Dynamic Modelling of Severe Accident Management for CANDU Reactors in Probabilistic Safety Assessment

Alexander V. Trifanov
Kinectrics, Toronto, Ontario, Canada
alexander.trifanov@gmail.com

Abstract: It is recognized in the Probabilistic Safety Assessment (PSA) community that modelling of complex accident scenarios may not be adequate using traditional techniques relying on event tree/fault tree approach. The traditional approach has a limited representation of the dynamic response of the plant systems and operating crew to an accident in terms of detailed scenario history, time-dependent process variables, transitioning plant states, change in the success criteria of mitigating systems with time, and change of performance shaping factors for the operator response. Usually, a bounding scenario represents a large spectrum of accident sequences that are less demanding for the required mitigating response. This likely leads to overestimate of the risk and loss of insights on time dependencies of event tree top events.

The severe accident mitigation governed by Severe Accident Management Guidance (SAMG) is especially complex and dynamic as it requires identification of as many as possible viable mitigating strategies to increase the likelihood of regaining control of the plant. SAMG considers unusual equipment configurations, restoration of failed equipment, and use of mobile systems named Emergency Mitigating Equipment (EME) in Canada (equivalent to FLEX in many other jurisdictions). EME is usually stored off-site and involves a relatively long deployment time (several hours). However, it provides flexible configurations for supplying water and electric power to multiple safety loads. Given the above specifics of SAMG, the ability to track the time history of multiple accident sequences and the automatic branching of event tree to account for additional mitigating strategies are critical for crediting SAMG in PSA. The dynamic event tree approach described in multiple publications may be implemented for addressing this problem.

This paper presents a case study for analyzing the dynamics of the severe accident management in CANDU Nuclear Power Plants (NPP) when EME is used for accident mitigation.

Keywords: PRA, PSA, Severe Accident Management, Dynamic PSA.

1. INTRODUCTION

The conventional event tree/fault tree approach used in most of the current PSAs for NPPs represent essentially static models of a limited set of bounding accident sequences. Although these conventional models are based on deterministic analyses of the accident progression and define the system and operator success criteria in terms of response time and equipment configuration, such models have a limited representation of time-dependent changes in the plant status that impact the demand for systems and operators. For example, a slower accident progression gives more time for operator response and increases chances of a successful end state even if the plant system configuration is the same, but this slower accident progression may be combined with (bounded by) a faster accident sequence in the event tree and assessed using more restrictive performance criteria and failure probabilities. Typically, failures on demand and failures during mission are combined in the same top event; however, the timing of system failure may have a significant impact on success of the downstream mitigating strategies.

In principle, the event tree accident sequences can be divided into multiple sub-sequences differentiated by timing of accident progression (e.g., define a large number of categories for Loss of Coolant Accidents (LOCA) and include multiple branches reflecting different timing of Emergency

Coolant Injection (ECI) system response and failure). However, such extensive subdivision of the initiating events and branch points will make the event tree logic unmanageable.

The dynamic event tree analysis techniques described in multiple publications (e.g., [1] to [5]) allow combining time-dependent phenomenological models of the plant status evolution with analysis of system and operator stochastic behavior. This provides means for addressing interactions between the stochastic events (e.g., failures of mitigating systems, human errors, physical phenomena) and dynamic processes in the reactor systems (deterministic response). Thus, probabilistic (frequency) considerations are coupled with deterministic (consequence) considerations. The dynamic models perform automatic branching of event trees in time domain to reflect changes in plant state variables and stochastic variables. This is essentially equivalent to automatic generation of very large event trees that overcome limitations of the traditional modelling techniques, produce more realistic results, and provide additional insights on risk drivers in complex accident scenarios.

Severe Accident Management (SAM) represents one of the complex accident scenarios that are difficult to address by static models. The Severe Accident Management Guidance (SAMG) is implemented once the severe core damage has occurred or is imminent. SAMG is intended to identify as many viable mitigating strategies as possible, including the use of EME, restoration of failed equipment, and novel use of existing equipment to achieve a stable safe plant state.

The accident progression prior to severe core damage is modelled in Level 1 PSA using a limited set of bounding event tree sequences. The mitigating actions governed by SAMG are modelled in Level 2 PSA where the operating crew activities are directed to ensuring stabilization of the damaged reactor core and preventing challenges to the containment integrity. Transition to Level 2 event trees may occur from multiple Level 1 PSA accident sequences, which are typically grouped in representative plant damage states. The plant damage states are bounded by the most conservative accident sequences in the group, both in terms of timing and consequences of the accident progression. The Level 2 event trees are built similarly to Level 1 event trees and include branches representing failures of mitigating functions and phenomenological events that reflect the bounding sequence of the accident progression. Thus, very limited time histories and dependencies are modelled enveloping the bounding scenarios. Given that the success of SAMG mitigating strategies significantly depends on the time available for testing various equipment configurations, implementation of recoveries, and deployment of EME, the realistic representation of the accident sequence timing is very important.

This paper provides an overview of the severe accident management for CANDU reactors, the typical use of EME in SAM, and presents a case study for analyzing the dynamics of the SAMG response in PSA when EME is used for accident mitigation.

