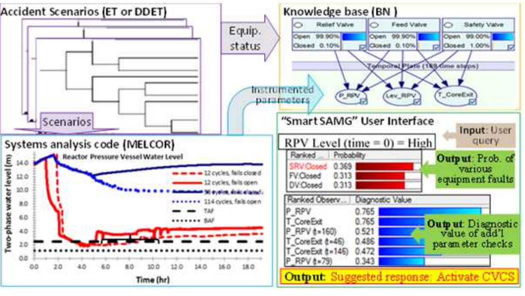
SAND2014-

SAND2014-15351PE



Sandia National Laboratories

Exceptional service in the national interest

"**Smart Procedures**": Using dynamic PRA to develop dynamic, context-specific accident severe management guidelines

Katrina M. Groth, Matthew R. Denman, Jeffrey N. Cardoni, & Timothy A. Wheeler

Sandia National Laboratories

Albuquerque, NM, USA

Probabilistic Safety and Management (PSAM 12)
25 June 2014, Honolulu, HI, USA

U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Challenge: Managing severe accidents is difficult

Fukushima response was especially challenging due to severe information limitations plus inherent human limitations

Information limitations:

- **Plant Design:** Current sensors were not designed for accident monitoring
- **Poor Guidance:** Lack of procedures and training to guide information gathering and diagnosis
- **Complexity/Dynamics:** Rapid scenario evolution, short response window

Cognitive challenges:

- **Understanding:** Developing a “big picture” from partial information
- **Filtering:** Deciding which information is relevant to the scenario
- **Prioritizing:** Deciding which information is worth expending limited resources to obtain

Objectives

- Build comprehensive, context-specific severe accident management guidelines (SAMGs)
  - Detailed, specific guidance for fault detection and data gathering
- Leverage advances in PRA and computation to build comprehensive understanding of accidents, before they happen.
  - And enable that information to be used during severe accident management

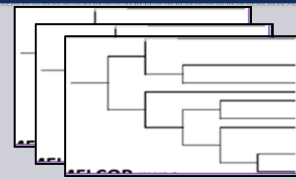
Methodology Overview

Sandia National Laboratories

Generate spectrum of accident scenarios

Goal: Identify potential accident scenarios

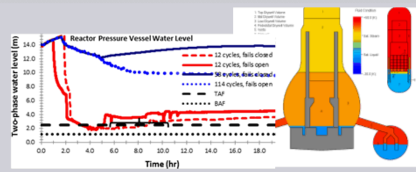
Tool: DDET/ADAPT simulation scheduler



Simulate reactor physics for each scenario

Goal: Predict range of plant parameters for known system faults

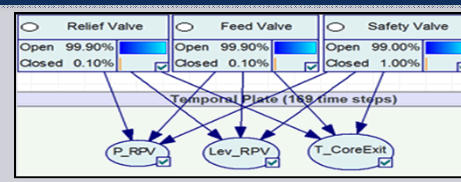
Tool: MELCOR



Encode results in a generic knowledge base

Goal: Build a map between known parameters and known faults

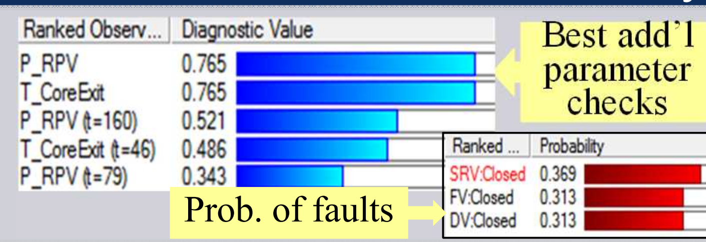
Tool: Bayesian Networks



Enable queries for specific parameters, faults, under uncertainty

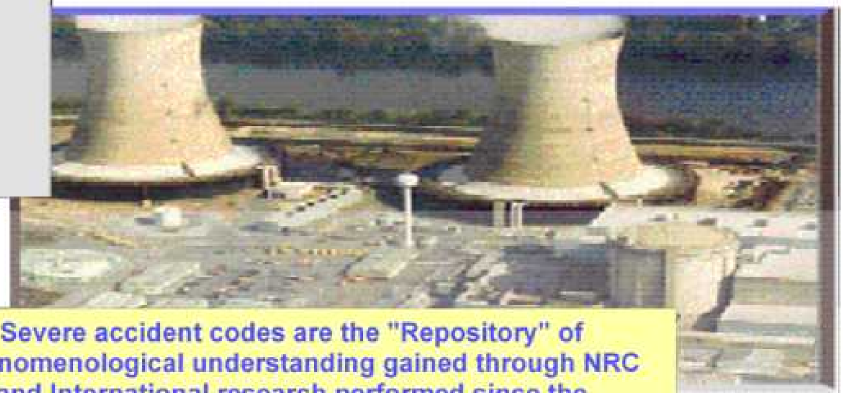
Goal: Enable users to diagnose specific faults, identify key indicators, ask "what-if"

Tool: Probabilistic queries, differential diagnosis, value of information



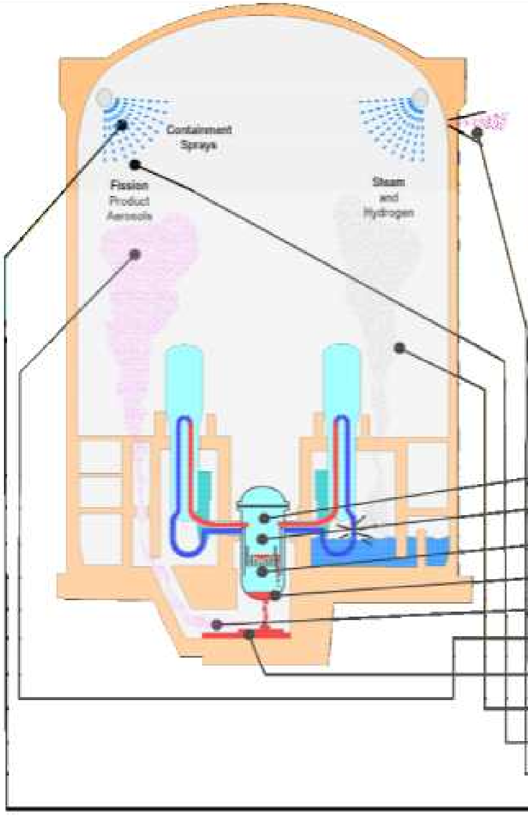
Tools (1a) – MELCOR [Simulator]

