PRA Methodology Overview

22.39 Elements of Reactor Design, Operations, and Safety

Lecture 9

Fall 2006

George E. Apostolakis
Massachusetts Institute of Technology

PRA Synopsis

Figure removed due to copyright restrictions.
Futron Corp., International Space Station PRA, Dec. 2000

NPP End States

- Various states of degradation of the reactor core.
- Release of radioactivity from the containment.
- Individual risk.
- Numbers of early and latent deaths.
- Number of injuries.
- Land contamination.

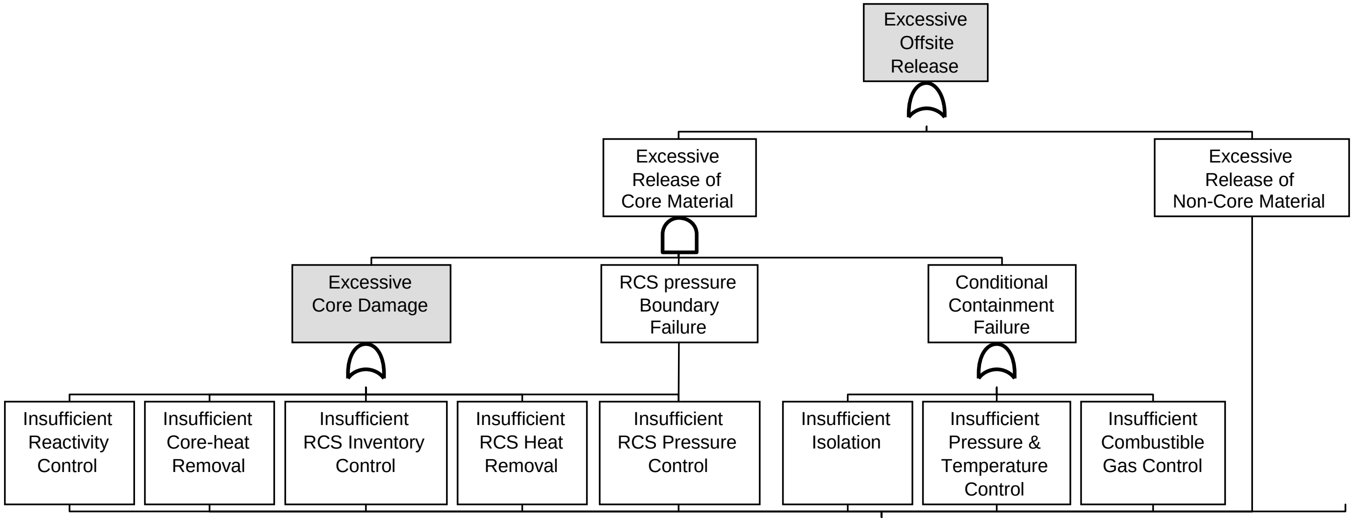
The Master Logic Diagram (MLD)

- **Developed to identify Initiating Events in a PRA.**
- **Hierarchical depiction of ways in which system perturbations can occur.**
- **Good check for completeness.**

MLD Development

- **Begin with a top event that is an end state.**
- **The top levels are typically functional.**
- **Develop into lower levels of subsystem and component failures.**
- **Stop when every level below the stopping level has the same consequence as the level above it.**

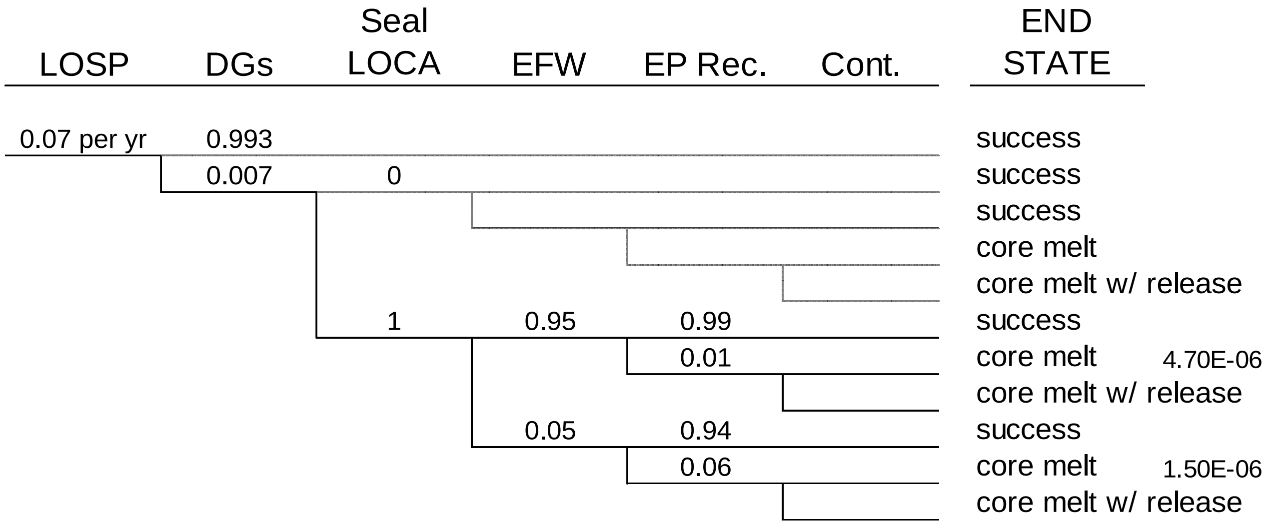
Nuclear Power Plant MLD



NPP: Initiating Events

- Transients
  - Loss of offsite power
  - Turbine trip
  - Others
- Loss-of-coolant accidents (LOCAs)
  - Small LOCA
  - Medium LOCA
  - Large LOCA