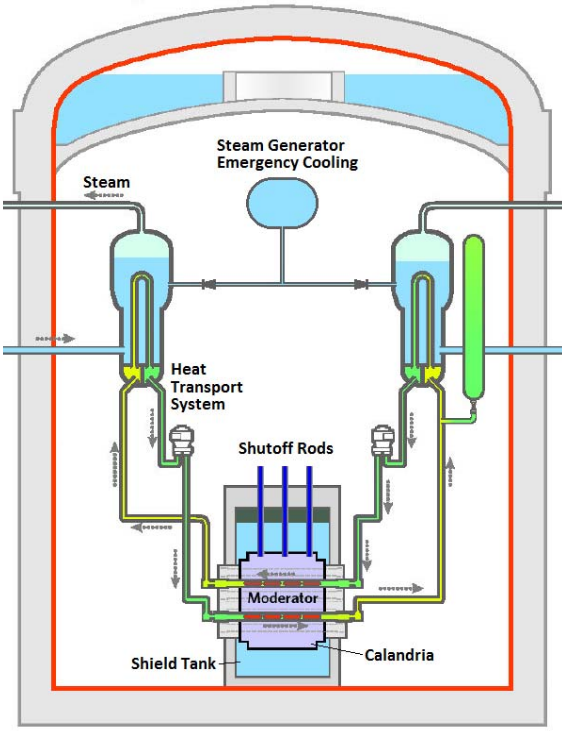
2. OVERVIEW OF THE CANDU ACCIDENT PROGRESSION

Figure 1 represents a generic schematic diagram of CANDU design for illustration of the analysis case considered in this paper. The intent is not to show all details of accident mitigating capabilities, but rather to overview the key features that impact the timing of accident progression prior and after transition to severe accident and, thus, the dynamics of the operators' response.

In case of a total station blackout, the reactor is shut down by one of two independent shutdown systems. The initial water inventory in Steam Generators allows for about one hour of decay heat removal by boil-off through steam relief valves into atmosphere and natural circulation of coolant in the primary heat transport system. Passive supply of water to Steam Generators from the Steam Generator Emergency Cooling System (SGECS) and from the Deaerator Storage Tank allows for an additional approximately eight hours of decay heat removal. During this time, water supply to Steam Generators may be restored from process systems, safety systems or EME, which can then maintain the stable reactor cooling as long as required. EME includes portable pumps and generators that may be connected to multiple safety loads provided the time for deployment of EME and establishing required connections is adequate.

Once the Steam Generator inventory is depleted, the primary heat transport system starts heating up, pressurizes, and releases the coolant inventory into Containment through liquid relief valves. Under the high pressure conditions, there is no means for refilling the heat transport system and maintaining the decay heat removal. This transient continues for about one hour, after which the fuel dries out and pressure tubes containing the fuel start to sag and contact Calandria tubes. The Calandria tubes are submerged during normal operation in the Moderator (heavy water). The Moderators starts to heat up and boil-off through rupture discs into Containment. If the Moderator cooling is restored, or make-up from engineered safety systems or EME is established, the reactor core can be maintained in this stable state using the Moderator heat sink as long as required (state 1 in Figure 2).

Figure 1: Generic Schematic Diagram of CANDU Design

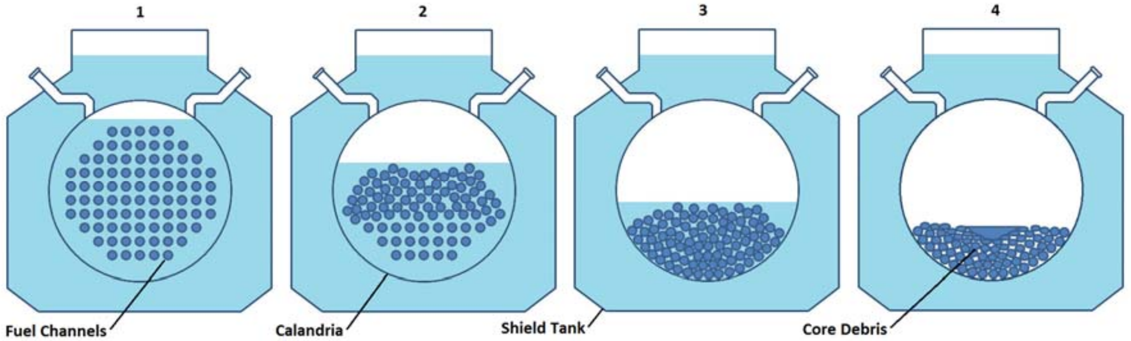


If the Moderator heat sink cannot be maintained, the Moderator will gradually boil-off uncovering fuel channels (states 2 and 3 in Figure 2). The entire Moderator inventory will be depleted in approximately five hours. During this time, the uncovered upper fuel channels will be gradually sagging, rupturing and falling on the lower fuel channels, still submerged in the remaining Moderator inventory, until all of the channels are relocated to the bottom of Calandria vessel and start melting.

At that time, the heat from fuel will be transferred through Calandria walls to the water in the Shield Tank, which will heat up and start boiling off into Containment. If the water inventory in the Shield Tank is maintained by make-up from EME, the core debris will be retained in the Calandria vessel (state 4 in Figure 2). Otherwise, the Shield Tank water will eventually boil-off, the Calandria will fail, the molten debris will fall on the Containment concrete floor and Core-Concrete Interaction (CCI) will be initiated. The CCI can create significant challenges to Containment via release of large amounts of aerosol and hydrogen. Therefore, the primary focus of SAMG in CANDU NPPs is to secure in-vessel retention (IVR) of the fuel debris in the Calandria and prevent challenges to containment associated with IVR.

