SAND2017-10141C

A DYNAMIC ASSESSMENT OF AN INTERFACING SYSTEM LOSS OF COOLANT ACCIDENT

Zachary K. Jankovsky*†, Matthew R. Denman*, Tunc Aldemir†

*Sandia National Laboratories, Albuquerque, New Mexico, Zachary.Jankovsky@sandia.gov
†The Ohio State University, Columbus, Ohio

Accident scenarios in nuclear power plants that bypass containment have the potential for large and early releases of radionuclides. They are typically guarded against using means such as redundant valves arranged in series and interlocks for systems that interface with the high pressure reactor coolant system. Some of these preventative arrangements rely on active systems that may fail in unique ways with the introduction of digital instrumentation and control. A hypothetical scenario in a pressurized water reactor plant is examined in which the digital controllers for the residual heat removal system intake valves are subjected to a common cause failure. This failure may cause simultaneous unintended valve opening while the reactor is at power which has the potential to overpressurize and damage piping in the residual heat removal system and cause a leak of primary system water past containment into the auxiliary building (interfacing system loss of coolant accident). If the controllers are in a persistent fault condition, plant personnel will have to traverse the potentially contaminated auxiliary building to override at least one controller and close its associated valve. A dynamic case is assembled and run using the ADAPT dynamic event tree driver and the MELCOR severe accident analysis code in which uncertainties in the progression of the accident as well as mitigating operator actions are explored for an interfacing systems loss of coolant accident initiator. The results are assessed using recently-developed tools to gain insight into the likely outcomes and key events.

I. INTRODUCTION

Probabilistic Safety Analysis (PSA), or Probabilistic Risk Assessment (PRA) of Nuclear Power Plants (NPPs) yields insights about possible outcomes stemming from an initiating event. These outcomes are compared based on their likelihood and impact for use in licensing and decision-making in repair and maintenance. Sequences which may lead to an early release of radionuclides from the plant may increase the risk to the public when compared to later releases of similar composition[1]. One general initiating event that may lead to early release in a Light Water Reactor (LWR) is the Interfacing System Loss of Coolant Accident (ISLOCA) in which inventory from the Reactor Coolant System (RCS) leaks into a lower-pressure system. The lower-pressure systems, often Residual Heat Removal (RHR) or Low Pressure Safety Injection (LPSI), have components outside of containment in some existing plants[2]. In some cases, particularly in Pressurized Water Reactors (PWRs), there is a chance that overpressurization will cause damage in the lower-pressure system leading to a leak of water and radionuclides from the RCS[3].

Because of the potential consequences, systems that may be subject to an ISLOCA have been designed to withstand single component failures lowering the likelihood of an ISLOCA. This has led to ISLOCAs, despite the potentially high consequences, being screened out of some safety analyses because the assessed risk is significantly lower than other more likely accident types[4].

The adoption of Digital Instrumentation & Control (DI&C) in existing plants[5;6] is expected to reduce cost and improve overall reliability but will also introduce failure modes that did not exist in the original analog systems. This work examines a cyber-induced failure of the digital controllers of the Motor-Operated Valves (MOVs) that isolate the intake of the RHR system from the primary system at a hypothetical PWR. Most ISLOCA pathways, and particularly those commonly considered in large-scale analyses, involve discharge lines that may be protected to a high level of reliability using multiple check valves in series[1;4]. The check valves are passive, operating without power or control signals from the plant. However, an ISLOCA at the RHR intake would be in the usual direction of flow and so check valves would not protect it. The intake must be isolated during some operating modes and must be open for others which is accomplished using actively-controlled systems. This work considers the effects of a postulated cyber exploit of the control network at a hypothetical plant that has upgraded shutdown system MOVs to DI&C[7].

This work explores the impact of uncertainties leading from the initiating event of the two RHR MOVs being persistently held open by controller failures on the likely consequences of the event. Physical parameters such as piping pressure capacity are considered as well as recovery actions taken by plant personnel whose timing will depend on the state of the auxiliary building when the actions are taken. These types of uncertainties are generally difficult to handle in a traditional PSA framework and usually require the use of dynamic PSA methods[8]. New data analysis features (dynamic importance measures) of the Analysis of Dynamic Accident Progression Trees (ADAPT) Dynamic Event Tree (DET) driver code are used to study the uncertainties relevant to ISLOCA using the MELCOR code. MELCOR is an LWR severe accident analysis code with the ability to represent diverse phenomena such as thermal-hydraulics, core degradation, radionuclide transport, core-concrete interaction, and hydrogen generation and combustion[9].

The DET generation process is presented in Figure 1 and is driven by the condition of the plant as reflected by a simulator code. When compared to traditional event trees the significant differences are the automated generation of the tree, the addition of a time axis, and the use of non-binary branching. A database stores the parent-child relationships of all branches which may be used to assemble outputs from

the initiating event (P_1) to any end state (e.g., P_{11112}) as a unique sequence. In a similar manner to a traditional event tree, the final output of a DET includes a set of plant states at the end of the accident each with a probability conditional on the initiating event. However, a richer set of data is returned that also includes the time that each branching condition was met as well as time series of chosen physical parameters.

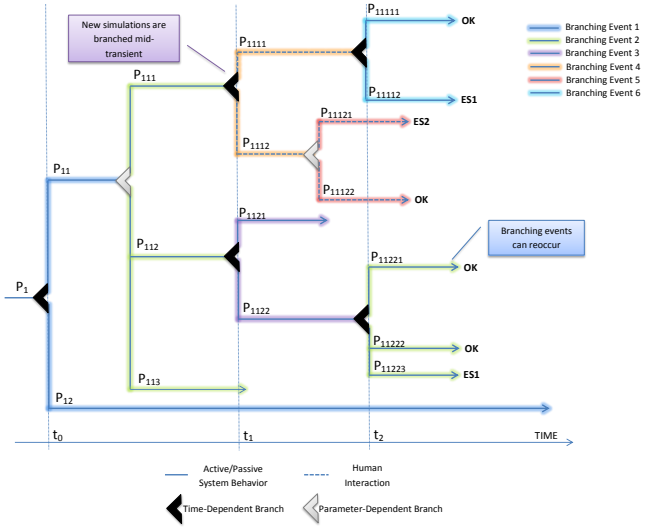

Fig. 1. General DET Behavior[10]

In this study, the results produced by the DET are examined for the impact of chosen uncertain parameters (e.g., timing of RHR pipe break isolation) on measures of consequence (e.g., hydrogen production) using the Dynamic Importance (DYI) measure calculation platform of ADAPT[1][11].