ILLUSTRATION EVENT TREE: Station Blackout Sequences



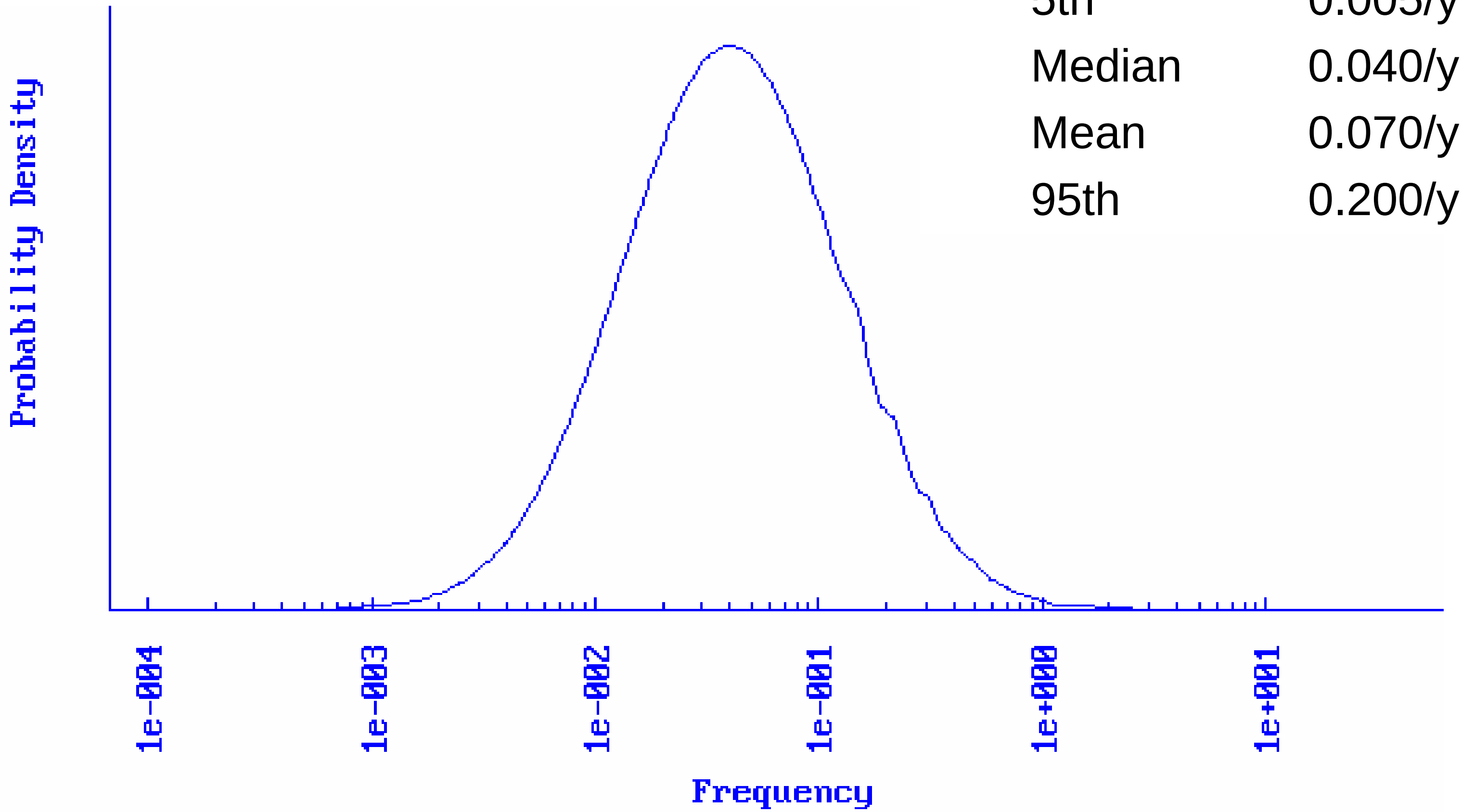
LOSP | DGs | Seal LOCA | EFW | EP Rec. | Cont. | END STATE

0.07 per yr
0.993 — success
0.007
0 — success
success
core melt
core melt w/ release
1
0.95
0.99 — success
0.01 — core melt 4.70E-06
core melt w/ release
0.05
0.94 — success
0.06 — core melt 1.50E-06
core melt w/ release

From: K. Kiper, MIT Lecture, 2006

Courtesy of K. Kiper. Used with permission.