The timeline of accident progression described above assumes that all of the above water inventories are available at the beginning of the accident. However, if the event is different from the station blackout (e.g., Loss of Coolant Accident (LOCA) or drain of Moderator), or if some of safety systems fail (e.g., failure to depressurize Steam Generators will make the passive make-up to Steam Generators unavailable), the timing will be significantly different. Early in the accident, the decay heat is higher and, for example, if the primary coolant is drained at the beginning of the accident due to a LOCA, the Moderator inventory will give less than five hours of decay heat removal compared to the case described above. This will provide fewer options and shorter time for operators' response.

Figure 2: Stages of Severe Accident Progression in CANDU Reactor Core



3. TYPICAL SEVERE ACCIDENT MANAGEMENT FOR CANDU REACTORS

The typical SAMG for CANDU NPPs is structured similarly to the Westinghouse Owners Group SAMG. SAMG is entered upon indication that severe core damage has occurred or is imminent when the conventional Emergency Operating Procedures (EOP) cannot maintain the fuel cooling. One of key features of SAMG is to identify as many viable mitigating strategies as possible, thereby increasing the likelihood that the accident can still be managed effectively despite the widespread unavailability of equipment. SAMG also provides an effective means to identify the unavailable equipment for which recovery operations should be attempted with the highest priority, or to use existing equipment in novel ways if necessary to regain control of the accident. This involves selection between multiple choices of mitigating strategies and prioritization of the resources to maximize the probability of recovery prior to the further degradation of the plant status.

Immediately following the initiating event, the control room personnel are responsible for taking actions in accordance with EOP. After the event has progressed to severe accident, the control room personnel are expected to recognize the pre-defined cues and transfer the control and command of the accident mitigation to the Site Management Centre (SMC). The SMC collects information from the control room and field operators, identifies the most effective mitigating strategies, and provides directions to the control room and other site resources for implementation of mitigating strategies.

EME plays a significant role during severe accident management, because it provides independent, diverse and flexible means of water and power supply to critical safety loads. However, EME is typically stored remotely from the site to prevent common-cause failure together with engineered site safety systems, if the site is impacted by an external hazard. Therefore, the EME deployment time is usually quite long (several hours). Prioritization of EME deployment to several reactors on a multi-unit site and re-configuration of supply to different loads, if required during the accident progression, involves a dynamic coordination of resources governed by the status of the plant.

4. APPROACH FOR MODELLING OF THE SAMG IN PSA

The dynamics of severe accident mitigation summarized in the previous sections is, in principle, possible to model in static event trees, but would require significant simplifications and introduction of large conservatism to keep a manageable size of event trees. For example, only bounding accident sequences would be considered and only a limited number of mitigating strategies would be explicitly modelled with the most restrictive assumptions on the timing of the accident and performance requirements of the credited systems. Alternatively, a dynamic event tree can simulate the timeline of the severe accident progression using coupled thermal-hydraulic codes, identify the phenomenological events that impact the effectiveness of mitigating strategies, identify the timing and type of cues for operator actions, track the record of the EME deployment time and implementation of other mitigating strategies, simulate various failures of equipment and operator interactions, and determine the feasibility of the available SAMG strategies.

For illustration purpose, Figure 3 represents a simplified event tree for a single-unit event prior to transitioning to severe accident. This type of event tree would be modelled in Level 1 PSA. Figure 4 represents a simplified event tree after transitioning to severe accident. This type of event tree would be modelled in Level 2 PSA. The severe accident progression event tree on Figure 4 intentionally omits branch points representing phenomenological events normally modelled in Level 2 PSA and a number of other mitigating capabilities governed by SAMG. This event tree shows that each Severe Accident Guidance (SAG) may have several implementation strategies (e.g., SAG-1-1 to SAG-1-4). Each of the implementation strategies may be selected as the first priority based on the plant status and availability of mitigating equipment. If the first selected strategy fails, the next best strategy will be selected, and so on until no option remains available in the SAG or it is too late to rely on this SAG.

The event tree in Figure 4 only shows the first iteration for selection of SAG strategies, but does not show implementation of subsequent strategies if the first selected strategy fails. This transition between strategies and how many of them may be tried given the time available in the accident progression may be simulated in the dynamic event tree based on the time history of the accident. Figure 5 shows potential branching of dynamic event tree to simulate iterative selection of SAMG strategies until one strategy successfully mitigates the event or until the accident degrades to the next plant state where SAG-1 becomes ineffective and alternate SAGs should be implemented.

