Journal Title
XX(X):1–12

DOI: 10.1177/ToBeAssigned
www.sagepub.com/
SAGE

Building and using dynamic risk-informed diagnosis procedures for severe accidents

Katrina M. Groth[1], Matthew R. Denman[2], Michael C. Darling[2,3], Thomas B. Jones[3], and George F. Luger[3]

Abstract

Severe accidents pose unique challenges for nuclear power plant operating crews, including limitations in plant status information and lack of detailed diagnosis and response planning support. Advances in severe accident simulation and Dynamic Probabilistic Risk Assessment (PRA) provide an opportunity to garner detailed insight into severe accidents. In this manuscript, we demonstrate how to build and use a framework which leverages dynamic PRA, simulation, and dynamic Bayesian networks to provide real-time diagnostic support for severe accidents in a nuclear power plant. We use general purpose modeling technology, the dynamic Bayesian network[1], and adapt it for risk management of nuclear reactors. This paper presents a prototype model for diagnosing system states associated with loss of flow and transient overpower accidents in a generic sodium fast reactor. We discuss using this framework to create a risk-informed accident management framework called *SMART Procedures*. This represents a new application of risk assessment, expanding PRA techniques beyond static decision support into dynamic, real-time software for accident diagnosis and management.

Keywords

Dynamic PRA, Accident Management, Artificial Intelligence, Dynamic Bayesian Networks, Decision Support Systems

Introduction

Dynamic Probabilistic Risk Assessment (PRA) offers a comprehensive understanding of the possible accident scenarios and their associated plant states. Recent advances in computing enable simulation-based dynamic PRA approaches to explore thousands of accident scenarios via mutliple approaches[2–6]. Coupling these scenarios with plant simulations allows for prediction of plant parameters and the consequences associated with the unfolding of each possible accident sequence. However, to date, PRA has largely been used as a static technology, but as noted by Goble and Bier[7], dynamic risk assessment has significant "game-changing" potential.

In this work we present a new view of PRA as a valuable tool for management of severe accidents. Simulation-based dynamic PRA methods can provide a scientific basis for supporting diagnosis and response planning for current and future reactor designs. Running thousands of dynamic PRA simulations allows experts to explicitly map out the relationships between known accident scenarios and observable reactor parameters. However, these simulations cannot currently be used in real-time to support accident management because the methods provide too much information to process in real-time, and even simple scenarios can take days to execute due to the complexity of the underlying physics models involved.

We introduced the new "SMART (Safely Managing Accidental Reactor Transients) procedures" methodology in[8–10]. The SMART approach uses dynamic Bayesian networks (DBNs) to aggregate the results of dynamic PRA into an efficient probabilistic framework for propagating information. In the present paper we have extended our earlier models to include a much larger coverage of the reactors "state space" i.e., the set of states or situations that the reactor can be in under normal as well as possible accident scenarios. In our case studies we show how an operator can diagnose the state of the reactor by inputting the values of observable parameters.

The SMART procedures system leverages advances in simulation and computations to build a comprehensive understanding of a large range of accidents before they are experienced. This is accomplished by processing reactor state information through dynamic Bayesian networks before an accident occurs, thus harnessing the results of dynamic PRA simulations in a probabilistic framework that can handle uncertainty across time. This framework explicitly ties plant observables to possible accident scenarios and can be used to support real-time decision making.

This model provides the means to infer the state of a reactor during an accident even when only a limited amount of information about plant status and plant parameters is available. This parameter fitting, with most likely values for missing information, given the system's current priors, is usually accomplished in stochastic models with some form

[1]University of Maryland, College Park MD, USA
[2]Sandia National Laboratories, Albuquerque NM, USA
[3]University of New Mexico, Albuquerque NM, USA

Corresponding author:
Katrina M. Groth, Department of Mechanical Engineering, University of Maryland, Glenn L. Martin Hall, College Park, MD 20742
Email: kgroth@umd.edu

of the expectation maximization (EM) algorithm[11]. In the near term, parameter fitting can be used to help determine the reactor parameters that should be instrumented in the control room. We demonstrate two examples of parameter fitting in this manuscript. In the longer term, this technology results in a first step toward a full SMART procedures system.

In summary, this paper demonstrates the SMART procedures methodology across a significant component of the state space of a Sodium Fast Reactor (SFR) as well as, through case studies, presents expanded accident preventing decision making capabilities once the reactor achieves various states.

Related work

Bayesian network-based decision support systems have been successfully implemented in many industries and are especially prevalent for diagnostic support in medical applications[12,13]. Bayesian Networks (BNs) offer a language for understanding and documenting causal relationships among variables as well as for diagnosis and prediction[14–17]. Previous researchers have explored the use of Bayesian methods for nuclear power plant diagnosis, using expert knowledge and simple rules to generate models[18,19]. Zhao et al. apply a DBN to nuclear fault diagnostics while also relying on expert judgment for probabilities[20]. Early attempts to use AI technology in support of nuclear power generation focused on the components of the nuclear power plants[21].

BNs have been used within human reliability analysis (HRA) to improve modeling of human error. In 2015, Mkrtchyan et al. reviewed applications of BNs for HRA[22], and in 2016, they reviewed methods for populating BN conditional probability tables[23]. Like most of the work with BNs in HRA, all of the reviewed methods rely on probabilities calculated, at least in part, on expert judgment. Fenton et al.[24] and Baraldi et al.[25] use Bayesian networks to encapsulate expert knowledge in their conditional probability tables. Podofillini et al. use a combination of expert judgment and an interpolation method for calculation of conditional probabilities[26]. With the use of interpolation Podofillini's work introduces rigor in BNs applied to HRA. Furthermore the approach extends the use of BNs beyond analyzing human reliability, using familiar models to enhance human performance by enabling more reliable diagnosis.

However, a key gap remains: there is little research that uses PRA information to support the development of BNs for diagnosis. One notable exception is the work of Kim and Seong[27], which proposed a BN model to mimic operator reasoning, including diagnosis. They used existing procedures to develop the BN structure and causal relationships found in a static "Level 1" PRA to assign probabilities to the causal relationships. This approach demonstrates the utility of BNs as an operator model, yet it is not coupled to the physical behavior of the reactor.

No research to date has employed the use of reactor simulations or dynamic PRA to build dynamic Bayesian networks for nuclear reactor diagnosis.The SMART procedures methodology in this manuscript advances upon previous work by bringing the rigor of both dynamic PRA and DBNs into nuclear reactor diagnosis.

Building SMART procedures

The Bayesian network (BN) is a directed acyclic graph where the nodes of the graph represent the states of the components of the power producing reactor system and the directed links reflect the causal relationships between the components of the reactor. The graph is built, and probabilistic data determined, using both the knowledge of human experts as well as data derived from modeling and simulation of the power system and its components. An important advanatage of the bayesian network is that it moves from the foundational assumption of correlation in traditional bayesian models to the attribution of causality within linked components of the statistical model[28].

The theoretical framework for developing SMART procedures involves coupling dynamic PRA, system simulation codes, and Bayesian Networks to provide fast-running diagnostic support[8,9]. The methodology, as shown in Figure 1, takes outputs from an advanced PRA and aggregates them into a Bayesian Network to provide decision support. This coupled approach provides a process for extensive and comprehensive modeling of both the accident space and the plant response, in a better-than-real-time framework.