LOSP Distribution

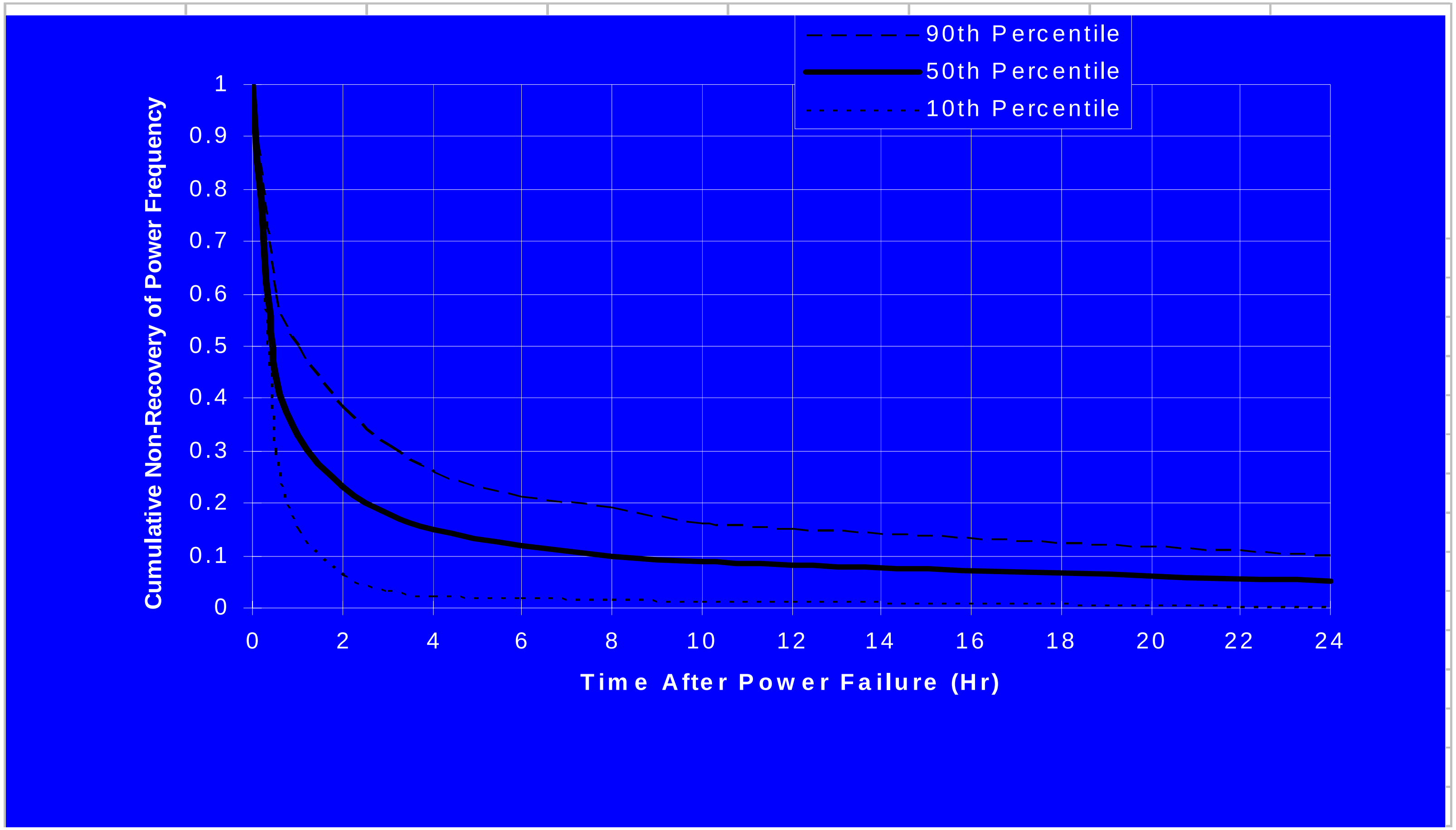


Epistemic Uncertainties		
5th	0.005/yr	(200 yr)
Median	0.040/yr	(25 yr)
Mean	0.070/yr	(14 yr)
95th	0.200/yr	(5 yr)

From: K. Kiper, MIT Lecture, 2006

Courtesy of K. Kiper. Used with permission.