Modeling and Analysis of Severe Accidents in Nuclear Power Plants



Severe accident codes are the "Repository" of phenomenological understanding gained through NRC and International research performed since the TMI-2 accident in 1979

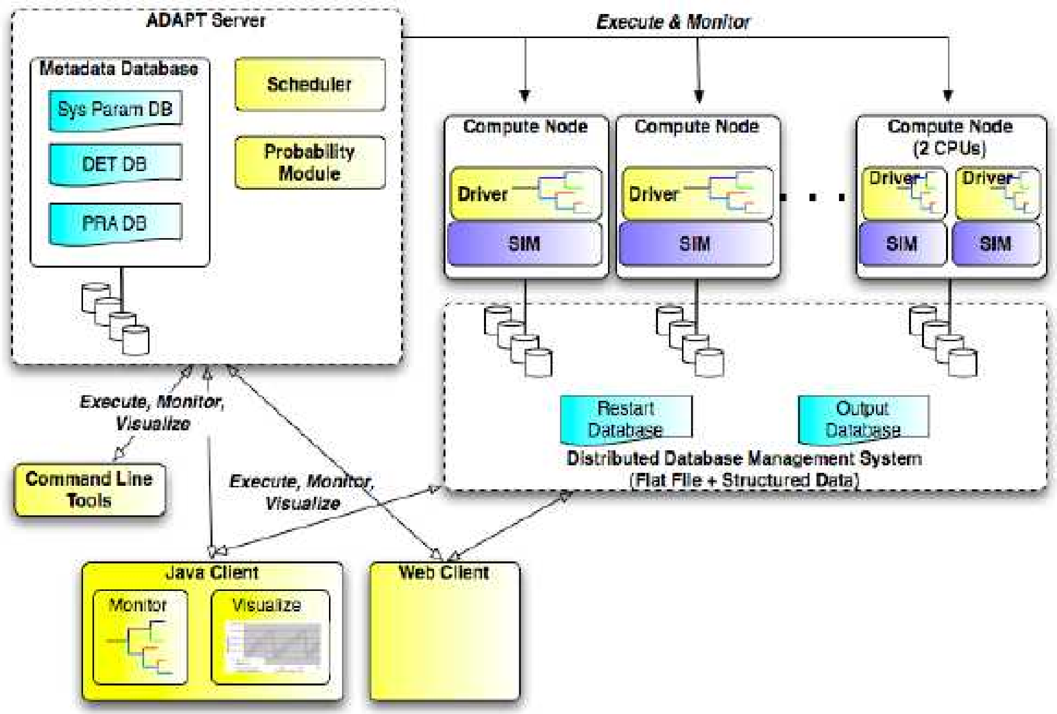
Integrated models required for self consistent analysis

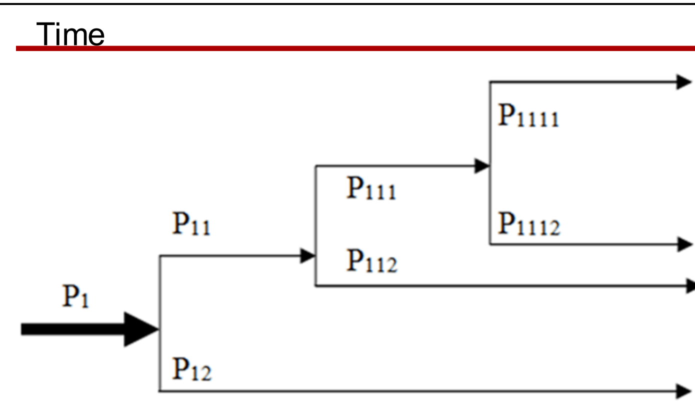


Important Severe Accident Phenomena	MELCOR	CONTAIN	VICTORIA	SCDAP RELAP5
Accident initiation	■			■
Reactor coolant thermal hydraulics	■			■
Loss of core coolant	■			■
Core meltdown and fission product release	■		◢	■
Reactor vessel failure	■			■
Transport of fission products in RCS and Containment	■	■	■	
Fission product aerosol dynamics	■	■	■	
Molten core/basemat interactions	■	■		
Containment thermal hydraulics	■	■		
Fission product removal processes	■	■	■	
Release of fission products to environment	■	■	■	
Engineered safety systems - sprays, fan coolers, etc	■	■		
Iodine chemistry, and more	■			

Tools (2) - Discrete-Dynamic-Event-Trees (DDET) [Uncertainty Exploration]

- DDET is a methodology for exploring large spectrum of possible accident scenarios via **Dynamic Programming**.
  - Simulates multiple accident sequences by branching based on physics calculations.
  - Scheduler (ADAPT) was created by a Sandia LDRD completed in 2008.

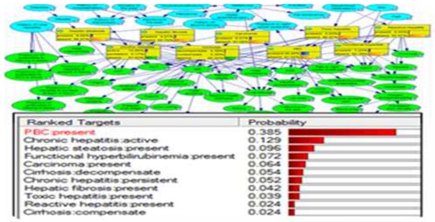




New simulations are branched mid-transient

Evolution of accident sequences is determined by physics and engineering calculations, not a priori analyst decisions.

Tools (3) - Bayesian Networks (BNs)



The generic knowledge base (BN) contains variables and [prior] probabilities

- Components of the system
- How possible defects manifest through symptoms, test results, error messages etc.