Section II describes the accident being studied as well as its expected effects on the plant. Section III presents the uncertainties that will be addressed in the dynamic simulation. The results of the case are given and interrogated for insights in Section IV. Finally, the work and its impact are briefly summarized in Section V.

II. PLANT SYSTEM AND NOMINAL ACCIDENT PROGRESSION

This section describes the plant system being studied (II.A.), the expected accident progression (II.B.), and the expected consequences (II.C.).

II.A. Plant Configuration

This work considers a hypothetical three loop PWR that utilizes a combined LPSI and RHR system[2] outside of containment which exists in several operating plants[2]. The LPSI and RHR systems are typically designed to operate at similar pressures and to discharge to similar locations and so it can be economical to combine them to reduce the number of pumps and the amount of piping in the plant. The maximum operating pressure for the RHR system in this case is assumed to be $2MPa$ and it can accommodate a flow rate of $3750gpm$.

The High Pressure Safety Injection (HPSI) system provides a flow of $375gpm$ and operates up to $12MPa$ which is below the RCS operating pressure of $15.5MPa$ but high enough that exposure to full RCS pressure is not expected to damage the system. Along with HPSI and LPSI, the Emergency Core Cooling System (ECCS) includes accumulators which store pressurized highly borated water and passively inject if the RCS pressure drops below $4.6MPa$. A diagram of the ECCS is shown in Figure 2 for reference. HPSI and LPSI both draw from the Refueling Water Storage Tank (RWST) when operating in injection mode. Water from the containment sump may be recirculated for LPSI if sufficient water has accumulated in the sump and Net Positive Suction Head (NPSH) requirements are met[12].

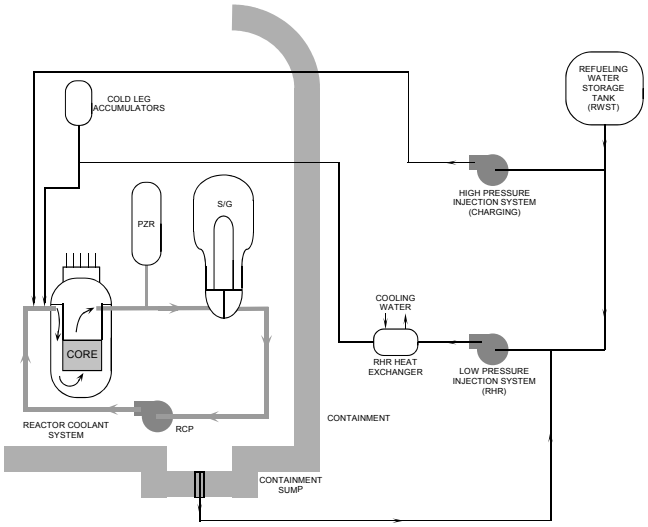

Fig. 2. Overview of the Emergency Core Cooling Systems[13]

The RHR system shown in Figure 3 is operational during reactor shutdown periods when the RCS is at a reduced pressure. The RHR system takes in water from the RCS hot leg which is isolated during operation by two MOVs on independent control systems. These MOVs are located inside the containment building to reduce the risk of a valve leak of outside of containment[3]. Water exits the containment structure to the RHR pumps and through the RHR Heat Exchanger (HX) tubes before being returned to the RCS cold leg[14]. The water is cooled by Component Cooling Water (CCW) on the shell side of the heat exchangers. CCW also provides cooling to the HPSI and RHR pumps. Not shown are RHR relief valves throughout the system which provide a small level of protection against overpressurization. These valves are not large enough to protect the RHR system against full RCS pressure[3] but may contribute to inventory loss in an ISLOCA.

[1] To avoid confusion, the measures referred to as DIM in Reference[11] are renamed to DYI in this and subsequent works

[2] When discussing the shared system of pumps and pipes this is referred to as RHR. Specific discussion of the injection function uses the term LPSI.

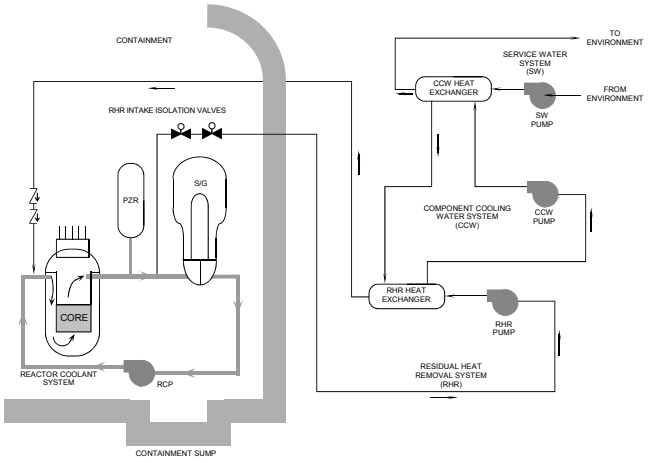

Fig. 3. Overview of the Residual Heat Removal System[13]