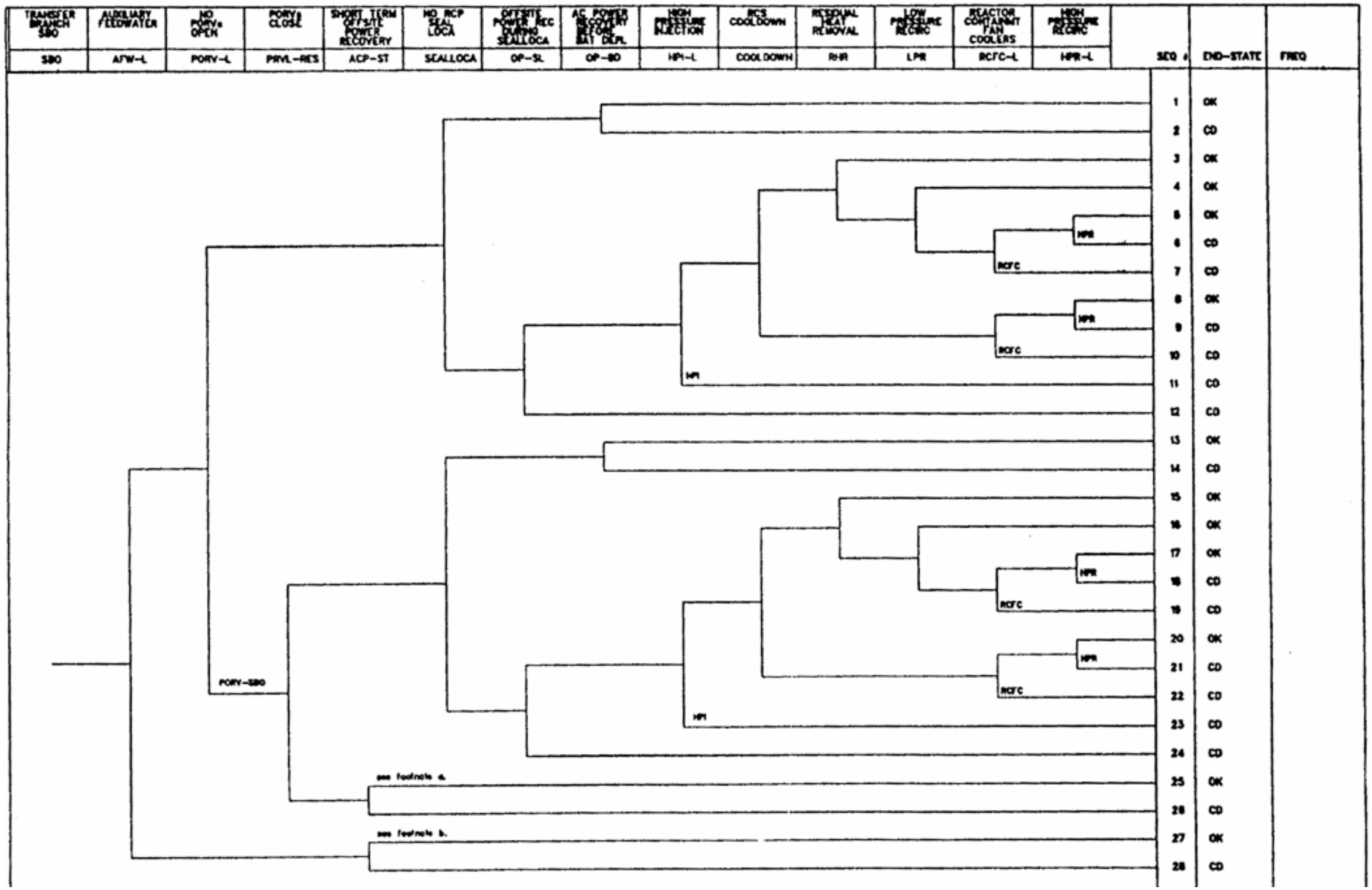
Offsite Power Recovery Curves



From: K. Kiper, MIT Lecture, 2006

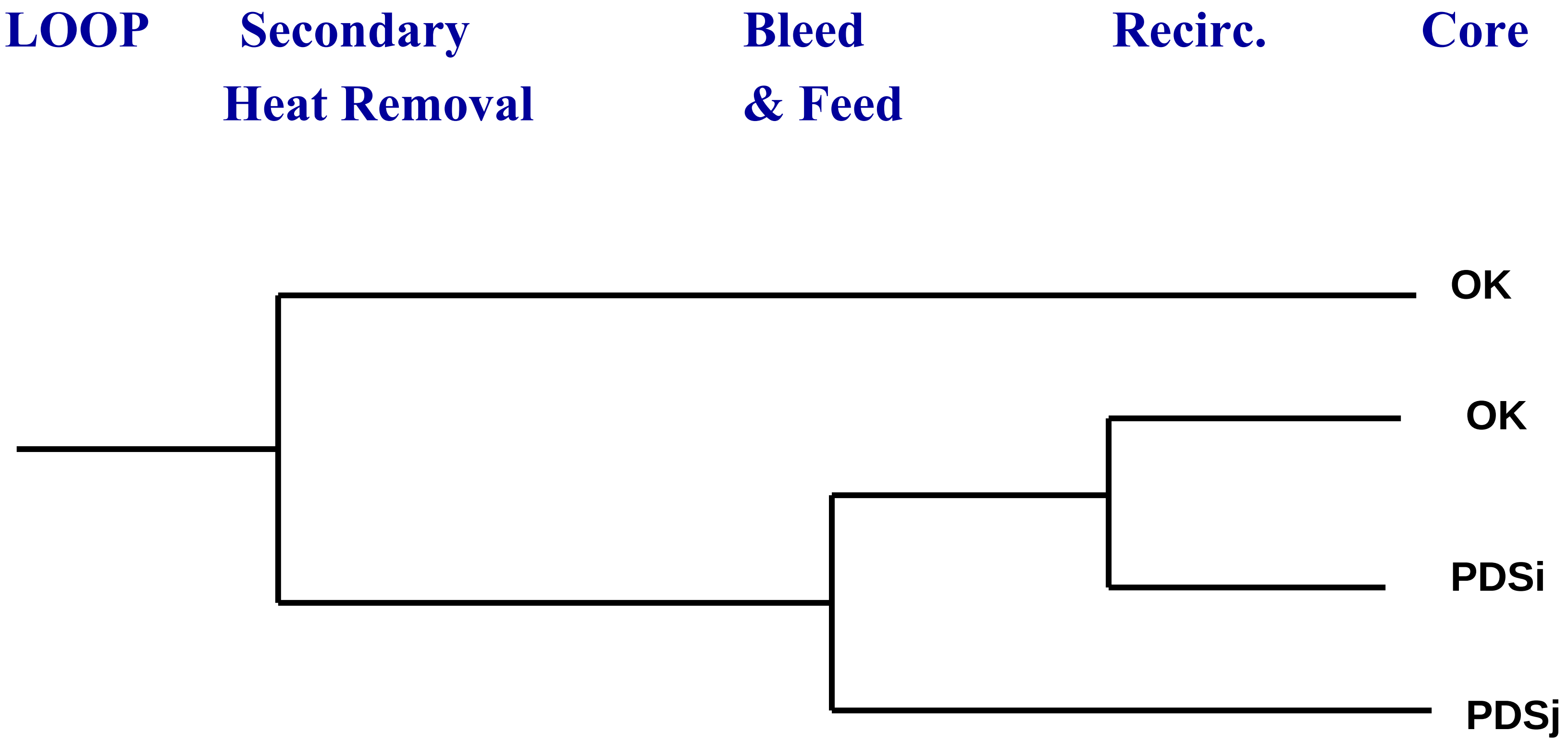
Courtesy of K. Kiper. Used with permission.

