IDEAS
for NextGen PSA Tools

Next Generation PSA Software Workshop

Kenneth L. Kiper
FPL Energy, Seabrook Station

October 2007

Challenges

1. Capability

   How do we handle larger & larger models within a reasonable runtime?

2. Tractability

   How do we ever truly understand & review these expanded PRAs?

3. Connectability

   (If we can get a PC & Mac to talk to each other), why not PRA software codes?

WHY These Challenges

1. Capability

   We are trying to model the reality of nuclear plant risk with increasing detail & accuracy in order to apply risk-informed insights to more challenging problems.

2. Tractability

   The current generation of PRA engineers grew up with the present tools and models - starting with simple tools & simplified models. The next generation PRA engineers will need to understand & own these models without the luxury of the development process that we went through.

3. Connectability

   We ended up with 2 approaches - linked event trees and linked fault trees - which are logically equivalent and both have strengths. Can we connect these two methods and end up with something superior?

The 1st PROBLEM

CAPABILITY

- PRA software needs to handle larger models, expanded in every direction:
  - more initiators to address external hazards and to model internal events with more fidelity;
  - larger fault trees with more basic events to model passive components and instrumentation;
  - more system alignments to model closer to reality;
  - more systems that include normal controls and secondary supports;
  - more operator actions and recovery; and
  - more plant operating states including low power and shutdown.
- Capability includes not only the capacity to model increasing size but also to solve the model within a reasonable time. Several hours to solve the complete model at high fidelity (low truncation) seems to be the acceptable criteria.

Existing Seabrook PRA Model

Integrated All Modes, All IEs, Level 1 & 2 Model:

- Scope: 109 initiators, including all internal & external events (fire, flood, seismic)
- Mode: 32 POSs, including full power, low power, shutdown modes
- Endstate: Level 1 (CDF) and Level 2 (release) bins
- Results: 4 million sequences at 1e-14 sequence truncation in ~5 hrs (7 orders of magnitude below LERF). Lower truncation is possible, it just takes longer.

CAPABILITY is currently available in (at least) one PRA tool.

The 2nd PROBLEM

TRACTABILITY - Three Layers

- Construction: PRA software must be constructed to assist PRA "owners", users, and reviewers to understand of any aspect of the model as well as the model as a whole.
- Modification: The PRA analyst-owner needs to understand the model construction so that modifications can be made to reflect the intended change without some unexpected impact on other parts of the model.
- Review: Somehow the entire model needs to be checked without relying entirely on cutset or sequence reviews – which verify only that a small number of expected sequences are present for the base case model, not that sequences are missing that may be important in some application.

PREMISE #1

The success in CAPABILITY expansion drives the TRACTABILITY crisis.

- As models have grown, they have outgrown the ability of users and reviewers to have a comprehensive understanding of the model as a whole.
- This is a fundamental problem of adequate quality assurance of risk models.

PREMISE #2

Current fault tree and event tree graphical tools have outgrown their usefulness in presenting logic modeling of complex systems / processes.

The IDEA

The IDEA: **Plant Data Tables (PDTs)**

Tables that document the systems relationships the PRA analyst understands - without use of fault trees or event trees.

The analyst builds the model in a series of Plant Data Tables using plant system/component IDs and plan language descriptions of attributes and relations.

The software would convert these tables to a lower level structure of detailed fault trees and event trees (the current software tools) required to model the PRA relationships.

The analyst could review at the lower level (the current world of fault trees and event trees), but most of the input and review would be at this higher level of PDTs.