Observations:

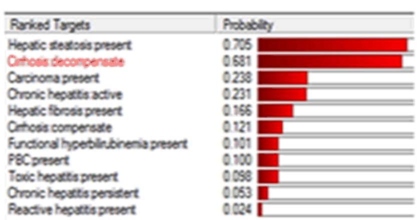
- Sex: male
- Irregular liver: present
- History of alcohol abuse: present
- Platelet count: 0-99

Users make observations about known symptoms or test results for a specific situation/person

	Parent	$Pr(a)$	$Pr(\overline{a})$
Child	$Pr(b)$	$Pr(b \mid a)$	$Pr(b \mid \overline{a})$
	$Pr(\overline{b})$	$Pr(\overline{b} \mid a)$	$Pr(\overline{b} \mid \overline{a})$

$$P(X_1, X_2, \ldots X_n) = \prod_i P(X_i \mid Par_G(X_i))$$

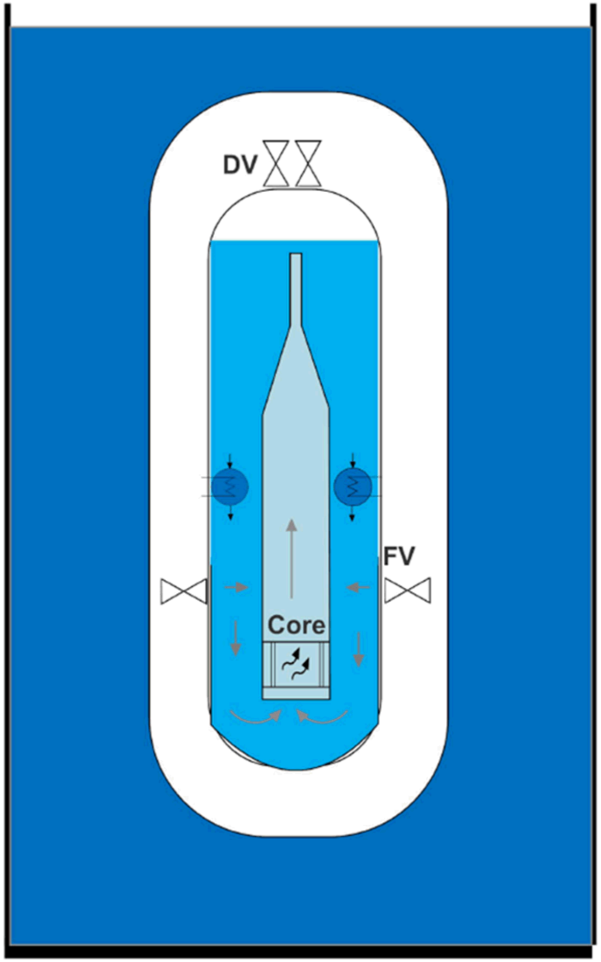
Observations are propagated (forward and backward) through the network to provide posterior probability of every node (diseases, symptoms, tests).



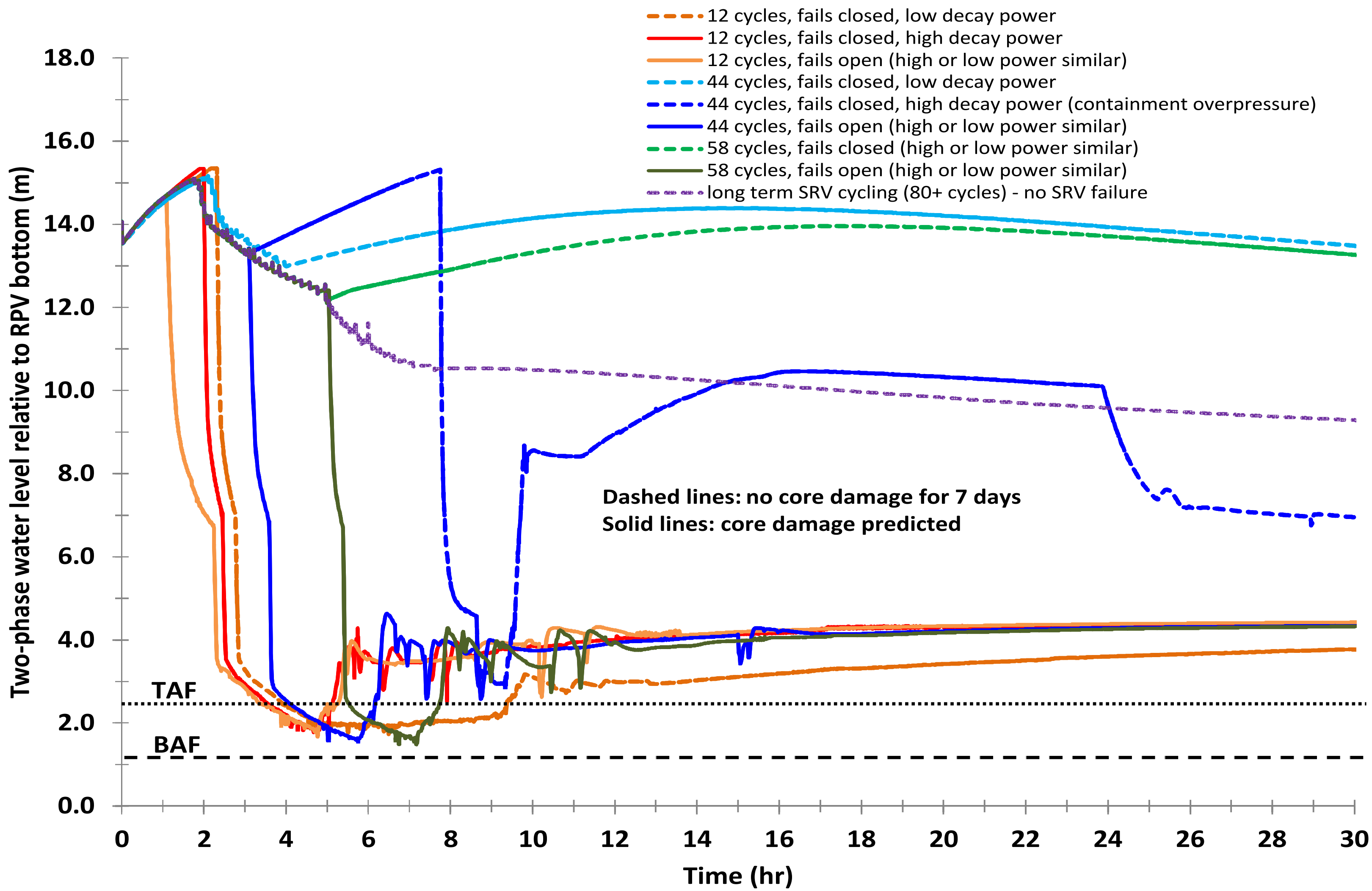
Posterior probability can be used for reasoning (e.g., ranking diseases, selecting tests, calculating value of information for tests)