Figure 3: Simplified Event Tree Prior to Transition to Severe Accident

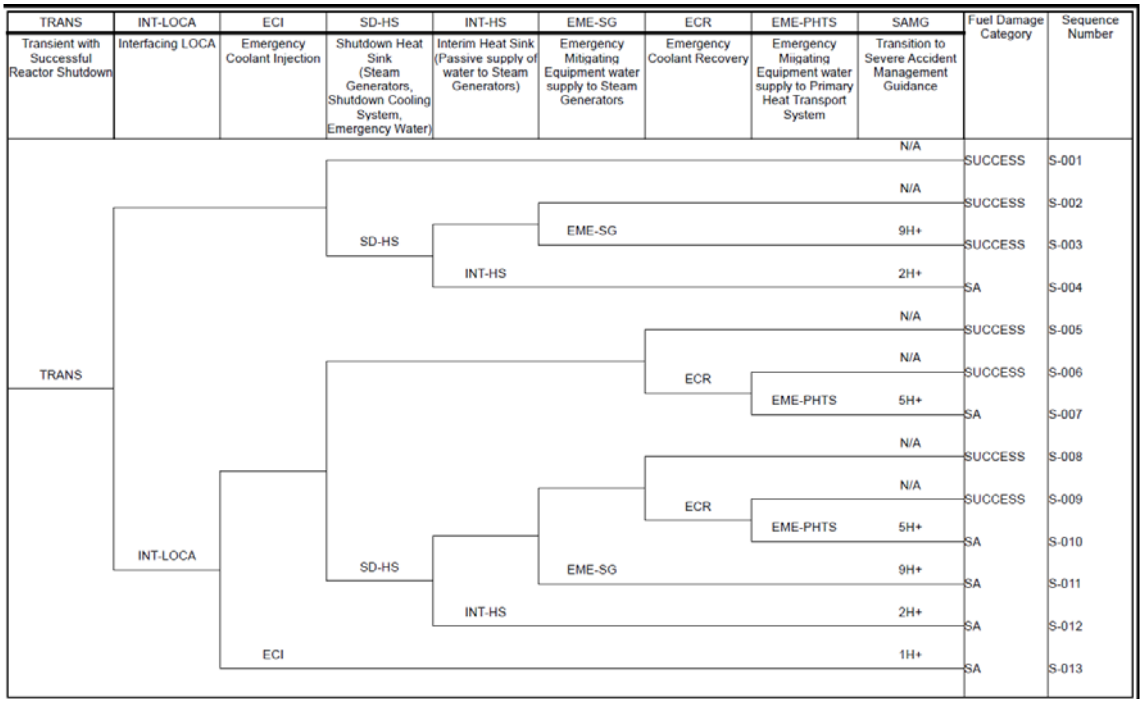

TRANS
Transient with Successful Reactor Shutdown
INT-LOCA
Interfacing LOCA
ECI
Emergency Coolant Injection
SD-HS
Shutdown Heat Sink (Steam Generators, Shutdown Cooling System, Emergency Water)
INT-HS
Interim Heat Sink (Passive supply of water to Steam Generators)
EME-SG
Emergency Mitigating Equipment water supply to Steam Generators
ECR
Emergency Coolant Recovery
EME-PHTS
Emergency Mitigating Equipment water supply to Primary Heat Transport System
SAMG
Transition to Severe Accident Management Guidance
Fuel Damage Category
Sequence Number
N/A
SUCCESS
S-001
N/A
SUCCESS
S-002
EME-SG
9H+
SUCCESS
S-003
SD-HS
INT-HS
2H+
SA
S-004
N/A
SUCCESS
S-005
N/A
SUCCESS
S-006
TRANS
ECR
EME-PHTS
5H+
SA
S-007
N/A
SUCCESS
S-008
N/A
SUCCESS
S-009
ECR
EME-PHTS
5H+
SA
S-010
INT-LOCA
SD-HS
EME-SG
9H+
SA
S-011
INT-HS
2H+
SA
S-012
ECI
1H+
SA
S-013