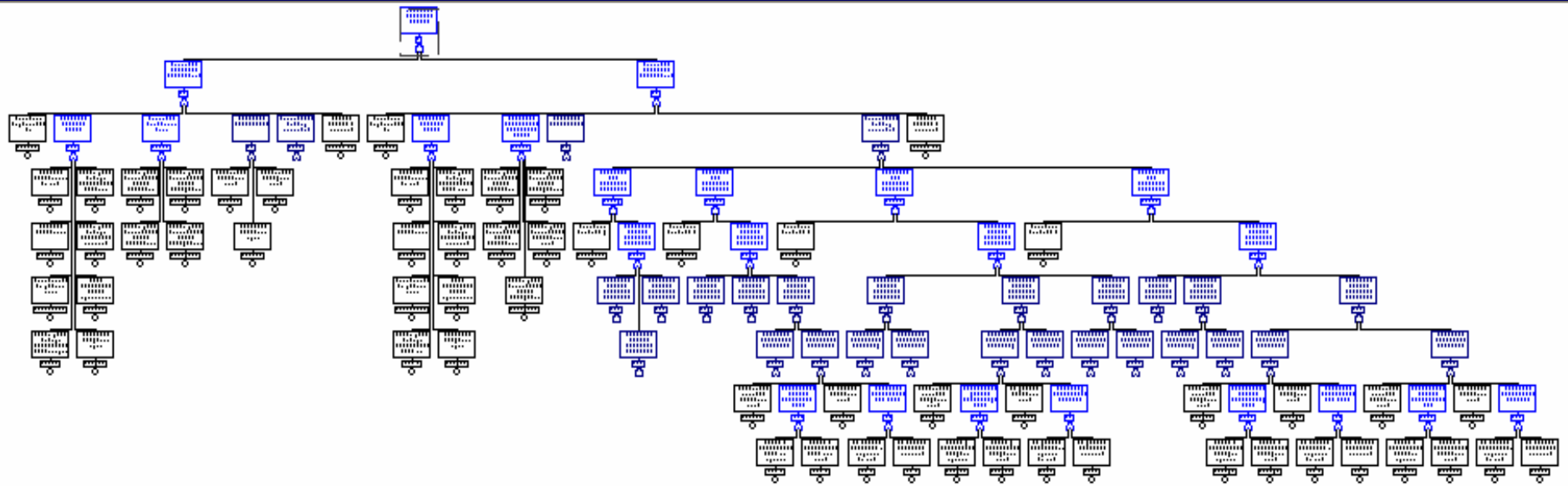
Plant Data Tables & RISK

- RISK → Accident Sequences
  - Combinations of KSF failures → accident end states
    - MELT, Release *(sequence success criteria)*
- KSFs (Key Safety Functions)
  - Combinations of IEs, systems/trains & operator actions *(functional success criteria)*
- Systems
  - Combinations of components under boundary conditions *(system success criteria)*