Example system: iPWR

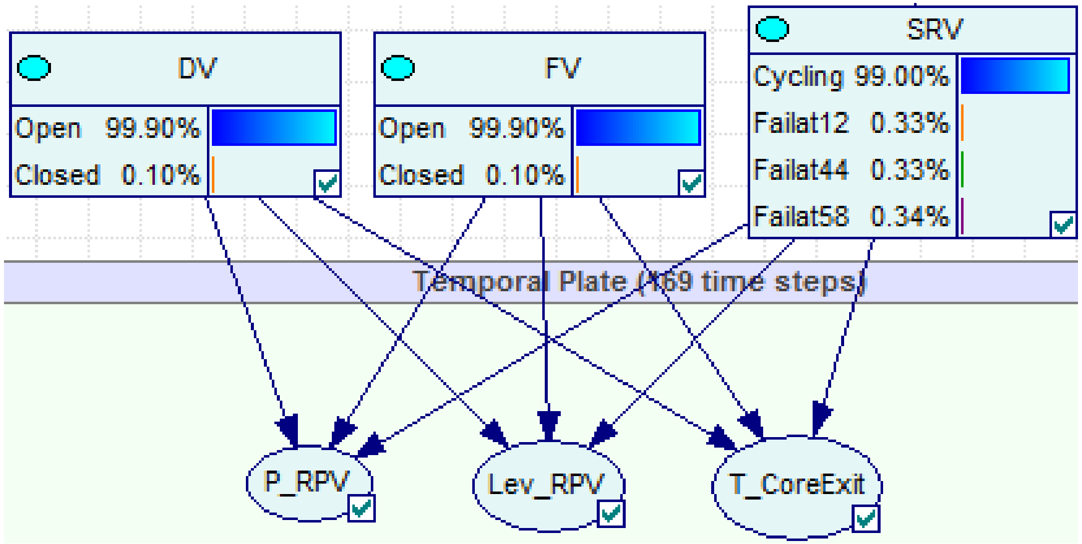
- Generic LWR SMR design (one unit)
  - 120 MW_{th} Reactor
  - Submerged in a pool
- Emergency Core Cooling System (ECCS) is composed of:
  - Depressurization Valves (DVs)
  - Feed Valves (FVs)
- Passive flow system, no safety related pumps
- Goal: diagnose loss of ECCS by assessing status of FV and DV.



SMR 1 Example – Depressurization Valves Fail to Open

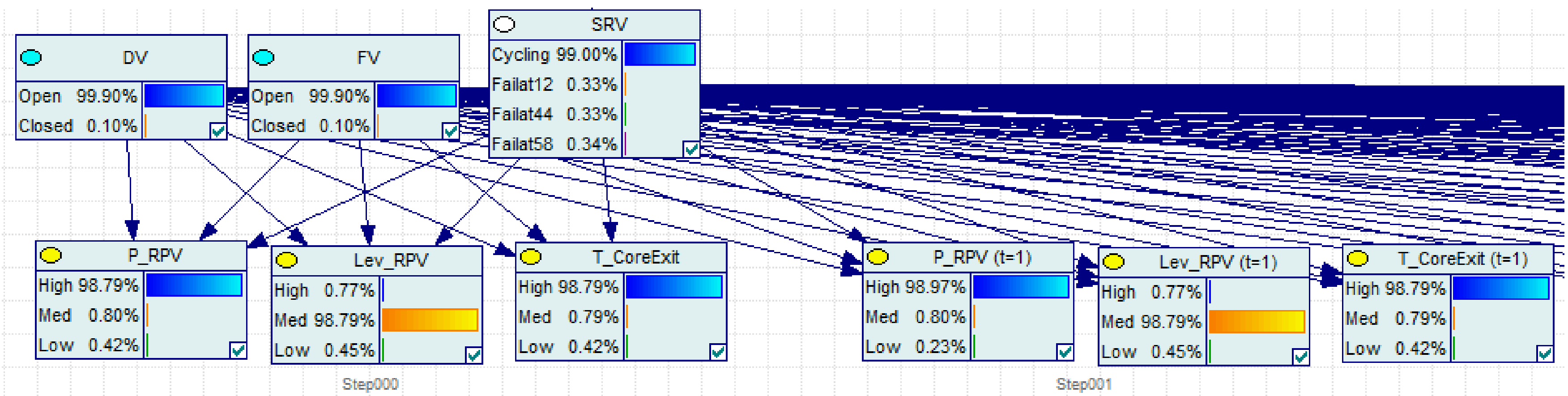


SMR 1 – iPWR Proof-of-concept structure(compact)



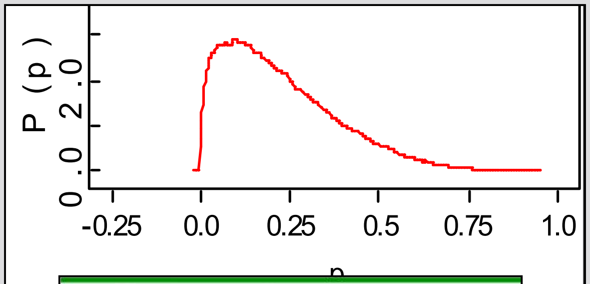
Equipment status (disease)

Indicators to check (tests)