Figure 4: Simplified Severe Accident Event Tree

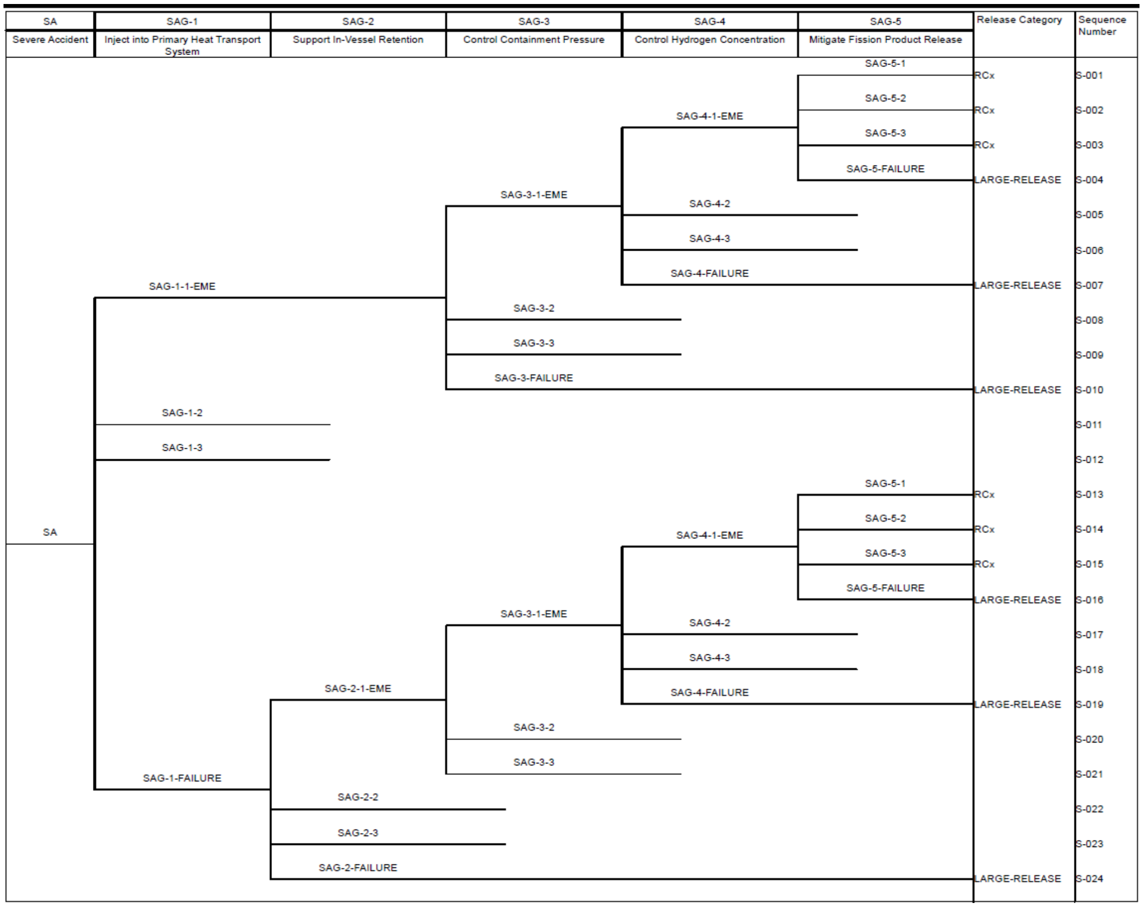


Figure 5: Potential Branching of SAMG Mitigating Strategies

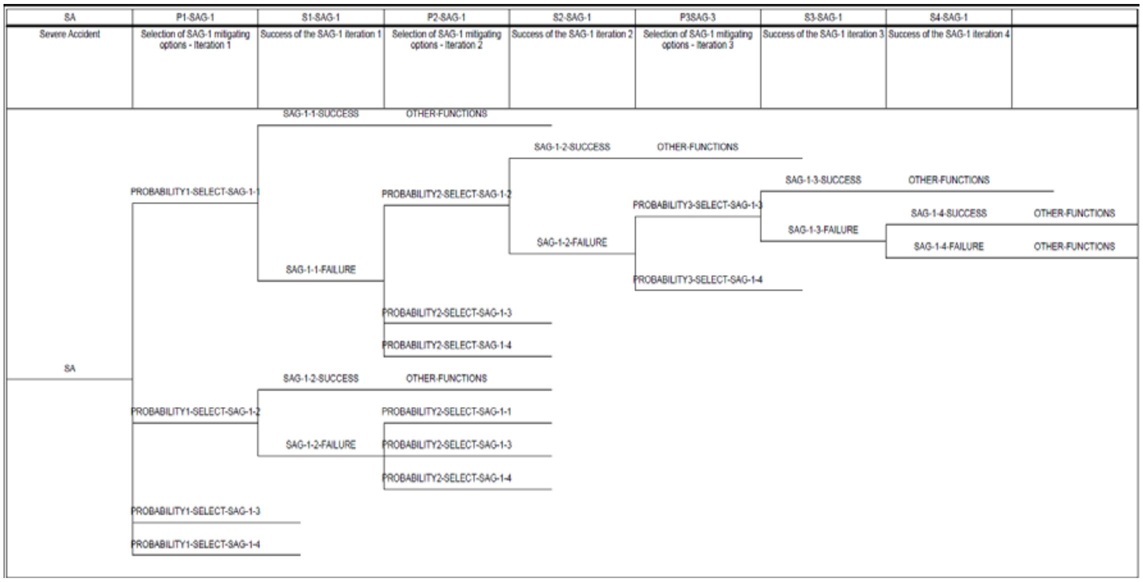

SA
P1-SAG-1
S1-SAG-1
P2-SAG-1
S2-SAG-1
P3SAG-3
S3-SAG-1
S4-SAG-1
Severe Accident
Selection of SAG-1 mitigating options - Iteration 1
Success of the SAG-1 iteration 1
Selection of SAG-1 mitigating options - Iteration 2
Success of the SAG-1 iteration 2
Selection of SAG-1 mitigating options - Iteration 3
Success of the SAG-1 iteration 3
Success of the SAG-1 iteration 4
SAG-1-1-SUCCESS
OTHER-FUNCTIONS
SAG-1-2-SUCCESS
OTHER-FUNCTIONS
SAG-1-3-SUCCESS
OTHER-FUNCTIONS
PROBABILITY1-SELECT-SAG-1-1
PROBABILITY2-SELECT-SAG-1-2
PROBABILITY3-SELECT-SAG-1-3
SAG-1-4-SUCCESS
OTHER-FUNCTIONS
SAG-1-3-FAILURE
SAG-1-2-FAILURE
SAG-1-4-FAILURE
OTHER-FUNCTIONS
SAG-1-1-FAILURE
PROBABILITY3-SELECT-SAG-1-4
PROBABILITY2-SELECT-SAG-1-3
PROBABILITY2-SELECT-SAG-1-4
SA
SAG-1-2-SUCCESS
OTHER-FUNCTIONS
PROBABILITY1-SELECT-SAG-1-2
PROBABILITY2-SELECT-SAG-1-1
SAG-1-2-FAILURE
PROBABILITY2-SELECT-SAG-1-3
PROBABILITY2-SELECT-SAG-1-4
PROBABILITY1-SELECT-SAG-1-3
PROBABILITY1-SELECT-SAG-1-4