SYSTEM Plant Data Tables

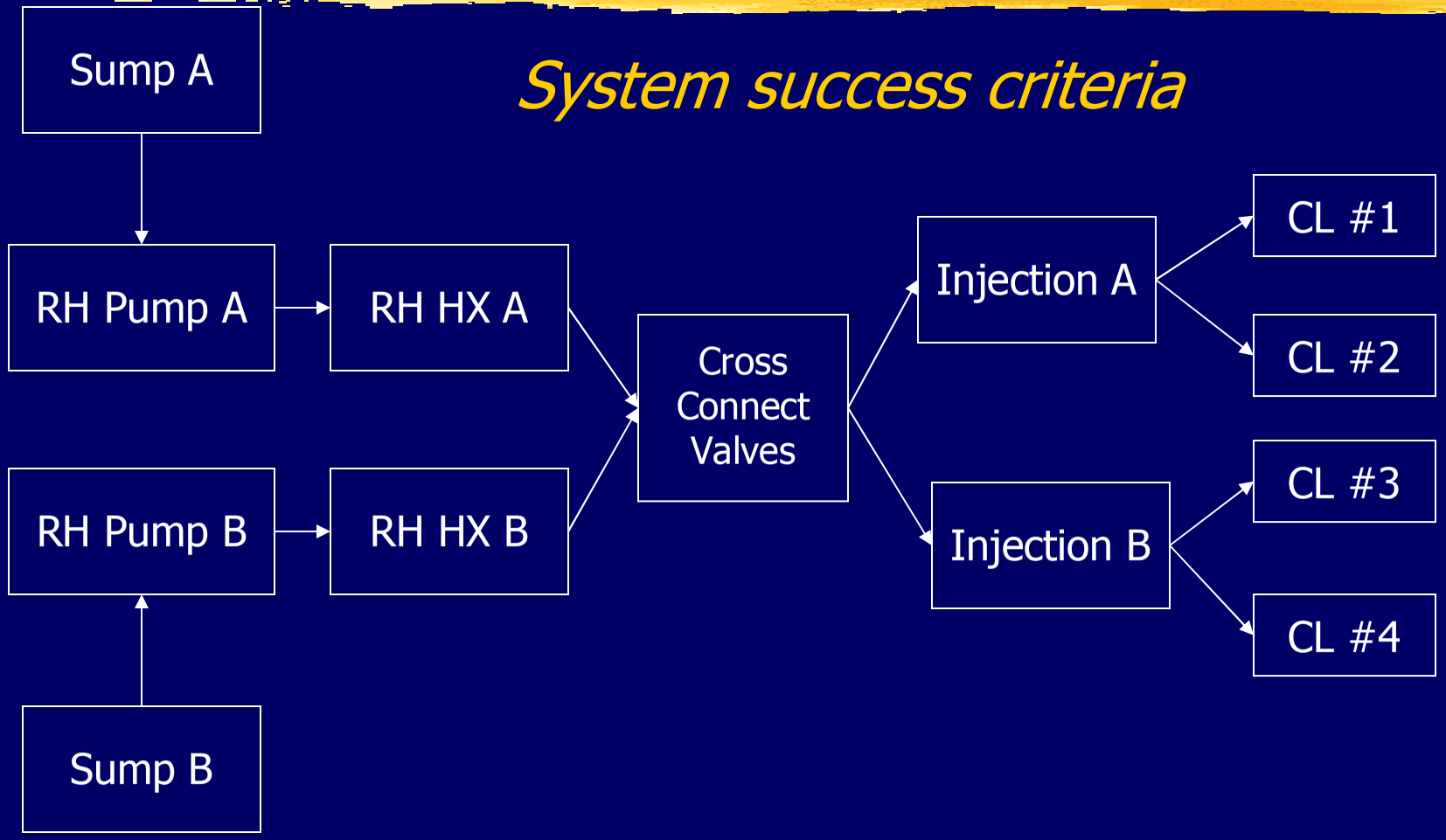
- Key Attributes
  - System boundary & function
  - Components, failure modes (CCF), failure rates, mission time
  - Logic relationship of components to system function
  - System alignments
  - Dependencies (boundary conditions):
    - Support systems
    - Initiating events / sequences