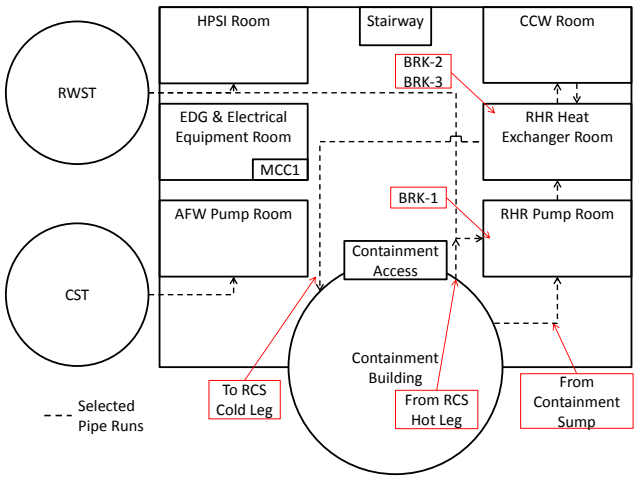

Fig. 4. Auxiliary Building Lower Level Layout

II.B. Accident Sequence and Nominal Response

A MELCOR model of the hypothetical plant was created for this and related analyses which includes relevant systems and pathways[15]. At time *t=0* both RHR isolation MOVs are assumed to be opened and held open by their compromised controllers while the reactor is operating at full power with possible damage to both the RHR piping and the RHR heat exchangers[3]. Shortly after any break the reactor will scram on low pressure followed by the main feedwater system tripping and engaging auxiliary feedwater. As the pressure decreases HPSI will engage if available. If the pressure continues to fall the accumulators will inject their inventory. LPSI will not be immediately available in the case of any RHR damage but may be recovered by isolating the damaged component(s).

If any RHR heat exchanger failure occurs, the CCW system will be subject to either high pressure or a leak and is assumed to be out of service until isolated from the RHR heat exchangers. It is further assumed that the systems that depend on CCW, including HPSI, will also be out of service until CCW isolation is achieved. The impact of overpressurization of the CCW system depends on the configuration. Some common configurations may be seen in[16].

In this study, it is assumed that if a pipe break occurs it will occur near the RHR pump intake and will cause a leak into the RHR pump room of the auxiliary building (see *BRK-1* in Figure 4). Water from the RCS as well as the RWST will flow into the RHR pump room until each source is isolated. The RWST may be isolated from the shared RHR system by closing its MOVs from the control room. If a heat exchanger tube break occurs (*BRK-2* in Figure 4), the CCW system will be overpressurized. If the heat exchanger shell also fails (*BRK-3* in Figure 4), RCS water and CCW will spill into the RHR heat exchanger room. This will continue until the CCW is isolated from the RHR heat exchanger and the RCS is isolated from RHR.

The Motor Control Center (MCC) for one RHR isolation valve is assumed to be on the same level of the auxiliary building as the control room and the MCC for the other valve is on lowest level (see *MCC1* in Figure 4). The MCC houses the power supply and controller for the motors that drive the MOVs. As the controllers will be in a persistent failed state, plant personnel will have to reach an MCC, override the controller, and manually send a signal to the valve motor to close the valve. Due to electrical safety hazards associated with MCCs, personnel will be required to don arc flash protection equipment delaying completion of the task[17]. There is a chance of an internal failure to close the MOV. In this case, the operators will have to attempt the procedure at the other MCC. Because the MOVs are in series, closing either one is assumed to be sufficient to isolate the RCS from RHR.

For the State-of-the-Art Reactor Consequence Analyses (SOARCA) study, operators at the Surry plant were subjected to a simulated ISLOCA and their performance of the emergency procedure was timed[4]. RWST isolation was accomplished 16 minutes after initiation of the accident which is used as the timing of RWST isolation in this case. The SOARCA ISLOCA analysis also examined the effects of the operators opening the Pilot-Operated Relief Valves (PORVs) after an ISLOCA is identified. This opens a path for high pressure RCS inventory to move into the containment structure reducing the total flow from the break outside of containment. In addition to potentially reducing the flow of radionuclides out of containment this retains some inventory in the containment sump where it may be used for recirculation (see Section II.A.).

The state of doors in the RHR pump room and RHR heat exchanger room can influence the ability of operators to perform isolation actions. Doors to high energy line break areas, which are considered to be at high risk for internal flooding, have been left open inappropriately in some recent cases[18;19]. Even with the door closed, there is a chance that seals have degraded similar to the case at an operating plant that identified "degraded flood penetration seals, conduit seals, and a 7.6*cm* (3 inch) gap in the weather stripping along the bottom of the Unit 2 reactor building railroad door"[20]. Finally, a closed door may burst if incoming water overcomes the room drains and the water level rises past the door's capacity[21]. Operators are assumed to be unable to safely complete tasks in a room while the water level is over 1 inch and so a flood that

propagates through the auxiliary building may delay multiple recovery actions.

II.C. Potential Consequences

This event challenges the integrity of the fuel as multiple failure modes of the RHR system allow RCS water to escape while disabling portions of the ECCS as well as shutdown cooling. The radioactivity of RCS water before fuel damage is not significant to offsite consequences but may delay plant personnel in performing recovery actions as they will be required to don radiation protection equipment[22]. If fuel damage occurs and the RHR isolation valves are still open, there is likely to be significant contamination of the auxiliary building which may prevent operators from performing further actions outside of the control room. Additionally, hydrogen may be transported to the auxiliary building and may reach appropriate conditions for combustion. This may cause the auxiliary building doors or roof to fail due to overpressurization opening a release path of radionuclides to the environment[4].

III. DYNAMIC CASE

This section first briefly describes the operation of the ADAPT DET driver code and its requirements (III.A.). The particular dynamic case developed for this work is presented in terms of the uncertainties that are addressed in accident initiation and operator response (III.B.).