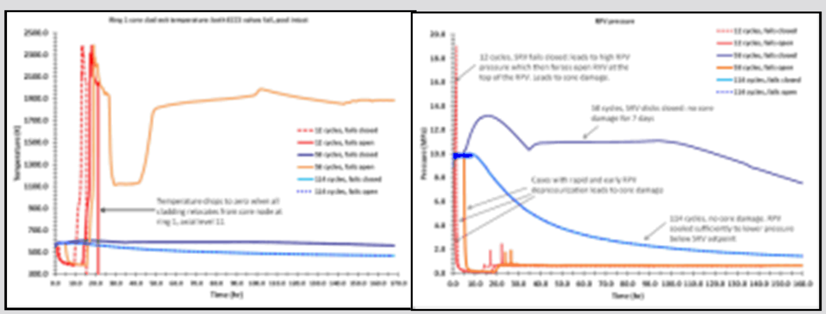
Quantifying the prior

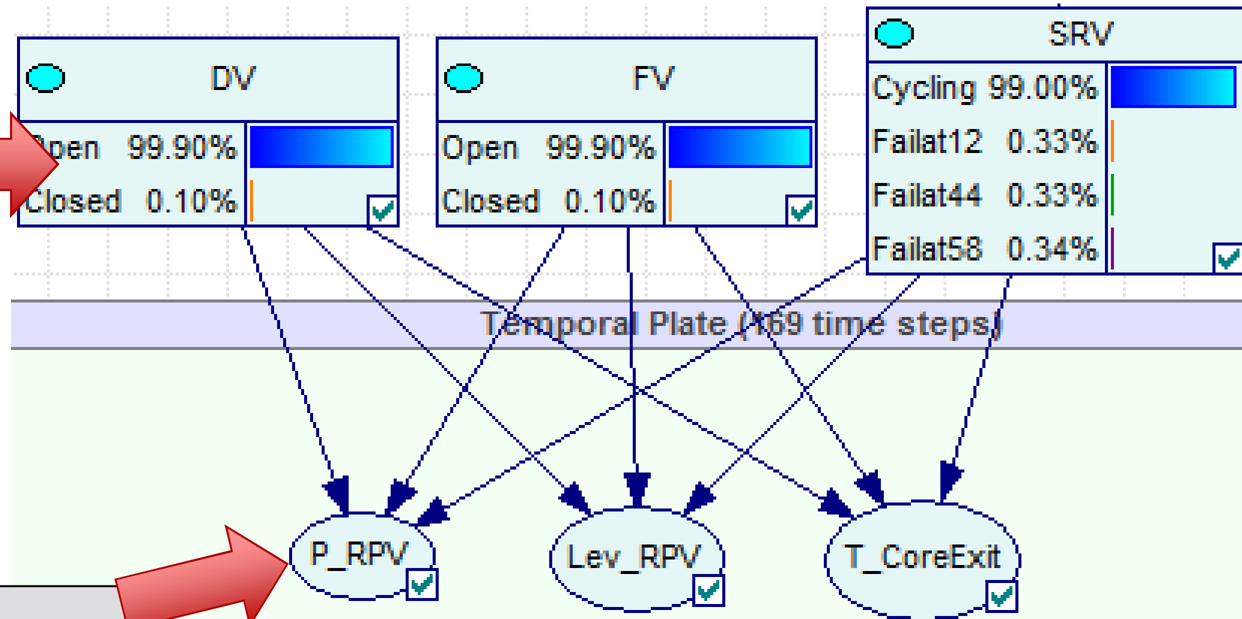
Generic PRA data



Failure Mode	Median	Mean
FTO	1.89E-03	7.71E-03
FTC	3.62E-04	7.95E-04
SO	1.24E-07	5.08E-07
FTCL	5.20E-02	1.00E-01

MELCOR runs

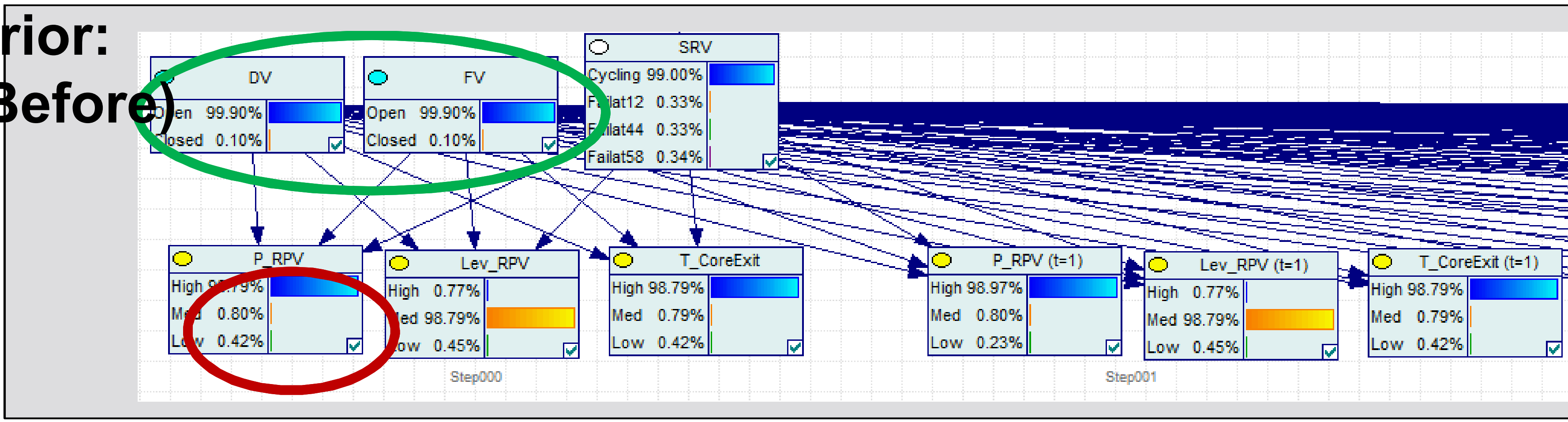




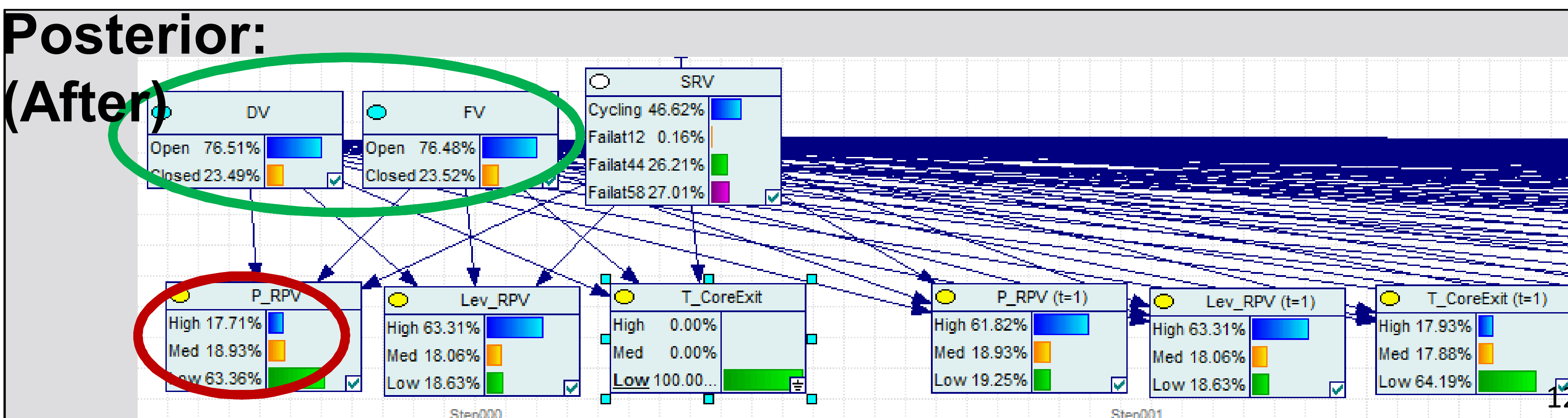
Backward reasoning (diagnosis)