STATION BLACKOUT EVENT TREE



Courtesy of U.S. NRC.

NPP: Loss-of-offsite-power event tree



LOOP

Secondary Heat Removal

Bleed & Feed

Recirc.

Core

OK

OK

PDSi

PDSj

Human Performance

- **The operators must decide to perform feed & bleed.**
- **Water is "fed" into the reactor vessel by the high-pressure system and is "bled" out through relief valves into the containment. Very costly to clean up.**
- **Must be initiated within about 30 minutes of losing secondary cooling (a thermal-hydraulic calculation).**

J. Rasmussen’s Categories of Behavior

- *Skill-based behavior:* Performance during acts that, after a statement of intention, take place without conscious control as smooth, automated, and highly integrated patterns of behavior.
- *Rule-based behavior:* Performance is consciously controlled by a stored rule or procedure.
- *Knowledge-based behavior:* Performance during unfamiliar situations for which no rules for control are available.

Reason's Categories

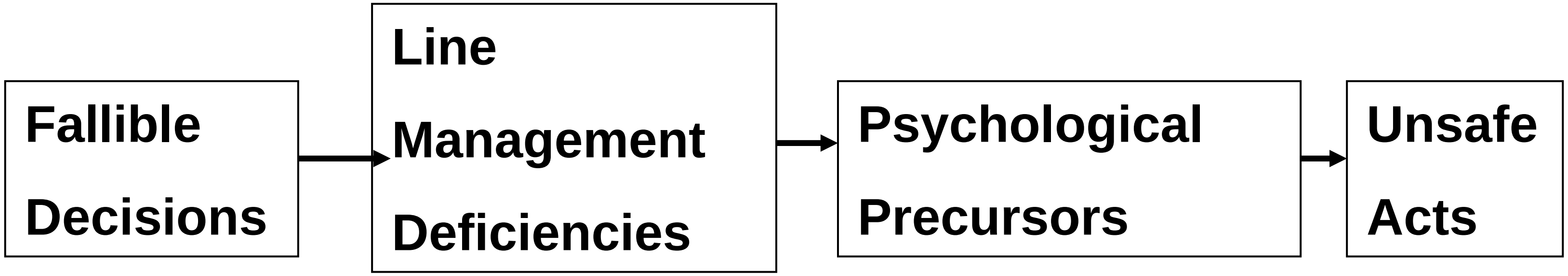
Unsafe acts

- Unintended action
  - Slip
  - Lapse
  - Mistake
- Intended violation

Latent conditions

- **Weaknesses that exist within a system that create *contexts* for human error beyond the scope of individual psychology.**
- **They have been found to be significant contributors to incidents.**
- **Incidents are usually a combination of hardware failures and human errors (latent and active).**