The research team develops and executes a full spectrum of runs using Discrete Dynamic Event Trees (DDETs) coupled to a reactor systems simulation code (e.g., MELCOR[29], SAS4A[30]); these runs are designed to simulate representative subsets of the expected state-space of the accident. DBNs are used to synthesize and reduce this information into a framework that can be used for faster-than-real-time decision support. This information is used in combination with PRA information, such as system failure probabilities, to provide a detailed, probabilistic model of the accident sequence space. The resulting BN model is an extensive knowledge base covering a wide spectrum of behaviors possible within the two modeled accidents. It encodes the best-available knowledge from PRA to be used when needed.

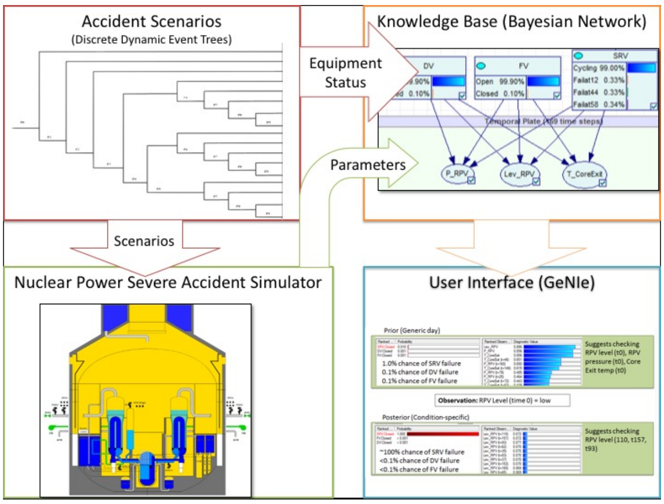

Figure 1. Conceptual process to develop risk-informed "Smart SAMG" procedures for nuclear power plant diagnostic support.

We implement the SMART procedures framework using general purpose representation and reasoning software for data simulation and Basyesian network modeling. Many software tools could be used in the SMART procedures framework to generate data and build Bayesian networks. In this paper we used the Structural Modeling, Inference, and Learning Engine (SMILE) and its associated Graphical Network Interface (GeNIe)[31], to generate the Dynamic Bayesian Network (DBN) models. We also use SAS4A[30], which is a system-level code that is capable of simulating SFR thermal-hydraulics (core and Reactor Coolant System), neutronics, and liquid metal reactor accident phenomena. Since dynamic PRA produces a large amount of data for each simulated scenario, we created a data processing system, ALADDIN[32], to automate post-processing of the SASA4A data for use in GeNIe.

Figure 2 illustrates how the structure of the model is defined to accurately capture known causal and temporal relationships. The development team designs a model by placing one node for each accident state and each modeled reactor system and component. A temporal plate is added to capture nodes whose values dynamically vary with time. A node is added inside the temporal plate for each plant parameter. Arcs are directed based on known causal relationships between the accident sequences, the reactor system components, and the plant parameters.

The team selects the number of possible states for each node based on PRA states for reactor systems and components; based on PRA definitions of accident states; and defines the desired number of time steps to be included in the model. The nodes representing the reactor systems are quantified by direct assignment in GeNIe using available system reliability and PRA data.

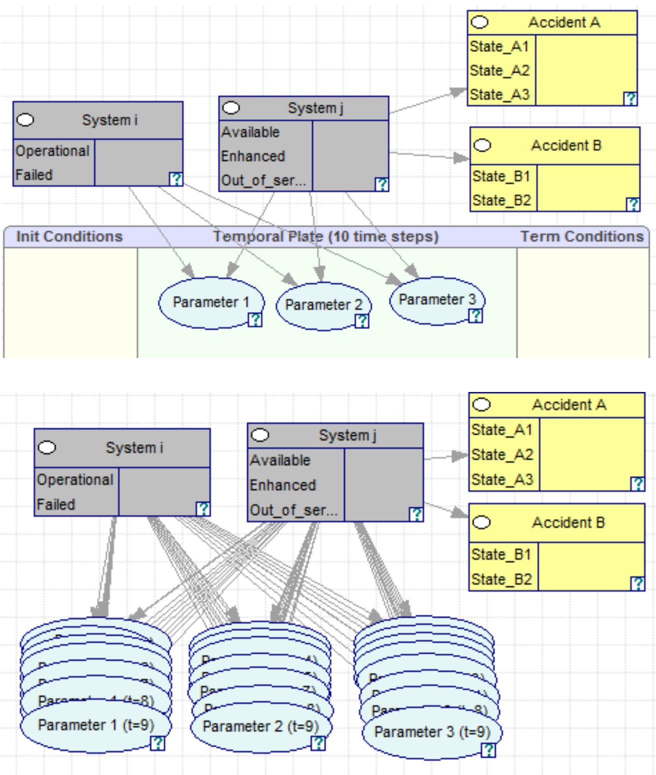

Figure 2. Illustration of the structure of the reactor diagnostic model. In the top figure, the dynamic nodes are placed in the temporal plate. In the bottom figure, the network has been unrolled: the dynamic nodes are replaced with nodes for each time step.

The parameter nodes are quantified using the results of the dynamic PRA simulations. ALADDIN, which is shown in Figure 3, automates the quantification of the DBN model by parsing and consolidating the SAS4A data to match the number of time steps and node states in the the DBN. The data for each parameter are partitioned using Equal Width Binning based on the parameter's value at each time step. The parameter node states are a user-defined number of bins e.g., high, medium, low. Whether Equal Width Binning is the most effective discretization scheme is an area for further research. ALADDIN uses the discretized data to build a conditional probability tree (which is a catalog of the conditional probabilities of each observed variable for every possible combination of node states). These probabilities are conditioned on the state of the reactor component system and accident state variables. ALADDIN then unrolls the GeNIe model and assigns a conditional probability for each node at each time step.

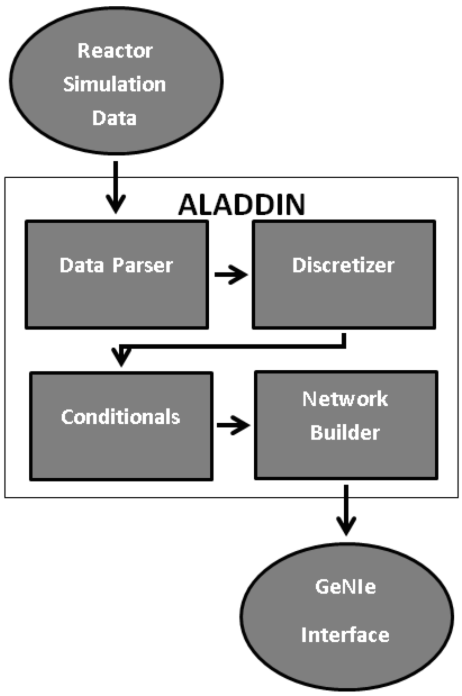

Figure 3. A data flow diagram of the SAS4A data parser (where rectangles denote processes and ovals denote inputs and outputs). Data is first read by the data parser, and then time steps are selected by the discretizer. This data is then transported by the network builder to the conditional class which calculates the conditional probabilities of each of the observed variables.

Case study

Problem Description

The prototype model is intended to focus on diagnosis of earthquake-induced Transient Overpower (TOP) scenarios and long-term reduction in heat removal, such as degraded cooling functionality, and primary pump trip (loss of flow, LOF).

The reactor model used in this study is a generic, small modular metallic fueled SFR with features adopted from the Advanced Liquid Metal Reactor design (see Figure 4).