III.A. ADAPT Operation

The uncertainties in this case include values of physical parameters (e.g., pressure capacities) as well as timing of actions in response to the initiating event which are difficult to address using traditional PRA. A simulator-driven DET is a form of dynamic PRA that can accommodate such uncertainties[8]. The basic progression is shown in Figure 1. An initial simulation is run until a point of interest is met either according to time (e.g., initiating event at time zero) or the value of a physical parameter (e.g., HPSI demanded due to low primary pressure). Uncertain parameters are sampled from their Cumulative Distribution Functions (CDFs). The granularity of the sampling is a compromise between coverage of the uncertainty space and available computational resources. Sampled values of an uncertain parameter are applied for each branch and the simulator is run to determine the effect of the branching values. The probability of each branch conditional on the initiating event is tracked in the ADAPT database. The following entries are stored in the ADAPT database for each branch:

- Branch number
- Parent branch number
- Branching condition of parent
- Simulator input file location
- ADAPT variable values
- Total branch probability
- Simulator to run

ADAPT is a DET generation and analysis code that has historically been used with a single simulator code for a given application that is broad enough to represent the entire scope of phenomena of interest. ADAPT was initially linked to MELCOR[23] and has since been used with RELAP5[24], SAS4A[25], and MAAP4[26]. A recent example of the use of ADAPT with multiple simulators utilized independent MELCOR models to represent the primary system and the auxiliary building during an ISLOCA to demonstrate the passing of information and control between codes[27].

The process followed for each branch in ADAPT is diagrammed in Figure 5. The simulator is run (*Execute Simulator*) with appropriate input until it stops at which point ADAPT ascertains the *Reason for Stopping*. The DET is considered finished when all sequences have ended with a branch with *Maximum Simulation Time Reached* or an abnormal *Simulator Failure*. In all cases, branches ending will *Update Database*. If a branching condition is reached, ADAPT will *Apply Branching Rules* to produce database entries and input files for the new branches which are added to the queue to be run when resources are available.

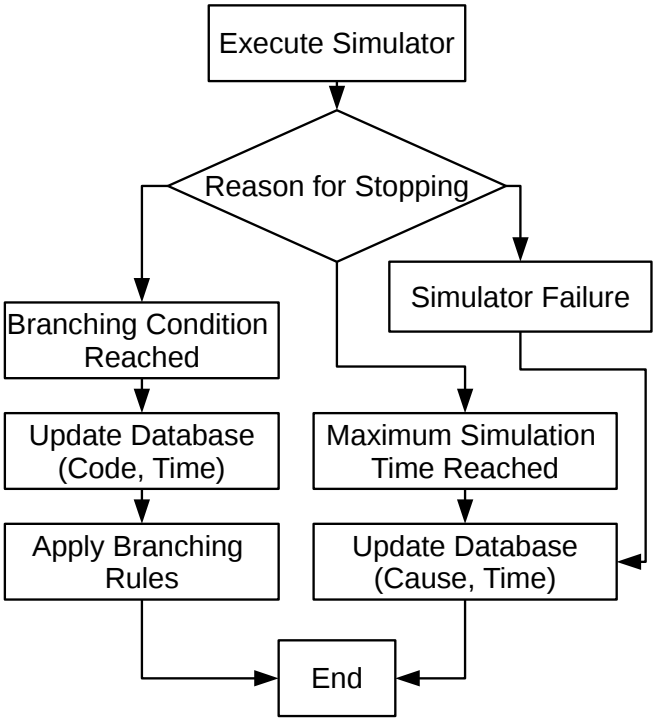

Fig. 5. ADAPT Branch Operations

A template simulator input file is provided by the user with uncertain parameters indicated with ADAPT variables. These variables are replaced with branched values according to the branching rules for each branching condition. The physical state of the plant as reflected by the simulator "restart" file and updated during the course of each branch is the starting point of each child branch.

III.B. MELCOR Uncertainty Treatment

III.B.1. ISLOCA Initiation

The capacities of the RHR piping and heat exchangers determine whether the initiating event will cause an ISLOCA. The RHR intake pipe is assumed to be 12 inches diameter thin-walled stainless steel[14]. The RHR heat exchanger tubes and shells are also constructed of stainless steel with capacities defined in[28]. The lognormal distribution parameters for these capacities are given in Table I. The pressure capacity CDFs as well as sampled values (25th and 50th percentile used in DET for illustration purposes) are shown in Figure 6. The capacities are branched independently after both RHR isolation valves have opened.

TABLE I. RHR Component Pressure Capacity

Component	Median (psig)	Log. Std. Dev.
Intake Pipe[14]	1284	0.36
Heat Exchanger Tube[28]	1650	0.23
Heat Exchanger Shell[28]	1370	0.27

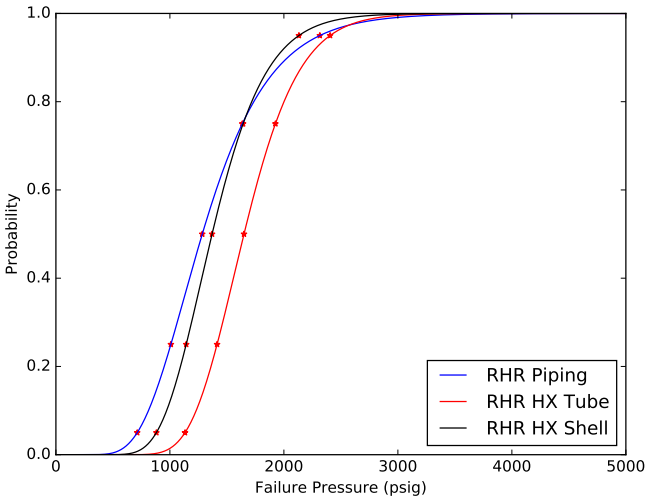

Fig. 6. CDF for RHR Component Pressure Capacities

III.B.2. Operator Response

Per the timing from the ISLOCA simulation performed for SOARCA, no operator actions are credited until 6 minutes after accident initiation[4]. This allows time for an ISLOCA outside of containment to be diagnosed and the appropriate emergency procedure to be identified. In some manual scenarios run for this study, it was found that 6 minutes after accident initiation the RCS pressure may be below the accumulator injection point. A decision must be made by operators to allow the pressure to rise once isolation has been regained or to keep the pressure low. At 6 minutes after initiation the DET is programmed to branch on the decision to either open and lock the PORVs or take no action. Opening the PORVs is a method that may be used in an ISLOCA to reduce the volume of water lost from the RCS as well as the release of radionuclides through the ISLOCA pathway[4]. The mitigating action of opening the PORVs is subject to internal PORV failure according to the probability of failure per demand values listed in Table II.