Typical Fault Tree



System *Logic Block Diagram*

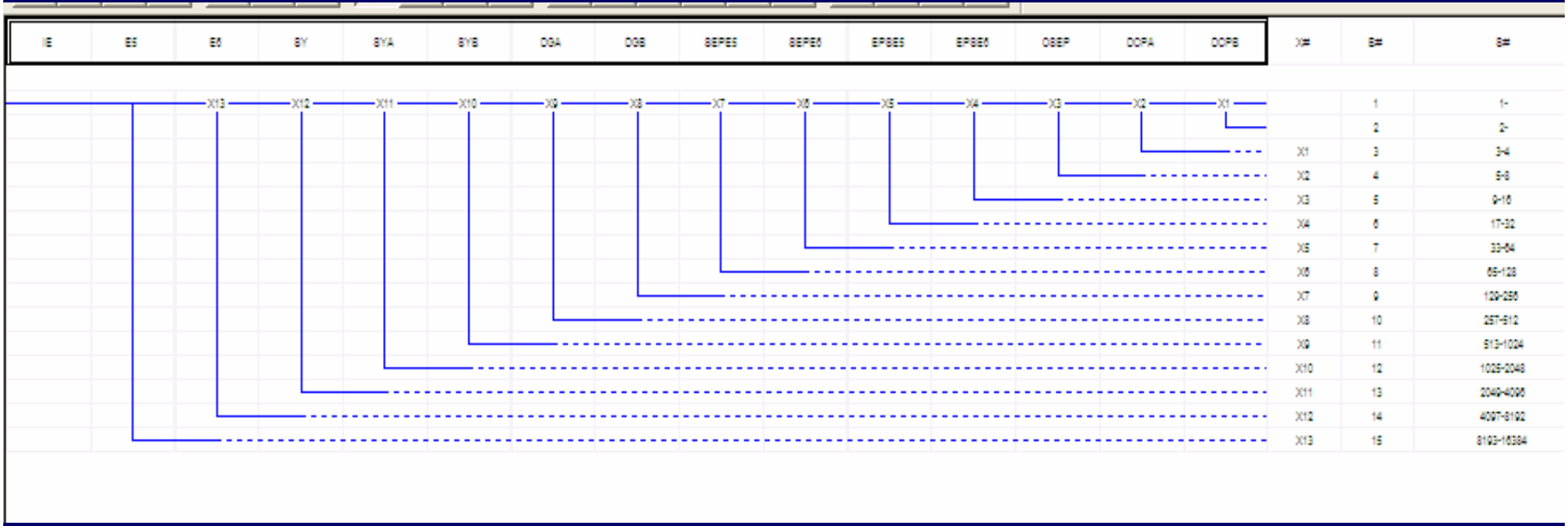
System success criteria



System *Plant Data Table*

System Function	Sub-system Block	Component	Type	Failure Mode (CCF Group)	Mission Time	Alignmt	Dependency (Impact)
LPR Low Pressure ECCS Recirculation	Pump A	RH-P8A	RHR Pump	FR(RHP)	24 hr	--	LPIA (F), BUSE5 (F), PCCA (F)
				OOS	--	MAINTA1	none
		RH-V4	CV	CL	24 hr	--	none
		RH-V9	MOV	CL	24 hr	--	none
		RH-V18	MOV	CL	24 hr	--	none
	Sump A	CBS-V8	MOV1	FTO(RHV)	--	--	BUSE51 (F)
				OOS	--	MAINTA2	none
	RH HX A	RH-E9A	HX	RT	24 hr	--	PCCA (F)
		RH-FCV-618	AOV	OP	24 hr + RF/2	--	none
		CC-V131	MV	CL	24 hr	--	none
		CC-V145	MOV	CL	24 hr		none
	Cross-connnect Valves	RH-V21	MOV	CL	24 hr	--	none
		RH-V22	MOV	CL	24 hr	--	none
		RH-V33	MOV	OP	24 hr	--	none
	Injection Line A	RH-V14	MOV	CL	24 hr	--	none
	Injection Line B	RH-V26	MOV	CL	24 hr	--	none
	CL1	RC-CL1	Pipe	RT	--		LOCA-CL1 (F)
		RH-V15	CV1	FTO	--	--	none
				CL	24 hr	--	none
		RH-V59	MOV	CL	24 hr	--	none
		SI-V5	CV1	FC	24 hr	--	none
				CL	24 hr	--	none

“Branch-Everywhere” Event Tree



Event Tree Rule Logic

Split Fraction	Split Fraction Rule	Comment
DGAF	E5=F + SYA=F * (INIT=LSWSA + INIT=LSWSA4 + INIT=LDCPA)	DGA - Guaranteed failure due to initiator, either loss of Bus E5 -or- loss of offsite power and SW Train A. Without SW cooling to the DG, the DG is assumed to fail.
DGAF	QDG=F + QDGR=F	DGA - EDG fails due to seismic hardware impact or seismic relay chatter (recovery of relay chatter in TRANS tree, split fraction RDGL1Q).
DGAF	SYA=F * INIT=FETASW + INIT=FCRAC * OFCR=F	DGA - Guaranteed failure due to fire. Note, FCRAC recovery given a seal leak is modeled in OFCRL & RDGL.
DGA2	INIT=LOSPW + INIT=LOSPW4 + INIT=LOSPF + INIT=LOSPF4 + SEIS123 + FIRE123 + FLOOD123	DGA - EDG fails to start & run for 24 hrs, given offsite power failed (weather-related event, or other events with longer expected time to recovery).
DGA1	1	DGA - EDG fails to start & run for 6 hrs, given plant-related or grid-related loss of offsite power (non-weather-related).
DGBN	SYB=S	DGB - EMERGENCY DIESEL GENERATOR TRAIN B. Not needed with offsite power available.
DGBF	E6=F + SYB=F * (INIT=LSWSB + INIT=LSWSB4 + INIT=LDCPB)	DGB - Guaranteed failure due to initiator, either loss of Bus E5 -or- loss of offsite power and SW Train A. Without SW cooling to the DG, the DG is assumed to fail.
DGBF	QDG=F + QDGR=F	DGB - EDG fails due to seismic hardware impact or seismic relay chatter (recovery of relay chatter in TRANS tree, split fraction RDGL1Q).
DGBF	SYB=F * INIT=FETBSW + INIT=FCRAC * OFCR=F	DGB - Guaranteed failure due to fire. Note, FCRAC recovery given a seal leak is modeled in OFCRL & RDGL.
DGBF2	(INIT=LOSPW + INIT=LOSPW4 + INIT=LOSPF + INIT=LOSPF4 + SEIS123 + FIRE123 + FLOOD123) * DGA=F	DGB - 24 hr mission time, given DG train A failure.
DGBS2	(INIT=LOSPW + INIT=LOSPW4 + INIT=LOSPF + INIT=LOSPF4 + SEIS123 + FIRE123 + FLOOD123) * DGA=S	DGB - 24 hr mission time, given DG train A successful.