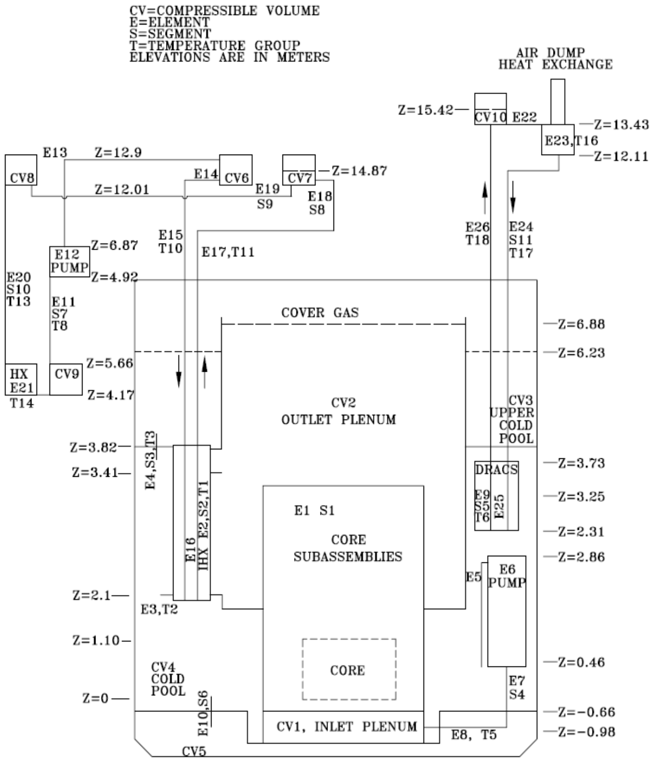

Figure 4. High level diagram of Sodium Fast Reactor used in SAS4A simulations. The primary system pumps (E6) flow relatively cold sodium over the reactor core. The fuel in the core (at a rate managed by control rods) heats the sodium which then transfers energy through the heat exchanger to secondary sodium. This secondary sodium heats water in a steam generator (E21) which drives a steam turbine. The secondary pumps (E12) return the cooled sodium from the steam generator to the heat exchanger for reuse.

Some key design features which are relevant to modeling the selected accident sequences are:

Four Electro-Magnetic Pumps
which provide force circulation in the primary system to cool the reactor core. Displayed as one pump element (E6) in Figure 4; each pump is assumed to contribute 25% of the maximum flow. These pumps may fail above 500 °C (773K) operating temperature.

Direct Reactor Auxiliary Cooling System
DRACS is a passive decay heat removal system which uses natural circulation to transfer heat to air (seen in Figure 4 as E9).

Inherent reactivity shutdown the reactor system exhibits strong negative reactivity feedback to increases in overall system temperature; thus the reactor can move from fission to decay heat levels without control rod insertion.

DDET / SAS4A simulations

The simulations provided for the prototype focuses on four types of accidents: both seismic and non-seismic-induced TOP and LOF. Each accident sequence might be either "protected" or "unprotected" depending on whether scram occurs. Each accident sequence has the potential for long-term reduction in heat removal, such as degraded auxiliary cooling functionality or primary pump trip damage.

The DDET was designed to branch on multiple conditions for the magnitude of an earthquake, balance of plant (BOP) availability, scram state, DRACS state, secondary pump power, reactivity response, and coolant pump status. The reactivity excursion occurs between 1 s and 50 s, pump trip effects occur between 80 s and 1000 s, and long-term cooling (or lack thereof) by the DRACS is important between 1000 s to the end of the simulation (48 hours or 1.7×10^5 seconds).

This branching is designed to cover all possible combinations of states of the modeled components. Some branching conditions, such as time of thermal pump failure, are determined dynamically by SAS4A. Thermal pump DDET branches occur if SAS4A predicts cold pool temperature exceeding 878.5K. Pump trip can also occur as an operator action in some branches once cold pool temperature reaches 798K.

The accident scenarios investigated in this work are earthquake-induced TOPs that involve axial and radial oscillations of the reactor, which are represented as sinusoidal functions of reactivity insertion near time = 0s. The axial oscillations characterize movement of the control rods. Oscillations may affect control rod (scram system) functionality: Control rods may scram correctly (full insertion), jam in a nominal state, or fully withdraw. Control rod expansion feedback is neglected. This assumption is somewhat conservative since the control rods tend to expand into the core as temperatures increase, thereby inserting negative reactivity; some thermal expansion into the core might still occur even with the rods oscillating.

BOP can be operational, decayed, or shutdown; in the latter the loss is simultaneous with the earthquake reactivity insertion (near time = 0 s). The DRACS is treated as functional, but the tube-to-air heat transfer coefficient for the Air Dump Heat Exchanger (ADHX) is variable (i.e., a DDET branch parameter) which can enhance or degrade DRACS functionality (the DBN states for DRACS). The pump torque and external reactivity tables are disabled in the SAS4A input to support dynamic pump trips and various reactivity insertions (e.g., earthquake and/or scram); instead, pump torque and external reactivity is linked to the control system input. Finally, pump coast-down is assumed constant in all scenarios with a 10 s halving time. Coast-down of the EMPs is an important safety feature for power and flow transients.

The event tree also includes nominal scenarios with no earthquake and thus no reactivity excursion. These nominal scenarios include various combinations of states of the other variables, including variations in occurrence of scram and balance of plant failures and variable DRACS and pump states. Such scenarios are investigated in order to provide baseline conditional probabilities in the BN.

Each SAS4A run corresponds to an event tree branch for various accident scenarios, operator actions, and dynamically-determined bifurcations in accident progression. The main event tree is comprised of 7188 distinct SAS4A simulations. Each simulation has 2588 time steps corresponding to the first 48 hours of the scenario. Example output of fuel temperatures for 50 of the 7188 scenarios is presented in Figure 5.

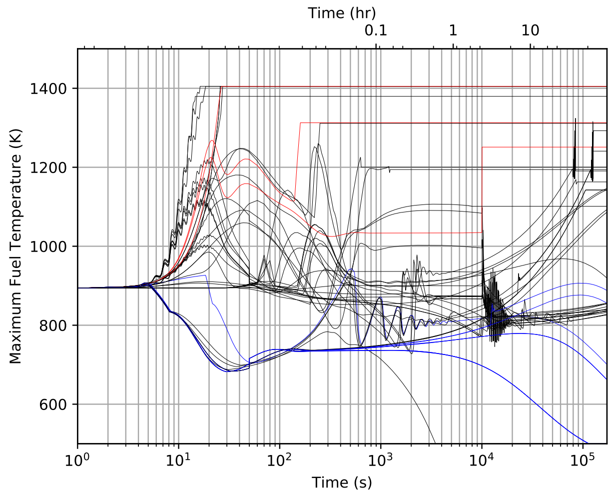

Figure 5. SAS4A results for Maximum Fuel Temperatures. Red lines correspond to simulations with degraded decay heat removal, blue lines correspond to simulations with functional decay heat removal, black lines signify simulations with varying degrees of decay heat removal functionality.

The DBN model for TOP/LOF diagnosis

The DBN Model Structure

Figure 6 provides the DBN structure for the TOP and LOF diagnosis problem. This figure contains a plate-based DBN modeling the relationship between reactor systems and components (denoted by gray, rectangular nodes), one unmonitored physical state (denoted by the blue, rectangular node), plant parameters (denoted by green, oval nodes), and accident types (denoted by yellow rectangular nodes).