TABLE II. Plant System Reliability

Event	Probability of failure per demand
PORV fail to open[29]	$7.0 * 10^{-3}$
PORV fail to close[29]	$1.0 * 10^{-3}$
MOV fail to open or close[29]	$1.0 * 10^{-3}$

After a break in the RHR system, the RWST will be leaking into the auxiliary building contributing to flooding and reducing inventory available for injection. At 16 minutes after ISLOCA initiation the DET branches on the success of the operator attempt to isolate the RWST from the RHR system using the timing from[4]. This action is taken from the control room and may fail due to internal MOV failure to close (see Table II).

Operator actions that must be taken outside of the control room are assumed to require time according to a distribution from[30] which was originally assigned to manual isolation of an Auxiliary Feedwater (AFW) train and is shown in Figure 7. Similarly to[30], additional minimum time was added to the base Weibull distribution seen in Figure 7 to account for unavoidable delays. In this case delays include donning protective equipment and moving through the auxiliary building. The stars in Figure 7 denote initially sampled values of each CDF. Only the 50th and 75th percentiles are used in DET generation. Delays are sampled from the CDF in Figure 7 for the following actions:

- Isolation of RHR pump suction from RCS
- Isolation of RHR heat exchanger from RHR
- Isolation of RHR heat exchanger from CCW

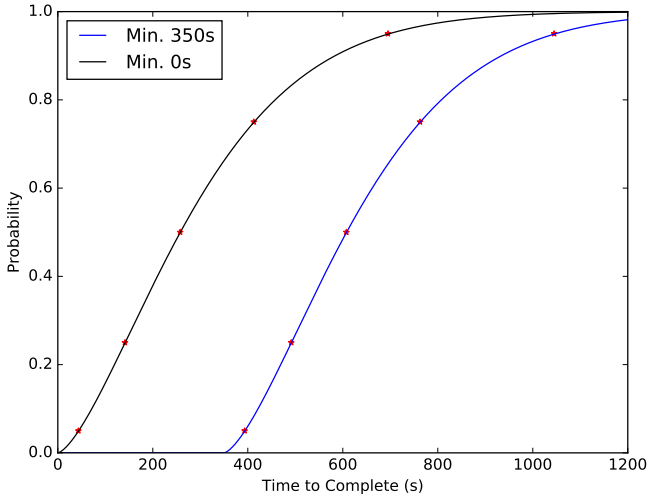

Fig. 7. CDF for Operator Action Timing[30]

III.C. Flooding

At the time of any break in the RHR system, a branching condition is used to determine the state of auxiliary building doors. This affects the extent to which rooms will flood as well as the general transport of radionuclides around the auxiliary building. First, branching determines whether the doors to the RHR pump room and RHR HX room are opened or closed with a 0.9 probability of each being closed and 0.1 probability of each being open. Next, if a door is closed branching is performed to determine the capacity of the door for the RHR pump room and the RHR HX room. Each door may fail at a room water level of either $4ft$ or $6ft$ with equal (0.5) probability[21]. Each room in the auxiliary building is assumed to have two 3 inch drains leading to a semi-infinite sink, while the main hall of the lower level (see Figure 4) has ten 3 inch drains.

IV. RESULTS AND DISCUSSION

The DET resulted in 31,000 total branches, which represent 26,000 unique sequences from the initiating event to end states. The computing cluster used consisted of three dual processor nodes running Red Hat Enterprise Linux 7. The case required 450 processor-days (or 4 calendar days using the 150 available processors). The conditional core damage probability was found to be $2.9 * 10^{-6}$. The resulting data set was 1.5 terabytes and the volume of output data has historically presented a challenge for extracting meaningful insights from DETs. DYIs measures are used to examine the impact of uncertain parameters on consequences of interest as introduced in[11].

The primary pressure of all sequences are plotted in Figure 8. Sequences where at most one RHR isolation valve opens terminate early and do not appear in the plot. With the series arrangement of RHR isolation valves, failing a single valve will not cause an ISLOCA outside containment. It is important to note that pipe and tube failures in this model account only for over-pressurization and not dynamic loading which may also contribute to failures in the RHR system (see Section II.A.).

At around $40s$, sequences diverge based on whether the RHR intake pipe failed, the RHR HX shell failed, or both. Between approximately $300s$ and $800s$ branching occurs on whether the operators open the PORVs and whether the RCS is isolated from the RHR system both of which influence the primary pressure.

The reactor vessel water level is shown in Figure 9 with the top of active fuel marked at 6.7m. The RHR ISLOCA results in a fast decrease in the level which may be slowly reversed if the leak is isolated and HPSI is available. The HPSI pump shutoff pressure does not exceed the PORV closing setpoints and so if pressure rises to a level that cycles the PORVs there is no automatic injection.

IV.A. Importance Assessments

Two key advantages of the simulator-based DET over traditional event trees are that non-binary parameter values