Figure 6 shows the dynamic time-dependent transitions between different plant states determined by success and failure of key mitigating systems. As it can be seen, the timing of transitioning to SAMG, time available for mitigating actions, possibilities of recovery, and further potential transitioning to failure of Calandria vessel and initiation of CCI significantly depends on response of various plant systems and types of their failure (failure to start or mission failure).

In case of a LOCA, the transition to SAMG may be as early as in the first hour after the accident initiation if Emergency Coolant Injection (ECI) fails, especially for relatively large LOCAs. At this time, the decay heat levels are high and the primary heat transport coolant will be quickly depleted through the break. The transition to Moderator boil-off heat sink will occur early and the boil-off rate will be high, significantly reducing the time provided by this interim heat sink. This imposes significant limitations on availability of mitigating systems and time for operator response. However if ECI is successful to inject the initial inventory from ECI storage tanks, the timing of the accident progression may be significantly extended, especially for relatively small LOCAs. Furthermore, if the ECI recovery is initially successful and only fails during mission, the fuel decay heat may already be low, the interim heat sinks, such as Moderator boil-off and Shield Tank inventory boil-off, will provide significant time for implementation of alternate mitigating capabilities or equipment recovery.

In case if there is no LOCA, the shortest time for transitioning to SAMG is when the shutdown heat sinks (e.g., feedwater supply to Steam Generators, Shutdown Cooling System, Emergency Water supply to Steam Generators, etc.) have failed and the interim heat sink via passive make-up to Steam Generators from SGECS and Deaerator Storage Tank has failed. This transition will occur between two and three hours into the accident. If the interim heat sinks through Steam Generators are available, the transition to SAMG will occur after ten hours and much later if, in addition, the shutdown heat sinks were initiated successfully, but have failed during mission.

The complex accident progression described above may be modelled in dynamic event trees by coupling the probabilistic model with deterministic thermal-hydraulic models, for example by using the Monte Carlo Dynamic Event Tree (MCDET) method described in [3]. Modular Accident Analysis Program (MAAP) is typically used in Canada for severe accident analysis of CANDU reactors. However, the processing time for calculating all time histories in a dynamic event tree may be excessive. Therefore, the following simplifications of analyses to reduce quantification time are recommended:

1. Use simple models for processes that are well understood.

   Using of simplified models for simulating the time history of the key plant variables in specific states will significantly reduce the quantification time compared to the use of complex thermal-hydraulic models. For example, the decay heat that needs to be removed from the reactor can be quite precisely characterized by decay heat curves. Such curves are measured, recorded and mathematically described for all power plants. If the plant is in an interim quasi-steady-state where the decay heat is removed from the core by boil-off of the Steam Generator inventory, Moderator inventory, or Shield Tank inventory, the duration of staying in this interim state and the inventory of the credited heat sink at each time can be calculated using the initial inventory of the coolant, the time of the transition to that state, the decay heat curve, and the latent heat of water vaporization. Some NPPs developed curves representing the boil-off rate as a function of time (see example in Figure 7).

2. Use pre-calculated dependencies of key variables for a range of conditions.

   For a number of interim plant states, it is possible to pre-run deterministic codes to quantify time of transition from one state to another as a function of specific plant variables. For example, the duration of the initial injection from ECI storage tanks to the primary heat transport system can be simply characterized by pre-calculated curves relating the injection time to the LOCA size (see example in Figure 8).

3. Use probabilistic truncation limits.

   The dynamic accident sequences reaching truncation limit should be screened out. This is especially important for SAMG actions where use of multiple mitigating options and restauration of equipment are credited, which may result in unmanageable branching of event trees, provided there is sufficient time for trying multiple options. However, the quantification process should take into account human error dependencies between various SAMG mitigating options in the same accident sequence. The human error dependency assessment results in increase of the joint human error probability in a sequence and should be applied before truncation of accident sequences.

The simplifications described above are not expected to introduce significant additional uncertainties in the calculation or reduce accuracy of the results, while should significantly reduce the quantification time. The simplified models of the key thermal-hydraulic processes in the interim quasi-steady-states of the plant between transitions are essentially the same as the ones used in the complex deterministic codes, but are executed much faster, because non-essential physical models that are not impacting the timing of the accident progression are not quantified. The pre-calculated dependencies of key variables are produced by the same deterministic codes that would be coupled with the dynamic event tree, and can be used as equations or look-up tables for a range of conditions instead of the actual execution of deterministic codes.