The model in Figure 6 contains two accident states, seven reactor systems and components (the DRACS, the BOP, four EMPs, and the scram system), and one unmonitored physical state (Differential Pressure, which is produced by operational EMPs). The model also contains twelve plant parameters which may provide insight into the status of the reactor systems and the accident states. These plant parameters and their ranges from the SAS4A data are shown in Table 1. The model structure shows that the four EMPs directly influence the amount of differential pressure; we assume each pump contributes up to 25% of the differential pressure. The time-varying reactor parameters are duplicated once for each time step, which were distributed as follows:

- 24 time steps for the first 0.1 hr
- 24 time steps from 0.1 hr to 1 hr
- 24 time steps from 1 hr to 10 hr
- 24 time steps after 10 hr

DRACS availability, scram status, BOP status, and pump differential pressure each influence the state of all twelve (including four monitored) plant parameters at each time step in the model. In this example model, the status of the DRACS, BOP, scram system, and EMPs remain constant throughout the duration of the accident (i.e., they are modeled in the DBN to either have failed at time 0 or remain operational: they do not fail during the accident).

The scram system influences the state of the TOP node; this represents the definitional relationship wherein an unprotected TOP is defined by failure of the scram system. Similarly the differential pressure influences LOF via a direct definitional relationship since a LOF accident is defined by loss of differential pressure.

Probability Tables

For reactor system and accident type nodes the probabilities were extracted from the PRISM reactor preliminary safety information document[33].

Accident State Nodes The conditional probability table for the LOF node in the DBN is shown in Table 2. Since the LOF accident is defined by a loss of differential pressure, the conditional probability table for LOF is deterministic; this means that the state of LOF is completely determined by the state of differential pressure. If there is 0% of the required differential pressure, a Total LOF has occurred. If there is 25% or 50% of the required differential pressure, a partial LOF has occurred. If there is approximately 100% of the required differential pressure, there is no LOF.

The conditional probability table for the TOP node is shown in Table 3. Since there is minimal available data on the reliability of SFR systems, the probability of transient overpower was assigned directly by the analysis team. The team will update these values if additional SFR reliability data becomes available.

Reactor Systems and Physical State Nodes The conditional probabilities for differential pressure are derived directly from the causal relationships between flow from the EMPs and differential pressure. The conditional probabilities for differential pressure are shown in Table 5. High probabilities (0.95 and above) are assigned to the expected state of differential pressure based on EMP status. To accommodate the possibility that unmodeled factors could impact the relationship between EMPs and differential pressure, a nominal probability (ranging from 0.0001 to 0.025) was assigned to some states. The probabilities have been assigned based on expert judgment about the likely state of differential pressure given the status of the pumps.

The marginal probability tables for the reactor systems (DRACS, EMPs, BOP, and the scram system) are shown in Table 4. With all four pumps working, the differential pressure is expected to be 100%. With one of four pumps in the failed state, the differential pressure is likely to be around 50%. With three pumps failed, the differential pressure is likely to be at 25% of what is necessary. If all four pumps are failed, the DP will have none of the necessary flow. These most likely states are thus assigned high probabilities. To accommodate the possibility that unmodeled factors could impact the relationship between EMPs and differential pressure, smaller probabilities have been assigned to other states that are possible.

Monitored Parameters The SAS4A data are used to quantify the monitored reactor parameter nodes. The SAS4A data matrices map the states of the system nodes onto the states of each plant parameter at each time step. This

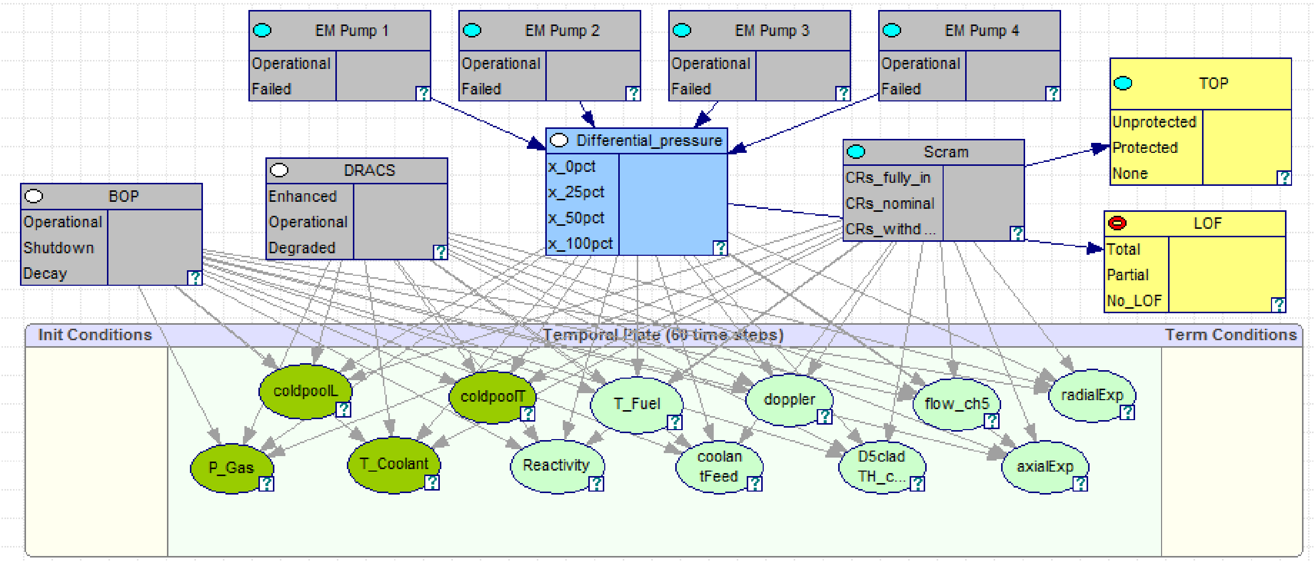

Figure 6. DBN Model Structure for the diagnosis of loss of flow and transient overpower accidents. The reactor parameters are dynamic nodes, and therefore, placed on a temporal plate.

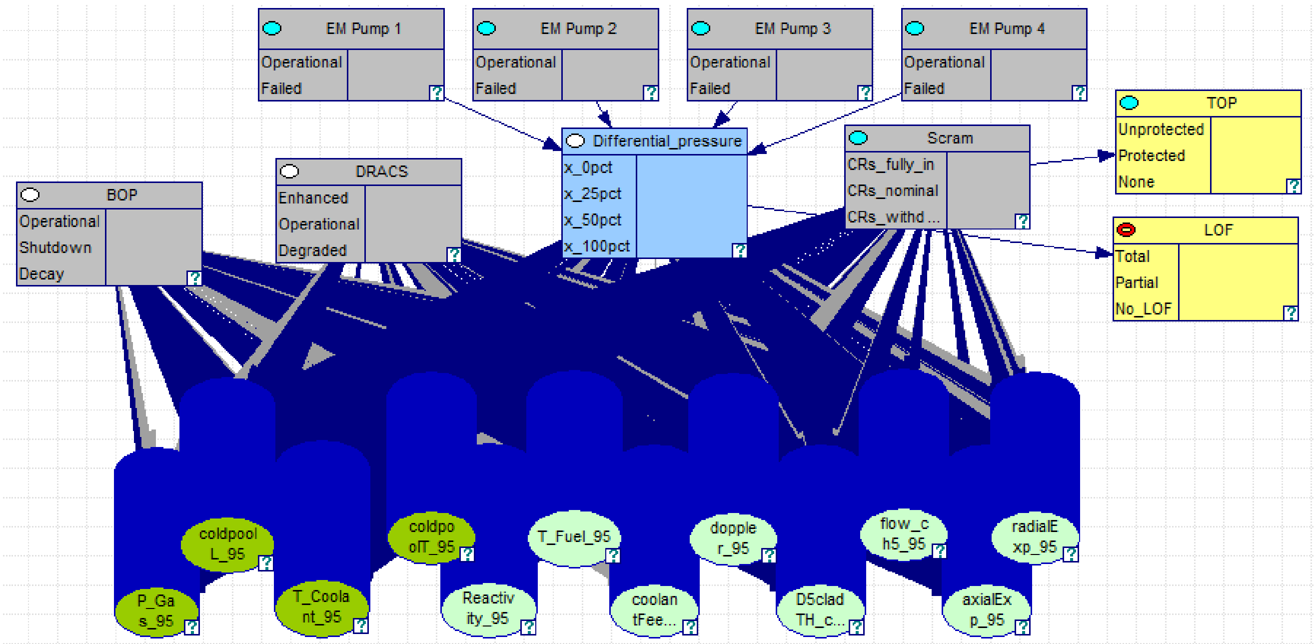

Figure 7. Unrolled DBN of figure 6: the dynamic nodes are replaced by a node representing the value of the parameter at each time step.