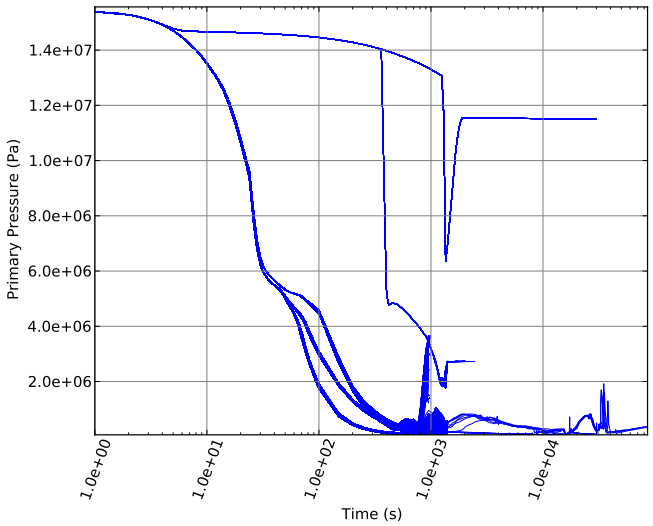

Fig. 8. Primary Pressure

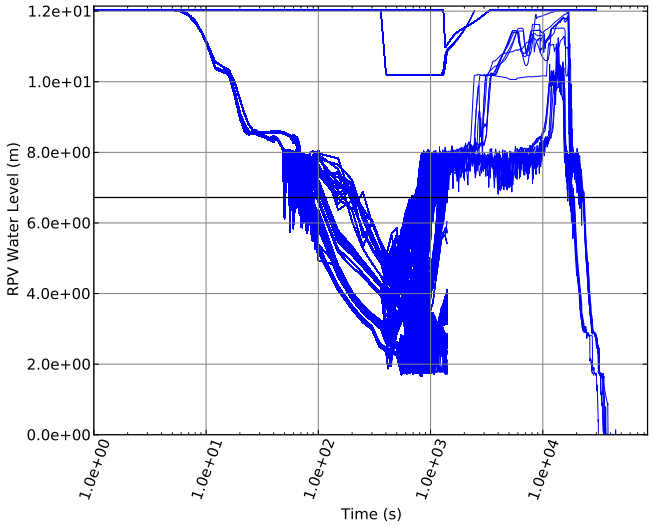

Fig. 9. Reactor Pressure Vessel Water Level

may be explored and a rich set of continuous output data is produced. This presents a challenge for traditional importance measures which were designed around binary branching conditions and outcomes. The recently-introduced DYIs[11] as seen in Table III may be used to search for relationships between the value of a chosen measure of consequence and the value of a branched parameter. In Table III, *R()* represents the expected value of a chosen consequence measure for a set of sequences, *x=1* refers to all sequences where event x occurs, *x=0* refers to sequences where x does not occur, and x_i indicates a value of occurrence i in the case of uncertain timing of an event or value of a physical parameter.

An example calculation of DYI1 is given in Equation 1 for the occurrence of an RHR intake pipe break. This event causes the RHR system to be permanently failed and LPSI to be unavailable until the break can be isolated. The consequence measure C is the level of hydrogen production.

TABLE III. Dynamic Importance Measures

Importance Measure	Comparison
$DYI1 = \frac{R(x=1)}{R(x=0)}$	Occurrence to non-occurrence
$DYI2(i) = \frac{R(x=1_i)}{R(x=0)}$	Occurrence i to non-occurrence
$DYI3(i) = \frac{R(x=1_i)}{R(x=1)}$	Occurrence i to all occurrence

The summations in the numerator of Equation 1 cover the set of $n_{x=1}$ sequences j where the failure occurs while the denominator summations cover the set of $n_{x=0}$ sequences k where the break does not occur. The weighted average of each set is found by dividing the product of the probability P and consequence C for each sequence by the sum of sequence probabilities in the set. The weighted average hydrogen production where the break occurs is $31.7kg$ while the expected value when the break does not occur is $1.69kg$. This renders a DYI1 value of 18.8 meaning that the expected hydrogen production when the break occurs is 18.8 times the expected production when the break does not occur. This and other DYI1 values appear in Table IV.

$$\begin{aligned} DYI1 &= \frac{R(x=1)}{R(x=0)} \\ &= \frac{\frac{\sum_{j=1}^{n_{x=1}} P_j * C_j}{\sum_{j=1}^{n_{x=1}} P_j} = 31.7}{\frac{\sum_{k=1}^{n_{x=0}} P_k * C_k}{\sum_{k=1}^{n_{x=0}} P_k} = 1.69} \\ &= 18.8 \end{aligned} \tag{1}$$

IV.A.1. Binary Events

DYI1 values are presented in Table IV for binary events and their relation to the extent of hydrogen production. This is used as a surrogate for core damage as hydrogen is produced in an accident when the fuel becomes uncovered and the zircaloy cladding reacts with steam. Note that the DYI values indicate the ratio of consequences when the event occurs vs does not occur regardless of whether the event is considered a "failure". Also note that a value of ∞ indicates that the hydrogen production was zero for all sequences where the event (e.g., *RHR HX Tube Break*) did not occur resulting in an infinite value of DYI1. Such a result is also possible with traditional Importance Measures (IMs)[31] and suggests that in this case avoiding the event may prevent fuel damage as in the case of RHR HX tube and shell failure. It can be seen that hydrogen production is 18.8 times greater in sequences where the RHR intake pipe fails than in sequences where this failure does not occur. Production is reduced when RHR HX shell isolation succeeds versus when it is failed (0.273 times the production when isolation succeeds versus fails) which was also expected.

IV.A.2. Physical Parameters

Uncertainty in the value of a physical parameter (e.g., RHR intake pipe pressure capacity) is difficult to capture in traditional fault tree / event tree PRA as it does not represent a binary event. Such parameters may be important to an analysis, however, and can be handled in a DET by branching on sampled values just before they are expected to have an impact on the analysis. For example, branching for the RHR intake pipe pressure capacity is triggered at the moment both RHR isolation valves have been opened. DYI3 values for relevant parameters are seen in Table V for their impact on production of hydrogen.

TABLE IV. DYI1 Values for Binary Events, H2 Production

Branching Condition	DYI1
RHR Pipe Break	18.8
RHR HX Tube Break	∞
RHR HX Shell Break	∞
RHR HX Shell Isolation	0.273

Production for an RHR intake pipe capacity of $7.1MPa$ is similar to that of all sampled sequences (1.18 times the expected value in all sequences). There is a stronger relationship for the low sampled values for RHR HX tube and shell capacities ($9.7MPa$ and $7.9MPa$, respectively), where production is 62.3 and 48.9, respectively, times the expected value across all sequences. For all capacities, the samples used were the 25th and 75th percentile values of the distributions seen in Figure 6. In each case, the higher sampled capacities led to lower expected consequences. For example, the expected consequences for the $11MPa$ sample of RHR pipe capacity are $1.37 * 10^{-2}$ times those for the overall DET.