- Changing about T_CoreExit (to "Low") changes belief about status of FV and DV (….and also the other parameters)

Prior: (Before)



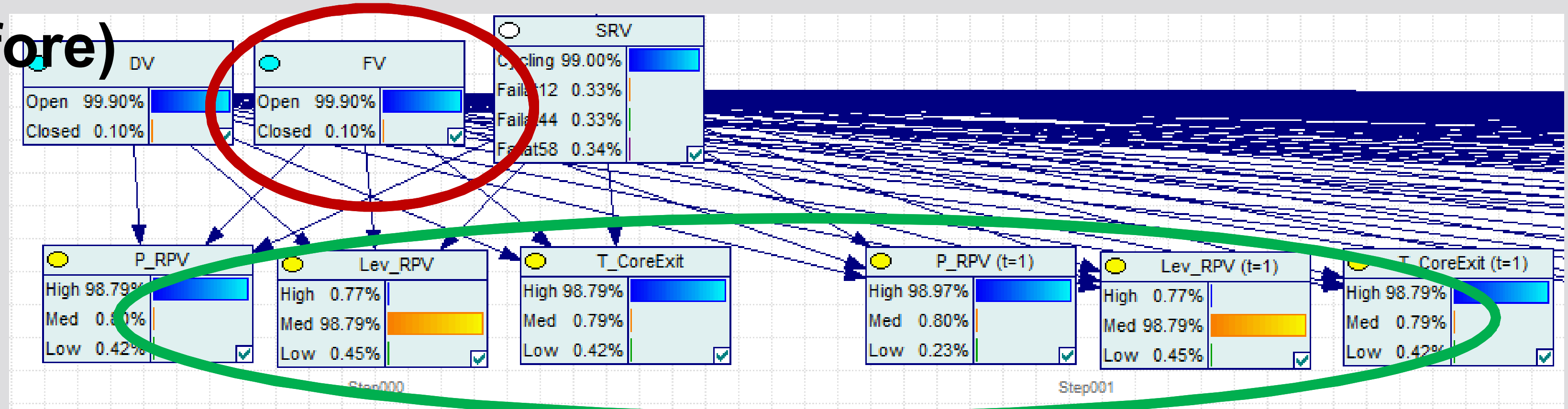
Posterior: (After)



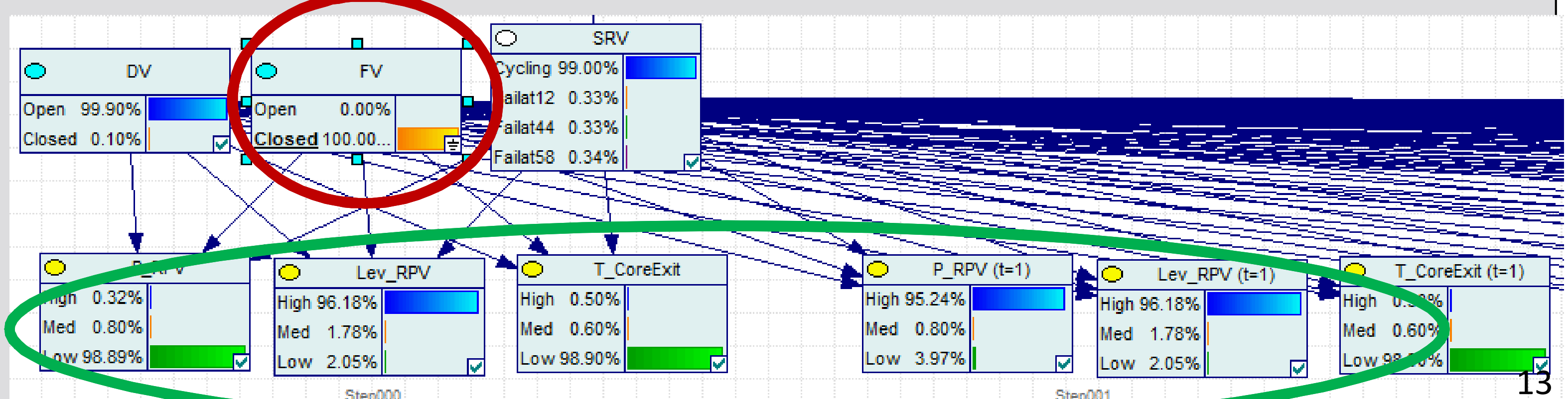
Forward reasoning

- Changing belief about FV (to FV=Closed) changes expectations about the parameters

Prior:
(Before)



Posterior:
(After)



Assisted diagnosis (real-time, iterative)

Sandia National Laboratories

Prior (Generic day)

Ranked ...	Probability
SRV:Closed	0.010
DV:Closed	0.001
FV:Closed	0.001

1.0% chance of SRV failure
0.1% chance of DV failure
0.1% chance of FV failure

Ranked Observ...	Diagnostic Value
Lev_RPV	0.896
P_RPV	0.856
T_CoreExit	0.856
T_CoreExit (t=46)	0.651
P_RPV (t=160)	0.650
T_CoreExit (t=146)	0.615
P_RPV (t=79)	0.485
P_RPV (t=25)	0.464
T_CoreExit (t=72)	0.443
T_CoreExit (t=63)	0.439

Suggests checking RPV level (t0), RPV pressure (t0), Core Exit temp (t0)

Observation: RPV Level (time 0) = low

Posterior (Condition-specific)

Ranked ...	Probability
SRV:Closed	1.000
FV:Closed	< 0.001
DV:Closed	< 0.001

~100% chance of SRV failure
<0.1% chance of DV failure
<0.1% chance of FV failure