time series data was parsed and discretized using an N-ary discretization procedure. Multiple simulations are run for many possible system configurations to cover as much of the accident state space as possible.

After parsing and discretization, ALADDIN calculates the conditional probabilities for each of the nodes in our DBN. If we let P be the number of plant parameter nodes, T be the number of time steps, N be the number of bins for each plant parameter node, and S be the number of reactor system state combinations, then the number of conditional probabilities is $P \cdot N \cdot S \cdot T$. For this example model where P = 12, T = 96, N = 3, and S = 108, we have $373,248$ conditional probabilities. Due to space considerations we have not included the probabilities for the plant parameter nodes.

Example results from the DBN

In this section we illustrate how to use the model to reason about specific scenarios. The DBN is a knowledge-based system capable of inferring current and future states of reactor systems and plant parameters. In some cases, the input of just a few observations change the predicted plant state.

The user sets evidence on any number of nodes in the model. This evidence automatically propagates to generate a posterior distribution of the probability of every unobserved node in the model. Since evidence can be added or retracted at any time, the DBN allows the user to experiment with the model in multiple ways. For example, to diagnose specific accidents the user assigns evidence to the plant

Table 1. Plant Parameter Nodes and their range of values as parsed into 3 discrete states by ALADDIN.

Node ID	Meaning	Min.	Bin0 Max	Bin1 Max	Bin2 Max
axialExp	Axial Expansion Reactivity Feedback ($)	-0.62	-0.34	-0.07	0.22
coldpoolT	Cold Pool Temperature (K)	400	438.89	828.79	1230.5
coldpoolL	Cold Pool Level (m)	5.68	3.3×10^4	6.6×10^4	1.0×10^5
coolantFeed	Coolant Reactivity Feedback ($)	-0.28	0.54	1.37	2.23
D5clad_TH	Cladding Thickness (Fraction of nominal)	0.0	0.34	0.66	1.0
doppler	Doppler Feedback Reactivity ($)	-0.29	0.21	0.71	1.23
flow_ch5	Flow Rate in Channel 5 (kg/s)	-96.47	-40.92	14.63	71.86
P_Gas	Cover Gas Pressure (Pa)	1.4×10^4	7.4×10^5	1.5×10^6	2.2×10^6
radialExp	Radial Expansion Reactivity Feedback ($)	-0.62	-0.22	0.18	0.60
Reactivity	Net Reactivity ($)	-24.60	-16.04	-7.47	1.35
T_Coolant	Peak Coolant Temperature (K)	400	571.56	1078.45	1600.7
T_Fuel	Peak Fuel Temperature (K)	400	Melt	Melt	Melt

Table 2. Conditional Probabilities for LOF, given Differential Pressure

Diff. Pres.	0pct	25pct	50pct	100pct
Total	1	0	0	0
Partial	0	1	1	0
No_LOF	0	0	0	1

Table 3. Conditional Probabilities for TOP, given scram State

Scram	Fully in	Nominal	Withdrawn
Unprotected	0	9.59×10^{-14}	2.9×10^{-7}
Protected	1	3.31×10^{-7}	˜1
None	0	˜1	0

Table 4. Marginal Probabilities for DRACS, the four EM Pumps, scram, and BOP.

	State	Probability
DRACS	Enhanced	1.19×10^{-12}
	Available	˜1
	Unavailable	3.97x10^{-13}
EM Pumps	Operational	0.9996
	Failed	4.38×10^{-4}
Scram	CRs_fully_in	0.0150
	CRs_nominal	0.985
	CRs_withdrawn	3.04×10^{-6}
BOP	Operational	0.985
	Shutdown	0.0150
	Decay	7.95×10^{-12}

parameter states and examines the posterior probability of those accidents. To predict possible future states the user sets evidence on the state of reactors systems and/or the observed plant parameters and examines the plant parameter states at subsequent time steps.

Tables 6 and 7 show the results of inputting evidence of specific conditions to illustrate diagnosis of the reactor's state. To identify the plant parameters most significant for diagnosis of the accident, we performed an Information Gain analysis (see next section and Figure 8).

Table 6 illustrates an example scenario for diagnosing the reactor systems and accidents given knowledge of a few plant parameters. The results of this example show that a few critical pieces of information about the plant state can make a significant change in the belief about the state of the reactor and which accident scenarios the reactor is and is not experiencing. The second column of Table 6 provides the prior probabilities for the reactor system states (i.e., the initial state of the DBN model). As shown in column 2, the differential pressure is highly likely to be at 100% of the needed flow, $P(DP = 100pct) = 0.998$, and the probability of a total LOF, $P(LOF = Total)$, is only 1.69×10^{-11}. Now we make two observations about the coolant temperature during the accident (column 3): we set the value of the coolant temperature to bin1 (between 571.5 K and 1078 K) at time steps 48 and 49 (3980 s and 4900 s, approximately 66 and 81 minutes into the accident).

Once the evidence is propagated, the posterior probabilities of the plant system nodes are calculated as seen in column 4. Column 4 shows a significant change in the probability of the state of differential pressure and thus also the probability of a LOF accident. In this situation, the differential pressure is highly likely (˜96%) to be at 0% of the needed flow. The probability of LOF=TOTAL went from 1.69×10^{-11} to almost 96%. Notice also that the probability distributions for the BOP, DRACS, and scram systems and the TOP accident have experienced almost no change as a result of this evidence: Both BOP and DRACS are highly likely to be operational and scram is highly likely to be nominal. Therefore, based on the evidence we have, it is highly likely that this reactor is experiencing a total LOF accident with no TOP.

Table 7 illustrates a second diagnostic example. The results of this example show that a few pieces of information can change the belief about the plant state without being entirely deterministic about the scenario, i.e., this is a case where the information supports narrowing down beliefs to a few possible conditions or accident states. The second column of Table 7 provides the prior probabilities for the reactor system states (these are identical to the prior situation presented in Table 6).

Now we can make a series of observations about the cold pool temperature being high (between $828.79K$ and $1230.5K$) – we set the value of cold pool temperature to $bin2$ at time steps 13, 24, 31, 32, 38 (30.7 s, 440 s (7.3 min), 1000

Table 5. Conditional probability table for differential pressure.