TABLE V. DYI3 Values for Physical Parameters, H2 Production

Branching Condition	Value	DYI3
RHR Pipe Capacity	7.1 MPa	1.18
	11 MPa	$1.37 * 10^{-2}$
RHR HX Tube Capacity	9.7 MPa	62.3
	13 MPa	$1.33 * 10^{-2}$
RHR HX Shell Capacity	7.9 MPa	48.9
	11 MPa	$2.13 * 10^{-2}$
RHR Pump Room Door Capacity	Open	1.90
	4 ft	55.2
	6 ft	$4.21 * 10^{-4}$
RHR HX Room Door Capacity	Open	4.02
	4 ft	47.4
	6 ft	$5.19 * 10^{-4}$

Apparent non-monotonic relationships are seen between the states of the RHR pump and HX room doors and hydrogen production using the DYI3 values in Table V. For the pump room door, the expected consequences when the door is left open are 1.90 times the expected consequences across the DET (See Table V). For the HX room door being left open, the ratio is 4.02. When the pump room door is closed and bursts at a water level of $4ft$, the consequence ratio against the overall DET is 55.2. The ratio for the HX room door is 47.4. However, when the pump room door is closed and has a capacity of $6ft$ the ratio is $4.21 * 10^{-4}$ indicating that the expected consequences are significantly lower at this water level capacity. For the same capacity of the HX room door,

the ratio is $5.19 * 10^{-4}$.

A door being left open in a room with a leak may result in more widespread immediate flooding of the auxiliary building but also faster draining as the water may flow through more drains. When flooding reached a level of 1 inch over the floor of the auxiliary building, all operator actions in the area were delayed. In this DET, many sequences with sampled door burst levels of $4ft$ did experience a door burst but none with a capacity of $6ft$ bursted. In sequences with a capacity of $6ft$, then, the flooding was contained to the room (or rooms) with a leak allowing operators to perform other mitigating actions. A capacity of $4ft$ appears to suffer both from early flooding of the room with the leak and of later flooding of the entire floor. This is also seen in the DYI2 values in Table VI which compare the expected consequences for each door capacity to the set of sequences where the door is left open. Compared to the RHR pump room door being left open, a capacity of $4ft$ leads to higher expected consequences (141 times the value of sequences with the door left open) while a capacity of $6ft$ leads to lower consequences ($1.07 * 10^{-3}$ times the value of sequences with the door left open).

TABLE VI. DYI2 Values for Door Capacity, H2 Production

Branching Condition	Value	DYI2
RHR Pump Room Door Capacity	4 ft	141
	6 ft	$1.07 * 10^{-3}$
RHR HX Room Door Capacity	4 ft	49.9
	6 ft	$5.46 * 10^{-4}$

IV.A.3. Isolation Event Timing

The values of DYI2 reflect the impact of a particular timing or extent of an event compared to cases where the event does not occur. An interpretation from Table VII is that relatively early isolation of an RHR HX shell rupture leads to reduced hydrogen production versus sequences where the isolation attempt fails. For example, the hydrogen production when isolation is achieved in $393s$ is $1.9 * 10^{-6}$ times the expected production when the isolation attempt fails. Late isolation ($1050s$) leads to greater production than cases where the isolation attempt fails with $2.6 * 10^{21}$ times the expected hydrogen production of a failure. Further study will be required to determine the cause of this relationship and to identify ranges of timing where isolation is either beneficial or harmful.

TABLE VII. DYI2 Values for Event Timing, H2 Production

Branching Condition	Value	DYI2
RHR HX Shell Isolation	393s	$1.9 * 10^{-6}$
	608s	$1.0 * 10^{-4}$
	1050s	$2.6 * 10^{21}$

V. CONCLUSIONS

The introduction of DI&C systems in NPPs brings with it new failure modes which may significantly affect the likelihood of accidents involving active components. The RHR ISLOCA was examined as an example of such an accident with uncertainties in the initiation and resolution phases that make it difficult to represent in a traditional PRA framework. An analysis was performed using some of the uncertainties outlined in the SOARCA study and the results were examined for insights into the RHR ISLOCA and similar accidents.

Refinement of the use of importance measures in a DET environment is expected to improve the insights that may be drawn from dynamic PRA. The implementation of a dynamic importance measure calculation framework as well as the particular set of measures used in this work have great promise for returning actionable insights from a DET comparable to importance measures used in traditional PRA. For example, the time required to isolate a break in the RHR heat exchanger was found to have a non-monotonic effect on hydrogen generation, a measure of the level of fuel damage. It was discovered that for this case earlier isolation times lead to reduced damage compared to a failed isolation attempt, but a later isolation time leads to greater damage than no isolation. When prioritizing emergency actions, such insights may be valuable in determining how long to continue dedicating resources to attempting a given action before switching to another. This is an example of the utility of dynamic PRA as the relationship may not have been discovered in a traditional PRA using binary success and failure of repair attempts. Additionally, operator depressurization of the RCS using the PORVs was demonstrated to be a viable mitigating option for this scenario as it was in the somewhat different SOARCA ISLOCA[4].

VI. ACKNOWLEDGMENTS

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

REFERENCES

1. "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants," NUREG-1150, United States Nuclear Regulatory Commission, Washington, DC (1990).

2. P. LOBNER, C. DONAHOE, and C. CAVALLIN, "Overview and Comparison of U.S. Commercial Nuclear Power Plants," NUREG/CR-5640, United States Nuclear Regulatory Commission, Washington, DC (September 1990).

3. G. BOZOKI, P. KOHUT, and R. FITZPATRICK, "Interfacing Systems LOCA: Pressurized Water Reactors," NUREG/CR-5102, United States Nuclear Regulatory Commission, Washington, DC (February 1989).

4. "State-of-the-Art Reactor Consequence Analyses Project Volume 2: Surry Integrated Analysis," NUREG/CR-7110

Vol. 2, United States Nuclear Regulatory Commission, Washington, DC (August 2013).

5. "Oconee Nuclear Station Units 1, 2, and 3, Issuance of Amendments regarding Acceptance of the Reactor Protective System and Engineered Safeguard Protection System Digital Upgrade," ML100220016, United States Nuclear Regulatory Commission (2010).