Figure 6: Dynamic Representation of Accident Progression

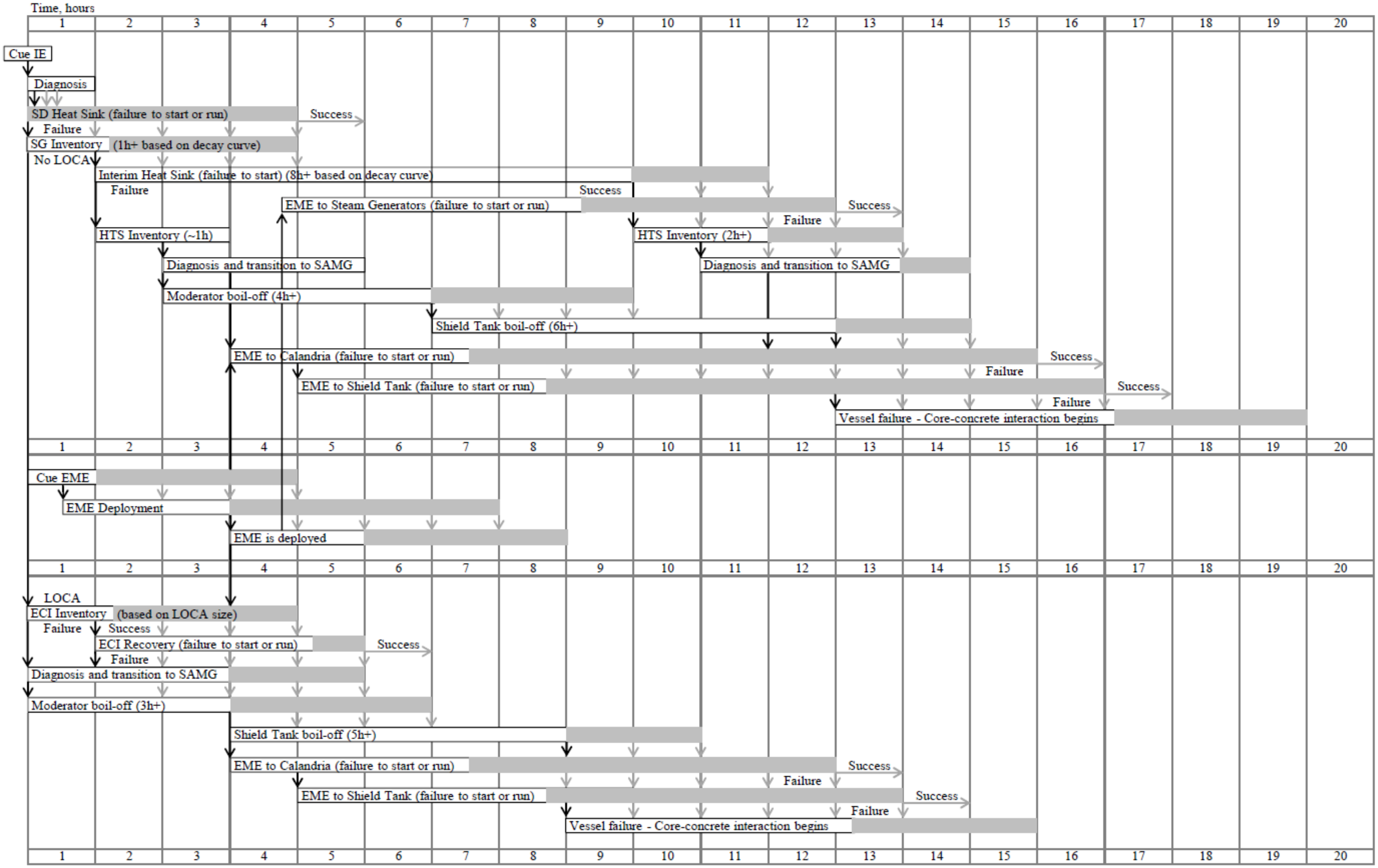

Time, hours
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
Cue IE
Diagnosis
SD Heat Sink (failure to start or run)
Success
Failure
SG Inventory
(1h+ based on decay curve)
No LOCA
Interim Heat Sink (failure to start) (8h+ based on decay curve)
Failure
Success
EME to Steam Generators (failure to start or run)
Success
Failure
HTS Inventory (~1h)
HTS Inventory (2h+)
Diagnosis and transition to SAMG
Diagnosis and transition to SAMG
Moderator boil-off (4h+)
Shield Tank boil-off (6h+)
EME to Calandria (failure to start or run)
Success
Failure
EME to Shield Tank (failure to start or run)
Success
Failure
Vessel failure - Core-concrete interaction begins
Cue EME
EME Deployment
EME is deployed
LOCA
ECI Inventory
(based on LOCA size)
Failure
Success
ECI Recovery (failure to start or run)
Success
Failure
Diagnosis and transition to SAMG
Moderator boil-off (3h+)
Shield Tank boil-off (5h+)
EME to Calandria (failure to start or run)
Success
Failure
EME to Shield Tank (failure to start or run)
Success
Failure
Vessel failure - Core-concrete interaction begins