Ranked Observ...	Diagnostic Value
Lev_RPV (t=110)	0.072
Lev_RPV (t=157)	0.072
Lev_RPV (t=93)	0.071
Lev_RPV (t=62)	0.070
Lev_RPV (t=35)	0.070
Lev_RPV (t=83)	0.070
Lev_RPV (t=37)	0.070
Lev_RPV (t=153)	0.070
Lev_RPV (t=165)	0.069
Lev_RPV (t=65)	0.069

Suggests checking RPV level (110, t157, t93)

A single key observation dramatically changes belief about ECCS status and value of additional tests

Diagnostic value of tests

Sandia National Laboratories

For FV failure

Ranked Observ...	Diagnostic Value
T_CoreExit (t=46)	0.319
Lev_RPV	0.316
T_CoreExit (t=146)	0.232
P_RPV (t=160)	0.224
P_RPV (t=128)	0.217
T_CoreExit (t=108)	0.202
Lev_RPV (t=157)	0.200
P_RPV (t=58)	0.197
Lev_RPV (t=68)	0.195
T_CoreExit	0.191
P_RPV	0.191
Lev_RPV (t=159)	0.188
Lev_RPV (t=151)	0.187
T_CoreExit (t=44)	0.184
P_RPV (t=79)	0.184
Lev_RPV (t=46)	0.182
T_CoreExit (t=123)	0.176
P_RPV (t=101)	0.175
T_CoreExit (t=72)	0.174
T_CoreExit (t=63)	0.171
Lev_RPV (t=106)	0.167

Suggested checks: Core exit temp (t46), RPV level(t0)

For SRV failure

Ranked Observ...	Diagnostic Value
Lev_RPV	0.896
P_RPV	0.856
T_CoreExit	0.856
T_CoreExit (t=46)	0.651
P_RPV (t=160)	0.650
T_CoreExit (t=146)	0.615
P_RPV (t=79)	0.485
P_RPV (t=25)	0.464
T_CoreExit (t=72)	0.443
T_CoreExit (t=63)	0.439
Lev_RPV (t=160)	0.433
Lev_RPV (t=61)	0.421
T_CoreExit (t=44)	0.414
P_RPV (t=58)	0.406
Lev_RPV (t=156)	0.406
T_CoreExit (t=123)	0.382
T_CoreExit (t=108)	0.372
Lev_RPV (t=161)	0.364
T_CoreExit (t=98)	0.361
P_RPV (t=128)	0.359
T_CoreExit (t=70)	0.358

Suggested checks: RPV Press(t0), RPV level(t_0)

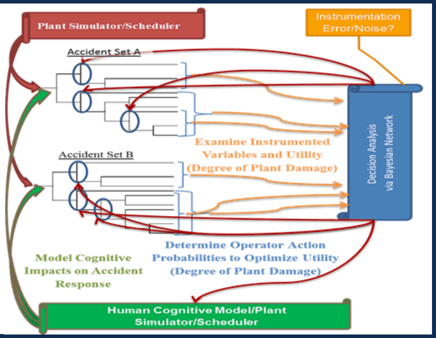
Different tests provide greater diagnostic power for different diseases (and some provide little value for either disease)

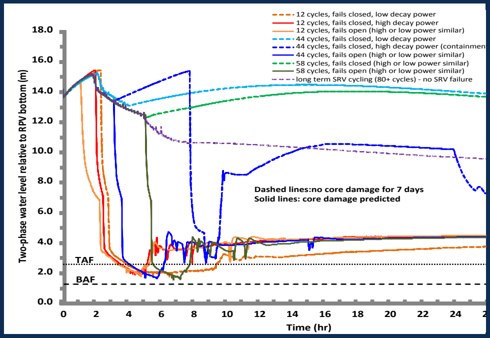
Conclusions

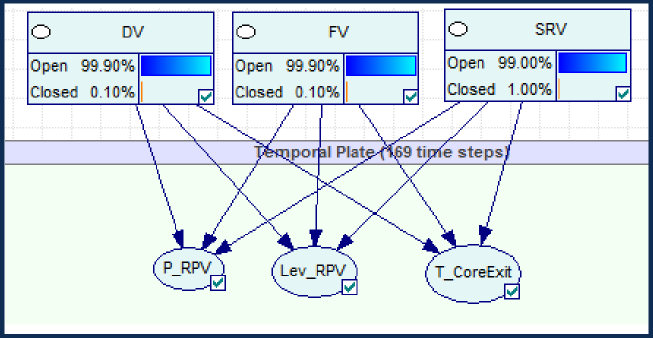
- Fukushima accident drives need for new procedures
- **“Smart SAMGs” – a new paradigm for accident management:**
- Evidence-based, automation-assisted guidance
  - Comprehensive –thousands of scenarios
  - Detailed – Examines accidents that experts may overlook.
  - Defensible – Built on the best knowledge
  - Faster-than-real-time – allows operators to project future states, and predict future impact of various corrective actions.

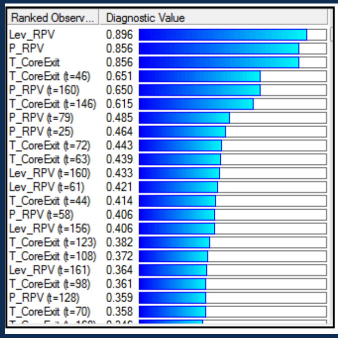
Exceptional service in the national interest

Sandia National Laboratories









Thank you!

Katrina Groth
Risk and Reliability Analysis
Sandia National Laboratories

U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2011-XXXXP

How are IMGs currently created?

- Combination of expert judgments and Best Estimate (BE) simulations
  - Hidden assumption: Active management is almost always safer.
  - Is this true?
- BE vs Risk-Informed
  - Flaw of Averages – Risks are underestimated in BE calculations

$$f(\bar{x}) \neq \int f(x)\, x\, dx\, , unless\ f(x)\ is\ linear$$

  - Severe accidents are not linear.