6. "Evaluation of the Proposed Change: License Amendment Request 11-07 Process Protection System Replacement," ML11307A332, United States Nuclear Regulatory Commission (2011).

7. M. DENMAN, ET AL., "Preliminary Cyber-Informed Dynamic Branch Conditions for Analysis with the Dynamic Simplified Cyber MELCOR Model," in "Transactions of the American Nuclear Society," American Nuclear Society, Las Vegas, NV (Nov 2016), vol. 115, pp. 787–790.

8. T. ALDEMIR, "A survey of dynamic methodologies for probabilistic safety assessment of nuclear power plants," *Annals of Nuclear Energy*, **52**, 113–124 (Feb 2013).

9. L. HUMPHRIES, ET AL., "MELCOR Computer Code Manuals - Vol. 1: Primer and User's Guide - Version 2.1.6840 2015," SAND2015-6691R, Sandia National Laboratories, Albuquerque, NM (2015).

10. N. S. MARTIN, M. R. DENMAN, and T. A. WHEELER, "Pruning of Discrete Dynamic Event Trees Using Density Peaks and Dynamic Time Warping," in "Transactions of the American Nuclear Society," American Nuclear Society, Las Vegas, NV (Nov 2016), vol. 115, pp. 783–786.

11. Z. JANKOVSKY, M. DENMAN, and T. ALDEMIR, "Dynamic Importance Measures in the ADAPT Framework," in "Transactions of the American Nuclear Society," American Nuclear Society, Las Vegas, NV (Nov 2016), vol. 115, pp. 799–802.

12. "Inadequate Net Positive Suction Head of Emergency Core Cooling System and Containment Heat Removal Pumps under Design Basis Accident Conditions," Information Notice 96-55, United States Nuclear Regulatory Commission (October 1996).

13. "Pressurized Water Reactor (PWR) Systems," in "Reactor Concepts Manual," United States Nuclear Regulatory Commission Technical Training Center, chap. 4.

14. D. WESLEY, "Interfacing Systems LOCA (ISLOCA) component pressure capacity methodology and typical plant results," *Nuclear Engineering and Design*, **142**, *2-3*, 209–224 (August 1993).

15. J. CARDONI, M. DENMAN, and T. WHEELER, "Severe Accident Modeling for Cyber Scenarios," in "Transactions of the American Nuclear Society," American Nuclear Society, Las Vegas, NV (Nov 2016), vol. 115, pp. 837–840.

16. R. LOFARO, ET AL., "Aging Assessment of Component Cooling Water Systems in Pressurized Water Reactors," NUREG/CR-5693, United States Nuclear Regulatory Commission, Washington, DC (June 1992).

17. "Motor-Operated Valves Course Manual," ML11347A388, United States Nuclear Regulatory Commission (May 2010).

18. "Turbine Driven Auxiliary Feedwater Pump HELB Door Left Open Resulting in Potential Loss of Safety Function," Millstone Unit 2 Licensee Event Report 2013-002-00, ML13141A286, United States Nuclear Regulatory Commission (May 2013).

19. "Turbine Driven Auxiliary Feedwater Pump HELB Door Left Open," Millstone Unit 2 Licensee Event Report 2016-001-00, ML16187A324, United States Nuclear Regulatory Commission (May 2016).

20. "Degraded Ability to Mitigate Flooding Events," Information Notice 2015-01, United States Nuclear Regulatory Commission (January 2015).

21. A. GULER, ET AL., "A Dynamic Treatment of Common Cause Failure in Seismic Events," in "Proceedings of the 2016 International Congress on Advances in Nuclear Power Plants," San Francisco, CA (April 2016).

22. "Radiation Protection Aspects of Primary Water Chemistry and Source-Term Management," NEA/CRPPH/R(2014)2, Organisation for Economic Co-operation and Development, Nuclear Energy Agency, Committee on Radiation Protection and Public Health (April 2014).

23. U. CATALYUREK, ET AL., "Development of a code-agnostic computational infrastructure for the dynamic generation of accident progression event trees," *Reliability Engineering & System Safety*, **95**, *3*, 278–294 (Mar 2010).

24. R. WINNINGHAM, ET AL., "Passive Heat Removal System Recovery following an Aircraft Crash using Dynamic Event Tree Analysis," in "Transactions of the American Nuclear Society," (2009), vol. 100, pp. 461–462.

25. Z. K. JANKOVSKY and M. R. DENMAN, "Modification of the SAS4A Safety Analysis Code for Integration with the ADAPT Discrete Dynamic Event Tree Framework," SAND2017-4764, Sandia National Laboratories, Albuquerque, NM (May 2017).

26. V. RYCHKOV and K. KAWAHARA, "ADAPT-MAAP4 Coupling for a Dynamic Event Tree Study," in "ANS PSA 2015 International Topical Meeting on Probabilistic Safety Assessment and Analysis," Sun Valley, ID (April 2015).

27. Z. JANKOVSKY, M. DENMAN, and T. ALDEMIR, "Extension of the ADAPT Framework for Multiple

Simulators," in "Transactions of the American Nuclear Society," American Nuclear Society, Las Vegas, NV (Nov 2016), vol. 115, pp. 557–560.

28. D. KELLY, J. AUFLICK, and L. HANEY, "Assessment of ISLOCA Risk-Methodology and Application to a Westinghouse Four-Loop Ice Condenser Plant," NUREG/CR-5744, United States Nuclear Regulatory Commission, Washington, DC (Apr 1992).

29. S. EIDE, T. WIERMAN, and C. GENTILLON, "Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants," NUREG/CR-6928, United States Nuclear Regulatory Commission, Washington, DC (February 2007).

30. K. COYNE, *A Predictive Model of Nuclear Power Plant Crew Decision-Making and Performance in a Dynamic Simulation Environment*, Ph.D. dissertation, The University of Maryland (2009).

31. W. VESELY, ET AL., "Measures of Risk Importance and Their Applications," NUREG/CR-3385, United States Nuclear Regulatory Commission, Washington, DC (July 1983).