EMP1	Operational								Failed							
EMP2	Operational				Failed				Operational				Failed			
EMP3	Operational		Failed		Operational		Failed		Operational		Failed		Operational		Failed	
EMP4	Op.	Failed	Op.	Failed	Op.	Failed	Op.	Failed	Op.	Failed	Op.	Failed	Op.	Failed	Op.	Failed
x_0%	0	0	0	0	0	0	0	0.05	0	0	0	0.05	0	0.05	0.05	0.9999
x_25%	0	0	0	0.05	0	0.05	0.05	0.9	0	0.05	0.05	0.9	0.05	0.9	0.9	0.0001
x_50%	0.0001	0.99	0.99	0.25	0.99	0.25	0.25	0.05	0.99	0.25	0.25	0.05	0.25	0.05	0.05	0
x_100%	0.9999	0.01	0.01	0.7	0.01	0.7	0.7	0	0.01	0.7	0.7	0	0.7	0	0	0

Table 6. Comparison of prior and posterior probabilities for reactor system states given evidence about coolant temperature at time steps 48 and 49 (3980 s and 4900 s).

System	Prior	Evidence	Posterior
BOP	Operational = 0.985 Shutdown = 1.5×10^{-2} Decay = 7.95×10^{-12}	t_coolant_48 = bin1 t_coolant_49 = bin1	Operational = 0.985 Shutdown = 1.5×10^{-2} Decay = 8.63×10^{-12}
DRACS	Enhanced = 1.19×10^{-12} Operational = ~1 Degraded = 3.97×10^{-13}		Enhanced = 1.71×10^{-12} Operational = ~1 Degraded= 5.53×10^{-13}
Differential Pressure	0_pct = 1.69×10^{-11} 25_pct = 5.79×10^{-8} 50_pct = 1.83×10^{-3} 100_pct = ~0.998		0_pct = ~0.96 25_pct = 2.18×10^{-9} 50_pct = 6.91×10^{-5} 100_pct = ~3.76×10^{-2}
Scram	Fully_In = 1.5×10^{-2} Nominal = ~0.985 Withdrawn = 3.04×10^{-6}		Fully_In = 5.65×10^{-4} Nominal = ~1 Withdrawn = 4.03×10^{-7}
TOP	Unprotected = 9.76×10^{-13} Protected = 1.50×10^{-2} None = ~0.98		Unprotected = 2.16×10^{-13} Protected = 5.66×10^{-4} None = ~1
LOF	Total = 1.69×10^{-11} Partial = 1.83×10^{-4} None = ~0.998		Total = ~0.96 Partial = 6.90×10^{-5} None = 3.76×10^{-2}

s (16.7 min), 1160 s (19.3 min), 2120 s (35.5 min). Once the evidence is propagated, the posterior probabilities of the plant systems node are calculated (again shown in column 4).

Column 4 shows a significant change in the probability distribution of each of the plant systems and both accident states. The model now illustrates a 19% chance of a protected TOP and an 81% chance of no TOP, along with a 19% chance of a total LOF and an 81% of a total LOF. Given the limited observations, either accident condition is plausible. This uncertainty about accident state is consistent with expected plant behavior. In a LOF accident, the channel coolant temperatures would be high early in the accident. In most protected TOP scenarios, the EM pumps also trip, reducing flow and increasing coolant temperature. In essence, the coolant temperature behaves similarly for both accidents.

The current information is sufficient to indicate that there is a high likelihood that the BOP is in a decayed state (the posterior is 81%, compared to the prior of 7.95×10^{-12}). However, we would need more information to fully diagnosis this accident. In this model, additional evidence about the cold pool temperature or about flow in channel 5 would help to differentiate further among the scenarios since the the cold pool temperature will likely stay low longer into a LOF accident. If we add evidence that ColdPoolT_45 = $bin0$ (less than $438.89K$), the probability of LOF=total and TOP=protected both increase above 99.8%, demonstrating that together all of this evidence indicates that both a total LOF and protected TOP are occurring.

Value of Reactor Parameters

To provide insight into which plant parameters are most useful for diagnosing the system failures that cause the two accident scenarios, we use Kullback-Leibler (KL) divergence[34]. KL divergence is commonly used in the machine learning community to measure impact of parameters on the results of a modeling process. The result of using KL divergence in our model confirmed the insight of our nuclear engineers that the most important parameters are coolant and cold pool temperatures, as demonstrated in tables 6 and 7.

KL divergence, also referred to as information gain or relative entropy, measures the informational "distance" between two related probability distributions. We use KL divergence to measure the information lost when a node is removed from the model[35]. Thus, conclusions about the importance of a particular parameter can be drawn. If a sufficient amount of information is lost when a parameter is removed, then it can be considered important. If a low amount of information is lost when a particular parameter is removed, then that data is not very relevant to the model and, therefore, not very useful for diagnosis of the accident. For a detailed explanation of our use of KL divergence, plus

Table 7. Comparison of prior and posterior probabilities for reactor system states given evidence about cold pool temperature at time steps 13, 24, 31, 32, 38 (30.7 s, 440 s, 1000 s, 1160 s, 2120 s)

System	Prior	Evidence	Posterior
BOP	Operational = 0.985 Shutdown = 1.5×10^{-2} Decay = 7.95×10^{-12}	ColdPoolT_13 = bin2 ColdPoolT_24 = bin2 ColdPoolT_31 = bin2 ColdPoolT_32 = bin2 ColdPoolT_38 = bin2	Operational = 0.19 Shutdown = 2.95×10^{-3} Decay = 0.81
DRACS	Enhanced = 1.19×10^{-12} Operational = ~1 Degraded = 3.97×10^{-13}		Enhanced = 0.53 Operational = 0.19 Degraded= 0.27
Differential Pressure	0_pct = 1.69×10^{-11} 25_pct = 5.79×10^{-8} 50_pct = 1.83×10^{-3} 100_pct = ~0.998		0_pct = ~0.19 25_pct = 7.46×10^{-8} 50_pct = 1.11×10^{-3} 100_pct = 0.81
Scram	Fully_In = 1.5×10^{-2} Nominal = ~0.985 Withdrawn = 3.04×10^{-6}		Fully_In = 2.18×10^{-6} Nominal = 0.81 Withdrawn = 0.19
TOP	Unprotected = 9.76×10^{-13} Protected = 1.50×10^{-2} None = ~0.98		Unprotected = 5.53×10^{-8} Protected = 0.19 None = 0.81
LOF	Total = 1.69×10^{-11} Partial = 1.83×10^{-4} None = ~0.998		Total = 0.19 Partial = 1.10×10^{-3} None = 0.81

numerical values to describe "sufficient" or "low" amounts of information in the measurement of reactor parameters, see [10].

Figure 8 contains the results of KL divergence calculated as a function of time for the twelve plant parameters. The KL divergence results indicate that coolant temperature, cold pool temperature, radial expansion reactivity, doppler, cladding temperature each have high diagnostic power for the accident scenarios in this model.

Figure 8 also indicates that T_fuel, P_Gas, cold pool level, and axial expansion reactivity have relatively low information gain. Doppler and radial expansion reactivity provide high information gain early in the accident, but drop off sharply around 120000 s (~34hrs into the accident).

The KL divergence results in Figure 8 affirms our nuclear engineer's prior beliefs regarding which parameters would be most useful when diagnosing these types of accidents. The conclusion that coolant outlet temperature has a high diagnostic value throughout the accident sequence is intuitive because: the low thermal capacity of sodium compared to water, the high dynamic operating range of the liquid phase of the coolant, between approximately 300 and 900 Celsius, and because the coolant output is the first measured location of the coolant after it was heated in the reactor core. The coolant outlet is also a measurable parameter, thus allowing for easy integration of the DBN results into the reactor digital control system without the need to develop additional sensors.

