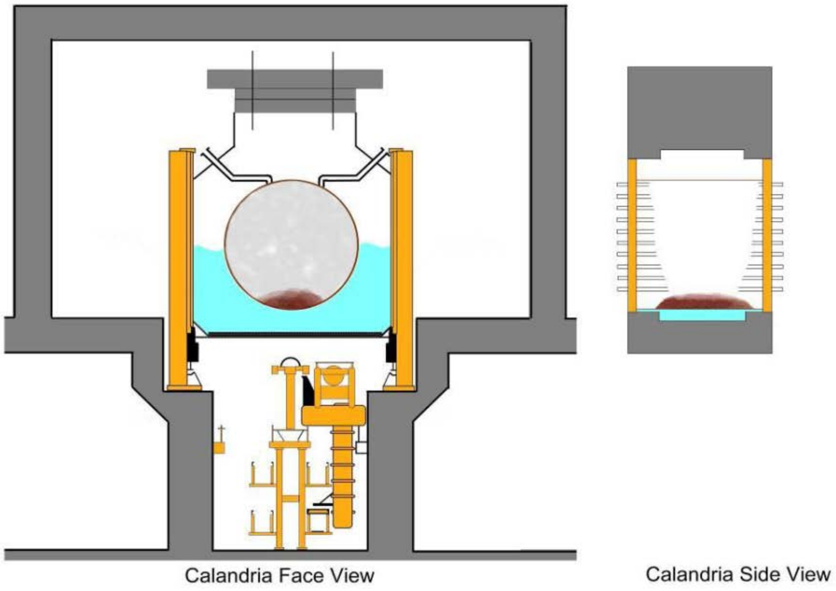
CDS 2 and CDS 3: Core disassembly and collapse

Moderator boil-off occurs through the opening of the calandria vessel rupture discs upon fuel channel failure. The moderator level decreases rapidly and uncovers the upper fuel channels in the core. With the fuel channels no longer submerged in moderator water and now exposed to a steam environment, they heat up significantly. At 10.7 hours, the weight of the debris suspended on the intact channels results in the collapse of the whole core to the bottom of the calandria vessel where it forms a debris bed.

Core damage state 2



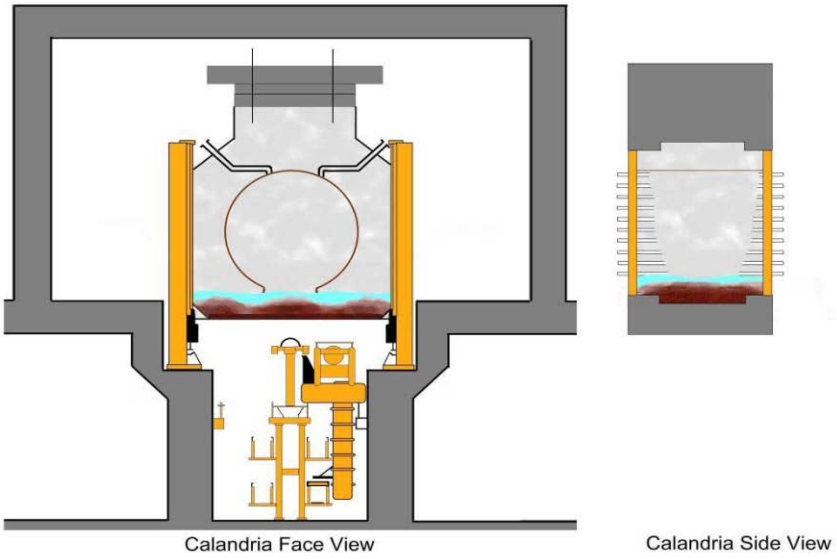
Core damage state 3



CDS 4: Shield tank overpressure and calandria vessel failure

The decay heat dissipation causes an increase in pressure inside the shield tank until a catastrophic failure occurs due to insufficient shield tank overpressure relief capacity in the design. Shield tank rupture is postulated at a bottom seam weld. This explains the rapid decrease in shield tank water mass at 22.8 hours. After depletion of the shield tank inventory, the corium decay heat is transferred to the calandria vessel walls. This continues for about 2 hours, at which point the calandria vessel fails due to overheating and creep. The molten corium mass relocates to the shield tank at this time.

Core damage state 4

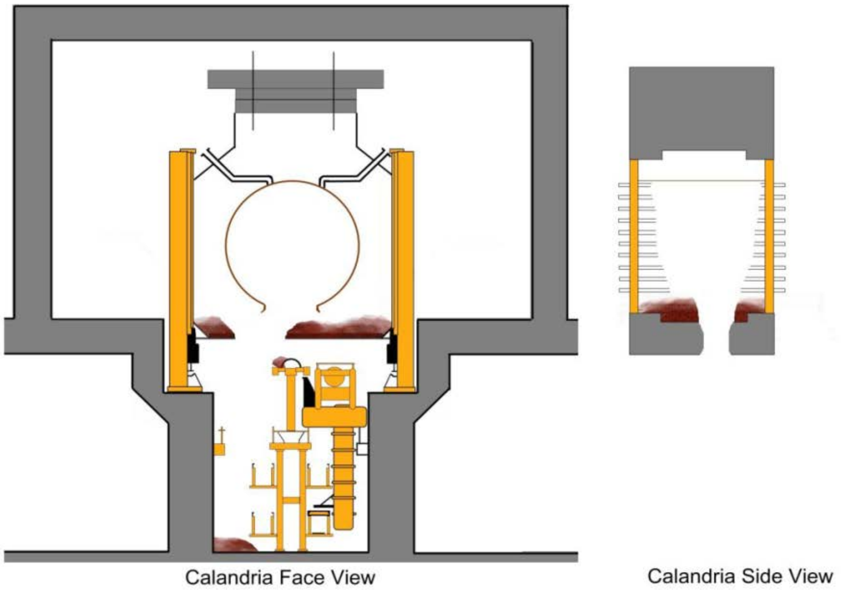


CDS 5: Shield tank failure and corium relocation to the fuelling machine duct

The corium remains in the shield tank for half an hour before its structural integrity is compromised. Shield tank melt-through is predicted by MAAP-CANDU at 25 hours into the accident. Upon failure of the shield tank, the corium drops into the fuelling machine duct (FMD) below.
Upon corium relocation into the FMD, there is potential for a steam explosion to occur as a result of the corium falling into the subcooled water pool on the FMD floor. For this sequence, MAAP-CANDU does predict a steam explosion when the corium enters the FMD.

When the corium relocates to the FMD, it is fully submerged in water. While the corium is covered in water, decay heat causes the water to boil off and limited melting of the concrete floor occurs until 58.3 hours. At that time, the water level is reduced to near the height of the corium pool and the corium temperature increases rapidly again to the concrete melting point.

Core damage state 5



This document is not controlled once printed.