Reason's model



Line Management Deficiencies

Fallible Decisions

Psychological Precursors

Unsafe Acts

J. Reason, *Human Error*, Cambridge University Press, 1990

Pre-IE ("routine") actions

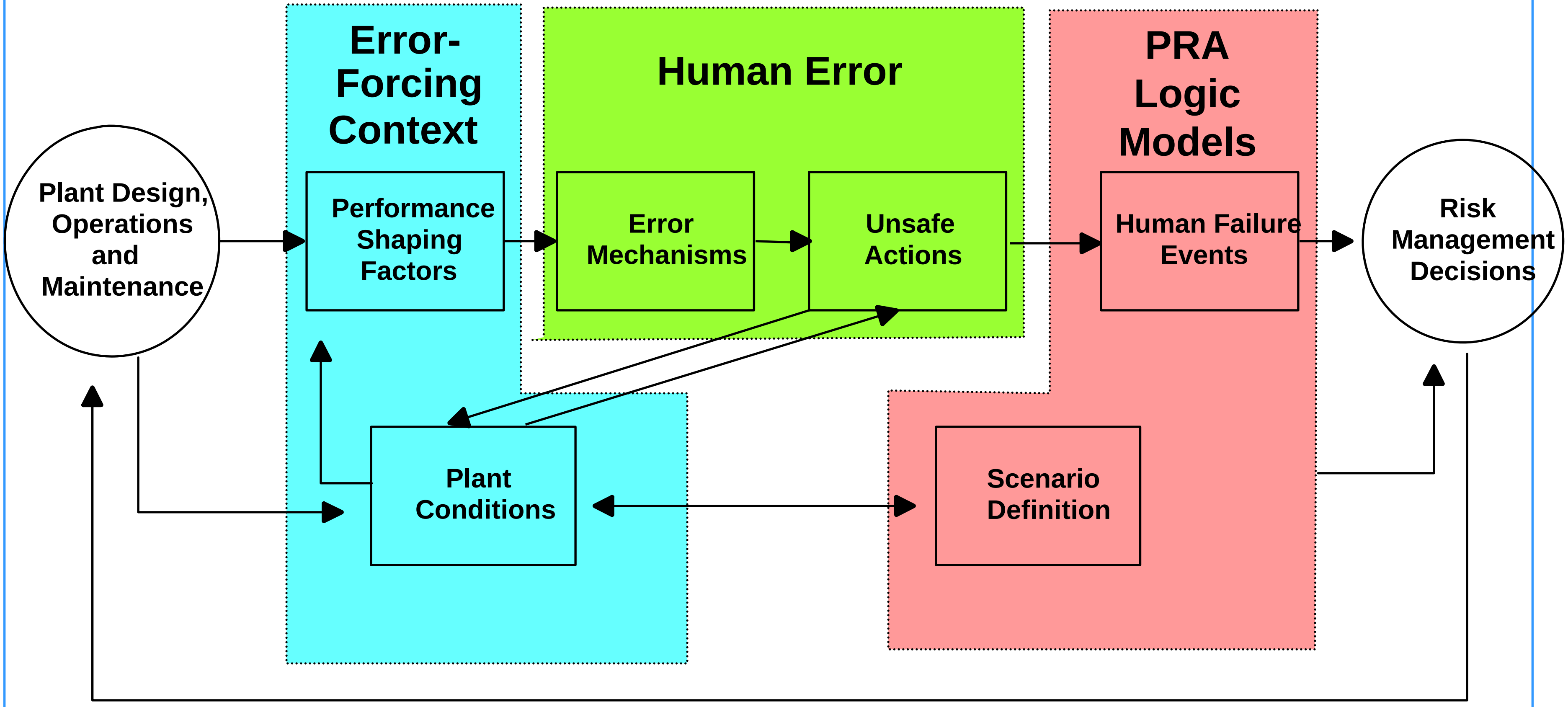
	Median	EF
Errors of commission	3×10^{-3}	3
Errors of omission	10^{-3}	5

A.D. Swain and H.E. Guttmann, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*, Report NUREG/CR-1278, US Nuclear Regulatory Commission, 1983.

Post-IE errors

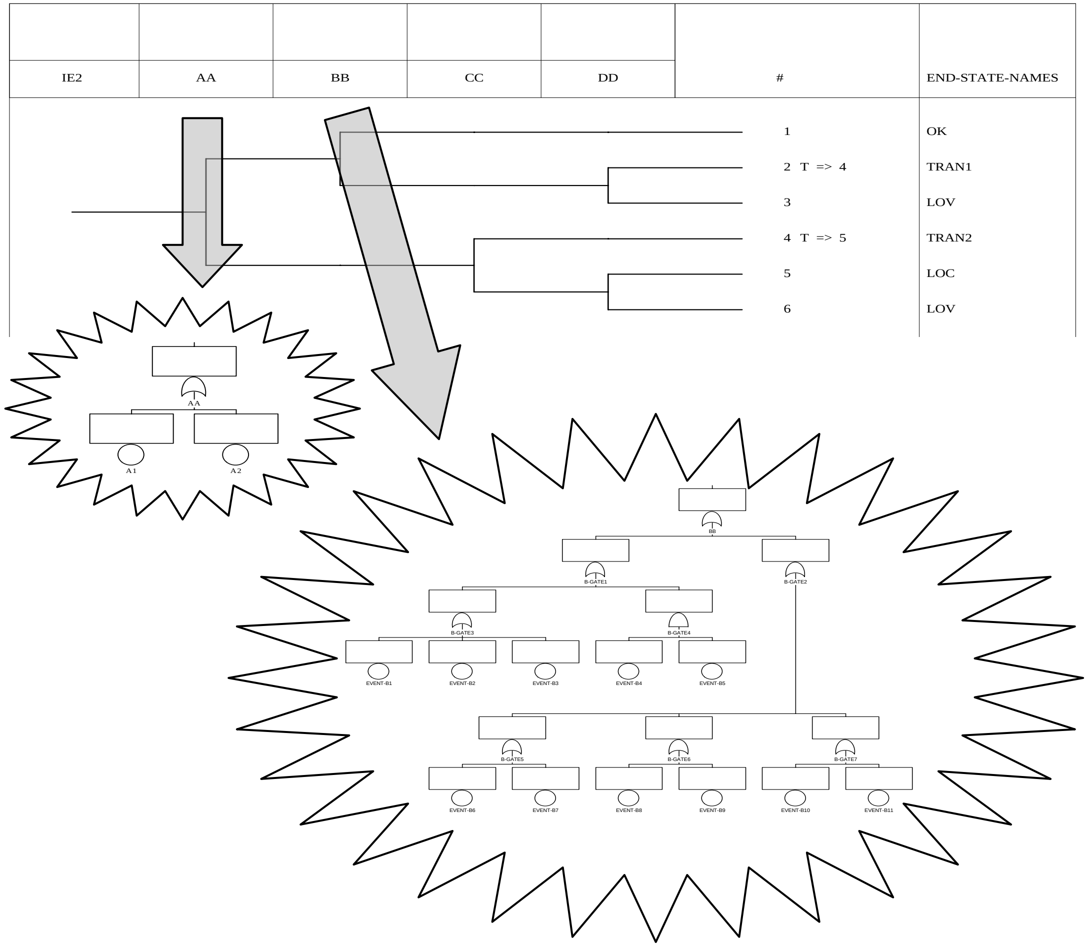
- Models still being developed.
- Typically, they include detailed task analyses, identification of performance shaping factors (PSFs), and the subjective assessment of probabilities.
- PSFs: System design, facility culture, organizational factors, stress level, others.