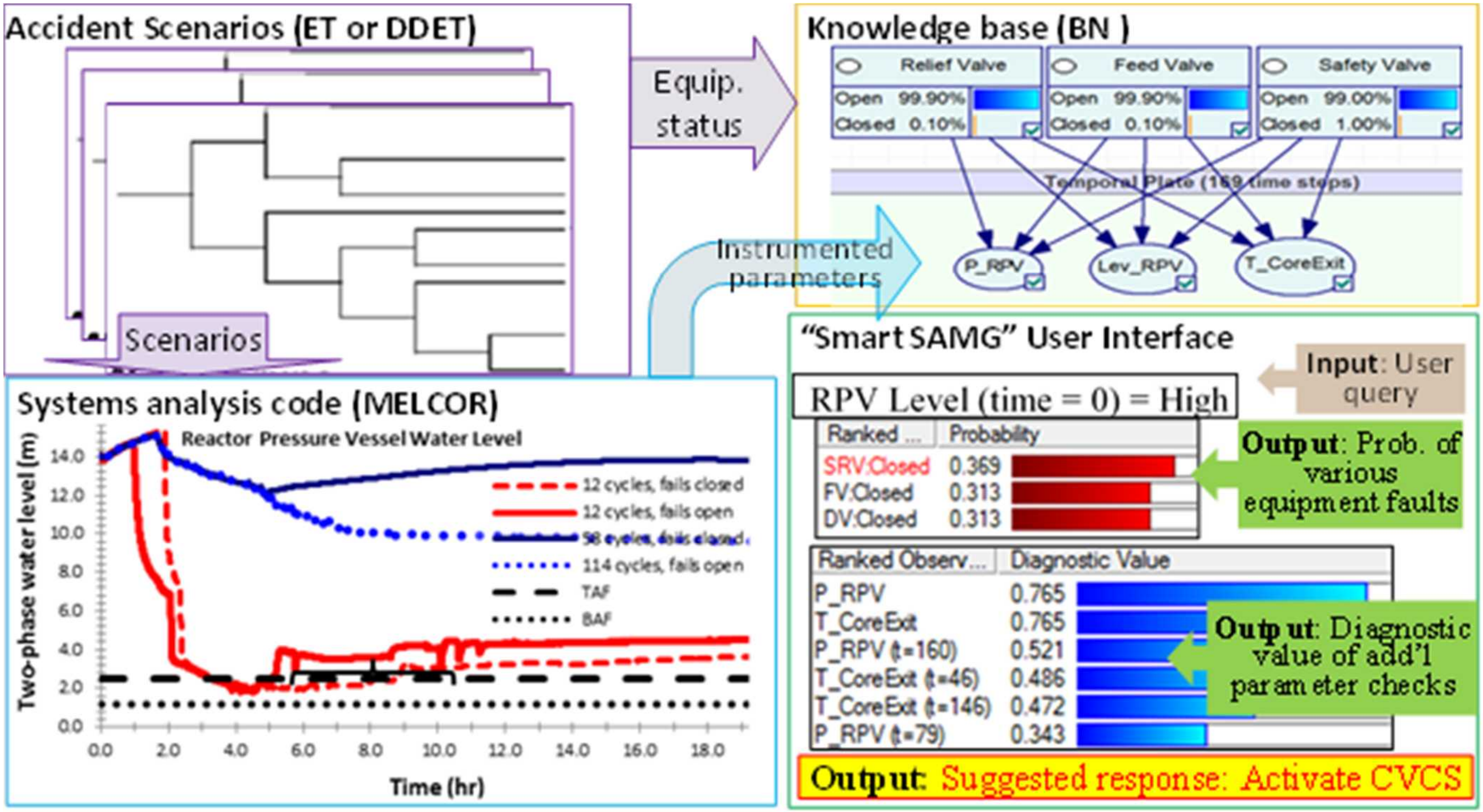
Probability is not really about numbers;

it is about the structure of reasoning.

Glenn Shafer

Rutgers University

Smart SAMGs in a nutshell



References

- Smart Procedures

  - Denman MR, Groth KM & Wheeler, TA (**2013**). "Proof of Principle Framework for risk informed Severe Accident Management Guidelines." *Proceedings of Risk Management for Complex Socio-Technical Systems (RM4CSS) – ANS Winter meeting,* Washington DC.

- DDET safety analyses

  - M Denman, J Cardoni, H Liao, T Wheeler, K Groth & D Zamalieva (**2013**). *Discrete Dynamic Event Tree Capability Study for Advanced Small Modular Reactors-- Proprietary Report*. SAND2013-3352.
  - Denman, MR (**2013**). "Safety Relief Valve Cyclic Failure Analysis for use in Discrete Dynamic Event Trees.." *Proceedings of PSA2013 -- the ANS Topical Meeting on Probabilistic Safety Assessment,* Columbia, SC.
  - Denman, MR, Cardoni, J, Liao, H, Wheeler, T & Groth, KM (**2013**). "Discrete Dynamic Event Tree Analysis of Small Modular Reactor Severe Accident Management." *Proceedings of PSA 2013,* Columbia, SC.
  - Liao, H, Cardoni, JN, Denman, MR, Wheeler, TA (**2013**). "Leveraging existing tools for simulating operator performance in discrete dynamic event trees." *Proceedings of PSA 2013,* Columbia, SC.

- MELCOR: (http://melcor.sandia.gov/)

Theories underlying this work

1. BN-based decision support systems (DSS) can be built to support diagnosis of severe accidents in NPPs.
   - Rationale: Direct analogue to work in other industries
   - Progress: Built proof of concept model to demonstrate this
2. These decision-support systems can also function as surrogate humans (following procedures).
   - Rationale: BNs are an expert system. The whole point of expert systems is to emulate human experts.
   - Future work:– Must implement sampling approaches to tie into ADAPT/IDAC.

Technical methods used to develop Smart SAMGs

- Identification of Accident Scenarios with temporal dependence (Discrete Dynamic Event Trees [DDET])
  - Reduces model simplification by realistically modeling the time-dependent aspects of physical phenomena – unlike traditional risk analysis tools.
  - Accident sequence pathways proceed “naturally” based on the evolution of specific plant conditions rather than a priori developed event trees.
- Accident Simulation (e.g., MELCOR for Nuclear Power Plants)
  - State-of-the-art severe accident physics simulator.
  - Used to model the spectrum of possible plant responses.
- Probabilistic Knowledge Base (Bayesian Networks [BNs])
  - Encodes the DDET and MELCOR results into a probabilistic knowledge-base.
  - Facilitates decision-making with uncertain and limited information.
  - Establishes a relationship between unobservable equipment status with observable plant parameters.