Figure 7: Water Boil-Off Rate as a Function of Time after Shutdown

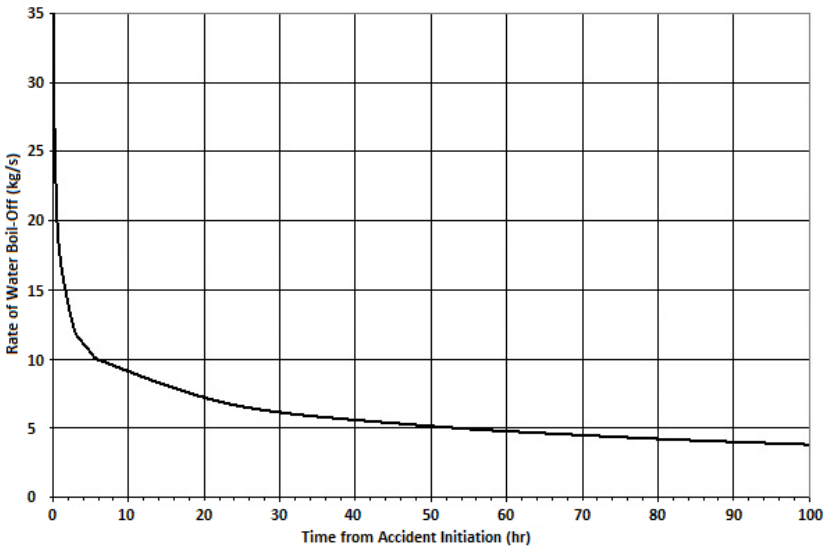
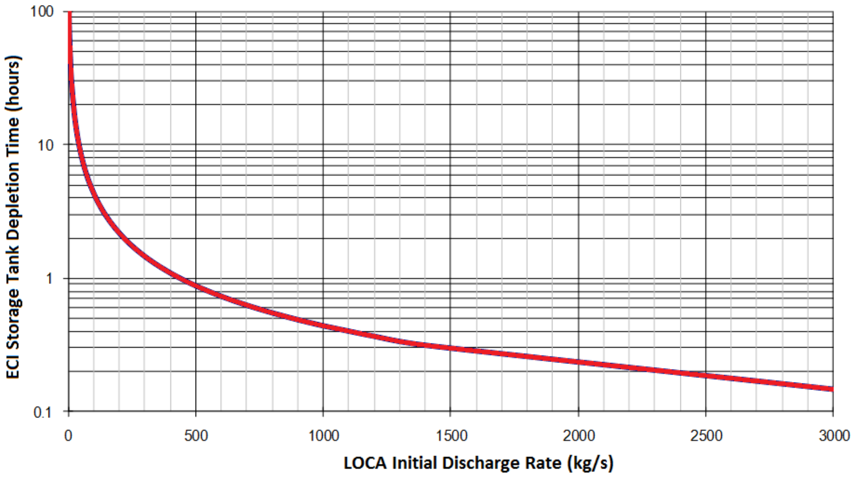


Figure 8: ECI Storage Tank Depletion Rate as a Function of LOCA Size



4. CONCLUSION

This paper primarily focused on modelling of the complex plant response in mitigation of severe accidents governed by SAMG. Specifics of the SAMG response are that SAMG involves multiple choices of mitigating strategies, novel use of equipment, use of EME with long deployment time but flexibility of use, and recovery of failed equipment. The time available for testing several mitigating strategies until an effective strategy is found and implemented depends on the time history of the accident. Therefore, the time history of the accident progression should be tracked in each accident sequence. At the same time, the branching of the event tree may be very extensive and is difficult to develop manually in static event trees.

The dynamic event tree modelling adds the time element to representation of accident progression in PSA. This allows to adequately characterizing the impact of the accident progression on the response of mitigating systems, their effectiveness at different points of time, and the probabilities of operator crew failure to mitigate the accident. The dynamic modelling methods overcome the deficiency of the static event tree modelling, which represents the accident progression by a limited number of bounding accident sequences typically leading to overestimate of the result and loss of insights on conditional probability distributions in the time domain. Thus, dynamic event tree approach is promising for modelling of severe accident management governed by SAMG. For CANDU NPPs, the probabilistic model may be coupled with the severe accident analysis code MAAP typically used in Level 2 PSA.

However, the dynamic event tree approach requires extensive computational time. The complex SAMG response may not be quantified in a meaningful timeframe. Therefore, the paper proposed some simplifications, such as the use of simple models and pre-calculated time dependencies of key variables instead of the complex thermal-hydraulic codes. These simplifications can be effectively used for a number of quasi-steady-state interim plant conditions. The complex codes would be used only in specific points of the time where transitions between states are expected and at the end of accident sequences to determine success or failure of mitigating strategies. This approach is expected to significantly reduce the computation time without losing insights and introducing additional uncertainties in the calculations.

References

[1] C. G. Acosta and N. O. Siu, "*Dynamic Event Tree Analysis Method (DETAM) for Accident Sequence Analysis*", Massachusetts Institute of Technology Nuclear Engineering Department, MITNE-285, October 1991.

[2] N. Siu, "*Risk Assessment for Dynamic Systems: An Overview*", Reliability Engineering and System Safety, 43, pp.43-73, (1994).

[3] M. Kloos at. al., "*MCDET: A probabilistic dynamic method combining Monte Carlo simulation with the discrete dynamic event tree approach*", Nuclear Science and Eng., 153, pp.137-156, (2006).

[4] A. Afonsi at. al., "*Dynamic Event Tree Analysis Through RAVEN*", International Topical Meeting on Probabilistic Safety Assessment and Analysis 2013, PSA 2013.

[5] T. Aldemir, "Advanced Concepts in Nuclear Energy Risk Assessment and Management", 2018.