The ATHEANA Framework

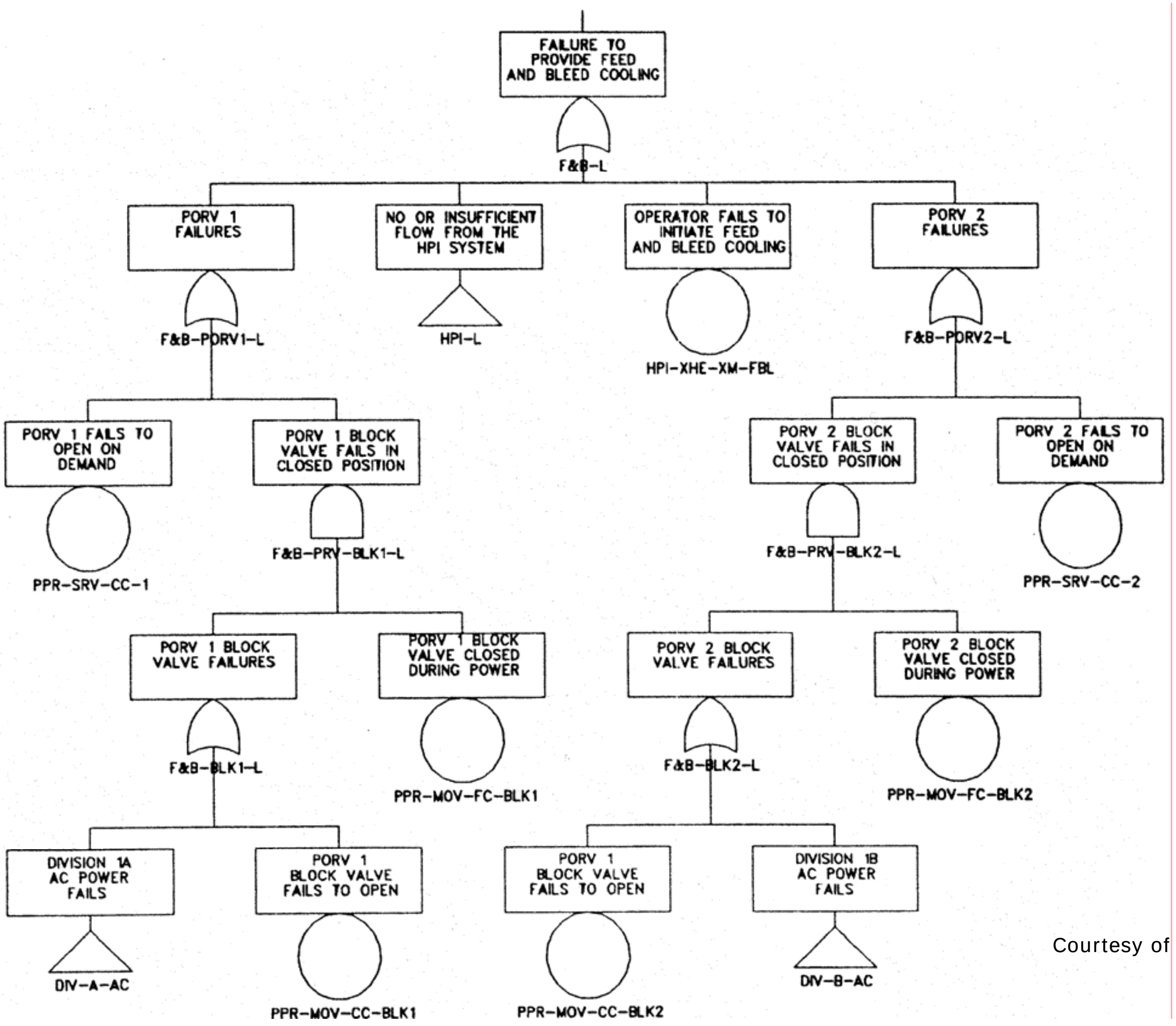


NUREG/CR-6350, May 1996.