Although the fuel temperature is not measurable during normal operations, it should still have diagnostic potential which the DBN model fails to realize. This diagnostic potential should be due to the fact that the fuel temperature and coolant temperature need to equalize for the accident to stabilize. The relative trajectory that the fuel and coolant temperature take to reach an equilibrium should be unique for each type of accident. Unfortunately, the N-ary binning used to discritize this variable was dominated by an outlier sequence which reduces its diagnostic capability.

Many of the other parameters have a significant degree of diagnostic capability early in the accident which decreases as the accident progresses. The observable target node for the cold pool sodium temperature is one such variable. The cold pool temperature will fluctuate as a strong function of balance of plant operations, DRACS effectiveness, and EM pump performance. As the impact of these systems decrease into the accident, e.g., most unprotected simulations migrate toward loss of flow due to the high pressure trip on the EM pump, the ability for the variable to offer diagnostic information is reduced.

The cold and hot pool levels and cover gas pressure target nodes have little diagnostic value. These variables were included in the model because they are measured variables in the plant. These measured variables are included in the plant to diagnose accidents, such as vessel leakage, that were not simulated in our SAS4A data training data set. Thus, while the lack of diagnostic value in the current model is expected, an expansion of the accident training set may see the diagnostic value of these nodes increase in future models.

The results of the KL divergence analysis can be used to provide insight into which instruments operators should consult or which instruments should be hardened to withstand severe accident conditions. Based on the results of the prototype model, two instruments would be most valuable: one for measuring hot pool temperature, and one for measuring cold pool temperature.

Limitations of Current Model and Future Work

Our DBN model contains the consolidated information about the probability of a wide range of LOF and TOP scenarios, system states, and the progression of the plant parameters; in a Bayesian sense this is the prior model. This model can be

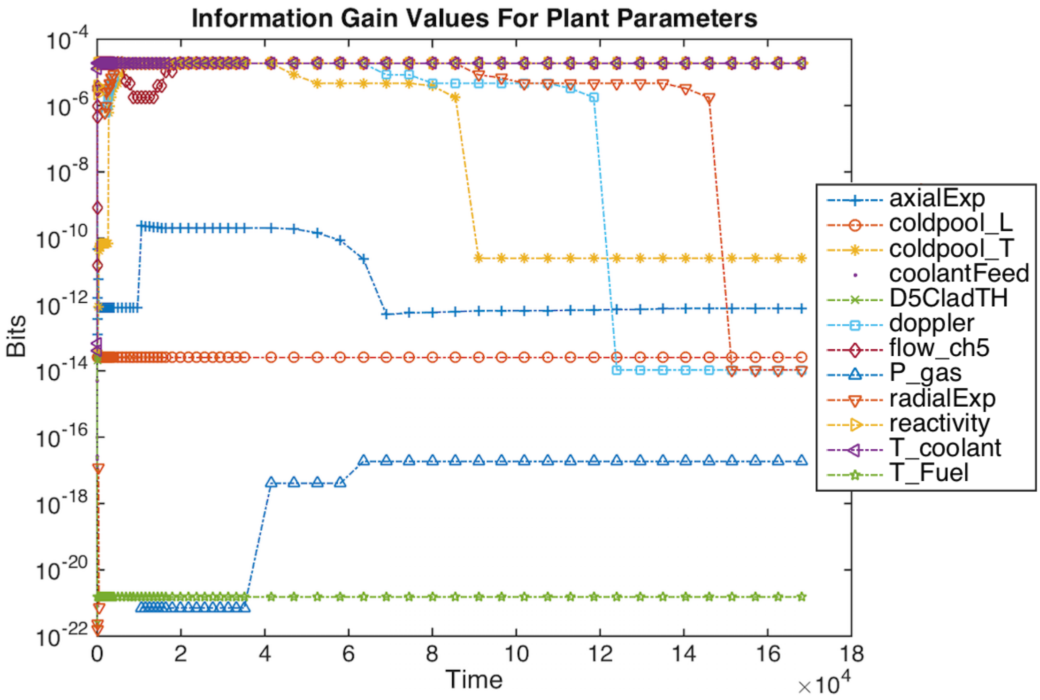

Figure 8. Information gain values for the plant parameters: The X-axis represents time; the Y-axis represents the information gain measured in bits.

used for reasoning tasks, such as diagnosing system failures, or for predicting the evolution of key reactor parameters for known system statuses. While it shows promising results, we must continue to expand and calibrate the model parameters and also expand the model in depth and breadth.

Key next steps include examining the impact of time discretization and reactor parameter discretization[36] and to assess whether different modeling choices would have greater predictive power. In the longer term, our focus will be on expanding the model to include a wider spectrum of accident scenarios. In future research the DBN could be enhanced such that it dynamically updates by receiving real-time evidence from SAS4A as simulations progress through time.

It is desirable to look at all internal and external events that cover all possible accident states of the reactor, our research is currently proof-of-concept; we have limited our models to two accident scenarios and seven system/components. Within these accident scenarios we comprehensively simulate the state space of possible changes in the reactor environment. To achieve the long-term vision, the model and data must be expanded in both the number of systems modeled and in accident scenarios.

In order to capture these critical simulations, we have created a set of dynamic and static variables in the model. The static variables reflect "boundary values" such as a certain pump failing at a specific time, that allow us to see the resulting effects within the set of dynamic parameters. To control the complexity of the model and to highlight certain scenarios, we chose all system state nodes to be static and measured the effects their states had on the dynamic reactor parameters. In future models, it will be desirable to make all of the nodes dynamic so we can capture variations in system failure times.

Conclusions

In this work we detail how to build a "SMART Procedures" risk-informed accident management model. These models have the potential to expand the use of risk information to provide real-time, dynamic support for severe accident management. The foundation of the methodology is to use dynamic PRA and severe accident simulations to build a map of the complex relationships between known accidents and evolving reactor parameters. Dynamic Bayesian networks provide a framework for reasoning with this information in real time when the plant status is uncertain.

This paper also demonstrates the use of the SMART Procedures methodology with a proof-of-concept model for diagnosing two types of accidents in SFRs. Our model is a first step toward a SMART procedures system which could provide real-time diagnostic support for TOP and LOF accidents. The model offers real-time insight into the expected temporal progression of these accidents. Our approach also provides essential insight into which reactor parameters are most useful for diagnosing and responding to severe accident situations. During severe accident progression, it may be difficult for operators to correctly diagnose and robustly manage the accident. Putting PRA simulation data into a probabilistic framework enables operating crews and other interested parties to use this knowledge base to facilitate accident diagnosis and response planning.

This system can result in increases in plant safety through accurate and timely response to critical conditions. Even if an accident experienced by the operators was not directly simulated by the advanced PRA, the probabilistic nature of the DBN will be able to use similar sequences in order to diagnose the state of the system. By formally encoding advanced PRA knowledge in SMART SAMGs, we can reduce the socio-technical challenges associated with responding to severe accidents, and provide a new, powerful line of defense against events which have traditionally been called "Beyond Design Basis" or "residual" risk.