LOCA End State Logic

Split Fraction	Split Fraction Rule	Comment
STABLE	LOCA123MD * INV_HPI * DHR_HPR	Stable STATE S5a: Medium LOCA with successful HP injection -AND- HP recirculation.
STABLE	LOCA123MD * INV_HPI * ODEP=S * DHR_LPR	Stable STATE S5b: Medium LOCA with successful HP injection -AND- depressurization -AND- LP recirculation.
STABLE	LOCA123LG * INV_ACCUM * INV_LPI * DHR_LPR * DHR_HLR	Stable STATE S5c: Large LOCA with successful LP injection -AND- LP recirculation -AND- hot leg recirculation.
CDFML1	LOCA123MD * -INV_HPI	Failed STATE ML1: Medium LOCA initiator with failure of primary inventory makeup.
CDFML2	LOCA123MD * INV_HPI * -DHR_HPR * (ODEP=F + -DHR_LPR)	Failed STATE ML2: Medium LOCA initiator with successful makeup but failure of sump recirculation (either high pressure recirc or low pressure recirc).
CDFLL1	LOCA123LG * (-INV_ACCUM + -INV_LPI)	Failed STATE LL1: Large LOCA initiator with failure of primary inventory makeup (failure of accumulators or failure of RHR injection).
CDFLL2	LOCA123LG * INV_ACCUM * INV_LPI * -DHR_LPR	Failed STATE LL2: Large LOCA initiator with successful makeup but failure of sump recirculation.
CDFLL3	LOCA123LG * INV_ACCUM * INV_LPI * DHR_LPR * -DHR_HLR	Failed STATE LL3: Large LOCA initiator with successful makeup and sump recirculation but failure of long term hot-leg recirculation.
CDFLL4	LOCA123EX	Failed STATE LL4: Excess LOCA initiator. This is assumed to be a LOCA larger than the ECCS can mitigate.

KSF Definitions (Macros)

Macro	Macro Rule	Comment
DHR_HLR	OHLR=S * (HLRA=S + HLRB=S)	INVENTORY & DHR: Low pressure, hot leg sump recirculation. This is required only for LLOCA in the long term.
DHR_HPR	OHPR=S * HPR=S * (LPRA=S + LPRB=S)	INVENTORY & DHR: High pressure sump recirculation.
DHR_LPR	OLPR=S * (LPRA=S + LPRB=S)	INVENTORY & DHR: Low pressure sump recirculation.
DHR_SG	EFWM=S + EFWT=S + SUFP=S	DHR: Successful decay heat removal via SGs with makeup from EFW or SUFP.
EXCESS_LOCA	LOCA123EX	CET STATUS: Excessive LOCA.
INV_ACCUM	ACCUM=S	INVENTORY: Low pressure injection via accumulators.
INV_HPI	CSA=S + CSB=S + SIA=S + SIB=S	INVENTORY: High pressure injection for small & medium LOCA.
INV_LPI	LPIA=S + LPIB=S	INVENTORY: Low pressure injection via RHR.

Conclusion

PREMISE #1. The success in CAPABILITY expansion drives the TRACTABILITY crisis.

PREMISE #2. Current fault tree and event tree graphical tools have outgrown their usefulness in presenting logic modeling of complex systems / processes.

CHALLENGE. The next generation PRA software MUST provide the next generation analyst with tools to provide assurance that the complex modeling is accurate.