Definitions

BN: Bayesian Network

DBN: Dynamic Bayesian Network

DDET: Discrete Dynamic Event Tree

DRACS: Direct Reactor Auxiliary Cooling System

EMP: Electromagnetic Pump

HRA: Human Reliability Analysis

KL: Kullback-Leibler

PRA: Probabilistic Risk Assessment

LOF: Loss of Flow

SAMG: Severe Accident Management Guideline

Scram: Control rod insertion

SFR: Sodium Fast Reactor

SMART: Safely Managing Accidental Reactor Transients

TOP: Transient Overpower

References

1. Luger GF. Artificial intelligence: Structures and strategies for complex problem solving sixth edition. *University of New Mexico, Addison Wesley, Pearson Education, Inc* 2009; .
2. Labeau PE, Smidts C and Swaminathan S. Dynamic reliability: towards an integrated platform for probabilistic risk assessment. *Reliability Engineering and System Safety* 2000; 68(3): 219–254.
3. Aldemir T. A survey of dynamic methodologies for probabilistic safety assessment of nuclear power plants. *Annals of Nuclear Energy* 2013; 52: 113–124.
4. Zio E. Integrated deterministic and probabilistic safety assessment: Concepts, challenges, research directions. *Nuclear Engineering and Design* 2014; 280: 413 – 419.
5. Acosta C and Siu N. Dynamic event trees in accident sequence analysis: application to steam generator tube rupture. *Reliability Engineering & System Safety* 1993; 41: 135154.
6. Kae-Sheng H and Mosleh A. The development and application of the accident dynamic simulator for dynamic probabilistic risk assessment of nuclear power plants. *Reliability Engineering & System Safety* 1996; 52: 297–314.
7. Goble R and Bier VM. Risk assessment can be a game-changing information technology – but too often it isn't. *Risk Analysis* 2013; 33(11): 1942–1951.
8. Groth KM, Denman MR, Cardoni JN et al. 'Smart Procedures': Using dynamic PRA to develop dynamic, context-specific severe accident management guidelines (SAMGs). In *Proceedings of the International Conference on Probabilistic Safety Assessment and Management (PSAM 12)*. Honolulu, HI.
9. Groth KM, Denman MR, Jones T et al. Proof-of-concept accident diagnostic support for sodium fast reactors. In *Proceedings of the European Society for Reliability Annual Meeting (ESREL 2015)*. Zurich, Switzerland.
10. Jones TJ, Darling MC, Groth KM et al. A dynamic bayesian network for diagnosing nuclear power plant accidents. In *The 29th International Florida Artificial Intelligence Research Society Conference*.
11. Dempster AP, Laird NM and Rubin DB. Maximum likelihood from incomplete data via the em algorithm. *JOURNAL OF THE ROYAL STATISTICAL SOCIETY, SERIES B* 1977; 39(1): 1–38.
12. Arroyo-Figueroa G and Suear LE. A temporal Bayesian network for diagnosis and prediction. In *Proceedings of the Fifteenth Annual Conference on Uncertainty in Artificial Intelligence (UAI-99)*. San Francisco, CA, USA: Morgan Kaufmann, pp. 13–20.
13. Lampis M and Andrews JD. Bayesian belief networks for system fault diagnostics. *Quality and Reliability Engineering International* 2009; 25(4): 409–426.
14. Jensen FV and Nielsen TD. *Bayesian networks and decision graphs*. Springer, 2009.
15. Pearl J. Causal inference without counterfactuals: Comment. *Journal of the American Statistical Association* 2000; 95(450): 428–431.
16. Druzdzel MJ. *Probabilistic Reasoning in Decision Support Systems: From Computation to Common Sense*. PhD Thesis, Carnegie Mellon University, 1993.
17. Weber P, Theilliol D and Aubrun C. Component reliability in fault-diagnosis decision making based on dynamic bayesian networks. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability* 2008; 222(2): 161–172.
18. Kaplan S, Keter A, Epstein SA et al. COPILOT – a PC-based expert system for reactor operational assistance using a Bayesian diagnostic module. *Reliability Engineering and System Safety* 1990; 30(13): 219–237.
19. Kang CW and Golay MW. A Bayesian belief network-based advisory system for operational availability focused diagnosis of complex nuclear power systems. *Expert Systems with Applications* 1999; 17(1): 21–32.
20. Zhao Y, Tong J, Zhang L et al. Pilot study of dynamic bayesian networks approach for fault diagnostics and accident progression prediction in HTR-PM . *Nuclear Engineering and Design* 2015; 291: 154 – 162.
21. Kim K and Bartlett EB. Nuclear power plant fault diagnosis using neural networks with error estimation by series association. *IEEE Transactions on Nuclear Science* 1996; 43(4): 2373–2388.
22. Mkrtchyan L, Podofillini L and Dang VN. Bayesian belief networks for human reliability analysis: A review of applications and gaps. *Reliability Engineering & System Safety* 2015; 139: 1 – 16.
23. Mkrtchyan L, Podofillini L and Dang VN. Methods for building conditional probability tables of Bayesian belief networks from limited judgment: An evaluation for human reliability application. *Reliability Engineering & System Safety* 2016; 151: 93 – 112.
24. Fenton NE, Neil M and Caballero JG. Using ranked nodes to model qualitative judgments in Bayesian networks. *IEEE Transactions on Knowledge and Data Engineering* 2007;

19(10): 1420–1432.
25. Baraldi P, Podofillini L, Mkrtchyan L et al. Comparing the treatment of uncertainty in Bayesian networks and fuzzy expert systems used for a human reliability analysis application. *Reliability Engineering and System Safety* 2015; 138: 176–193.
26. Podofillini L, Mkrtchyan L and Dang VN. Quantifying human reliability analysis bbns from partial information: combining operational event analyses and expert judgment. In *Proceedings of the European Society for Reliability Annual Meeting (ESREL 2016)*. Glasgow, Scotland.
27. Kim MC and Seong PH. An analytic model for situation assessment of nuclear power plant operators based on Bayesian inference. *Reliability Engineering and System Safety* 2006; 91(3): 270–282.
28. Pearl J. *Causality: models, reasoning, and inference*. Cambridge University Press, 2000.
29. Humphries LL, Cole RK, Louie DL et al. *MELCOR Computer Code Manuals, Vol. 2: Reference Manual, Version 2.1.6840*. Sandia National Laboratories, Albuquerque, NM, 2015.
30. Argonne National Laboratory. The SAS4A/SASSYS-1 safety analysis code system. ANL/NE-12/4, Argonne National Laboratory, 2011.
31. Druzdzel MJ. SMILE: Structural modeling, inference, and learning engine and GeNIe: a development environment for graphical decision-theoretic models. In *Proceedings of American Association for Artificial Intelligence (AAAI-99)*. pp. 902–903.
32. Darling MC, Jones TB, Luger GF et al. ALADDIN: The automatic loader of accident data for dynamic inferencing networks. SAND2015-10401, Sandia National Laboratories, Albuquerque, NM, 2015.
33. General Electric. PRISM preliminary safety information document. Technical Report GEFR-00793, General Electric, San Jose, California, 1987.
34. Cowell RG. Conditions under which conditional independence and scoring methods lead to identical selection of Bayesian network models. In *Proceedings of the Seventeenth conference on Uncertainty in artificial intelligence*. Morgan Kaufmann Publishers Inc., pp. 91–97.
35. Vergara JR and Estévez PA. A review of feature selection methods based on mutual information. *Neural Computing and Applications* 2014; 24(1): 175–186.
36. Clarke EJ and Barton BA. Entropy and MDL discretization of continuous variables for Bayesian belief networks. *International Journal of Intelligent Systems* 2000; 15(1): 61–92.

Acknowledgements

Sandia National Laboratories is a multi-mission laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's (DOE) National Nuclear Security Administration under contract DE-AC04-94AL85000. This project was funded in part by the DOE Office of Nuclear Energy Advanced Reactor Technologies Program under work package number AT-15SN200304.

The authors would like thank Jeff Cardoni and Zac Jankovsky, who conducted the SAS4A simulations referenced in this paper; Argonne National Laboratories for their assistance in providing an initial SAS4A model for the analysis.