Risk Models

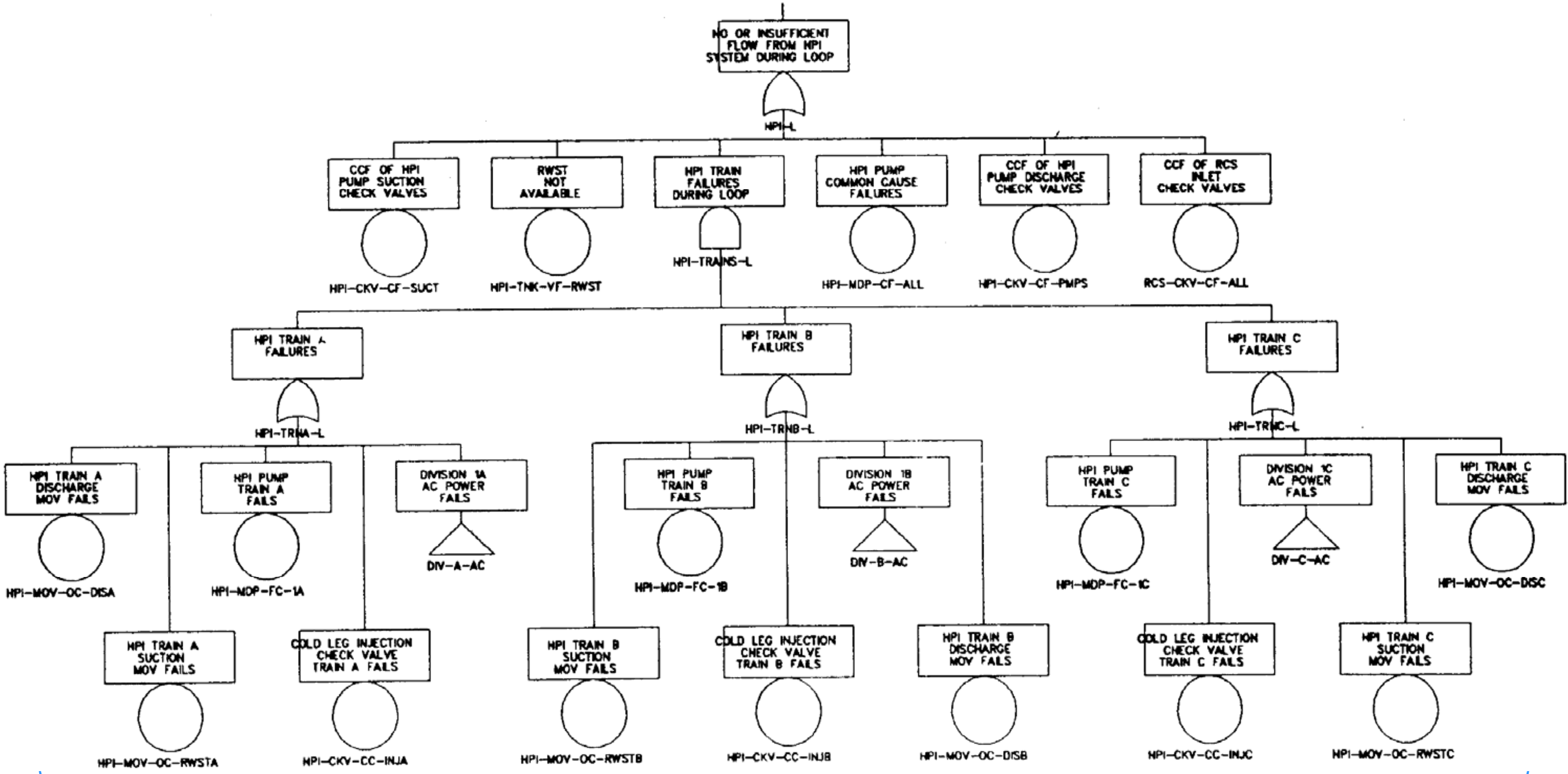

IE2
AA
BB
CC
DD
#
END-STATE-NAMES
1
OK
2 T => 4
TRAN1
3
LOV
4 T => 5
TRAN2
5
LOC
6
LOV
AA
A1
A2
BB
B-GATE1
B-GATE2
B-GATE3
B-GATE4
EVENT-B1
EVENT-B2
EVENT-B3
EVENT-B4
EVENT-B5
B-GATE5
B-GATE6
B-GATE7
EVENT-B6
EVENT-B7
EVENT-B8
EVENT-B9
EVENT-B10
EVENT-B11

FEED & BLEED COOLING DURING LOOP 1-OF-3 SI TRAINS AND 2-OF-2 PORVS FOR SUCCESS



Courtesy of U.S. NRC.

HIGH PRESSURE INJECTION DURING LOOP 1-0F-3 TRAINS FOR SUCCESS



Courtesy of U.S. NRC.

Cut sets and minimal cut sets

- ***CUT SET*:** **Any set of events (failures of components and human actions) that cause system failure.**

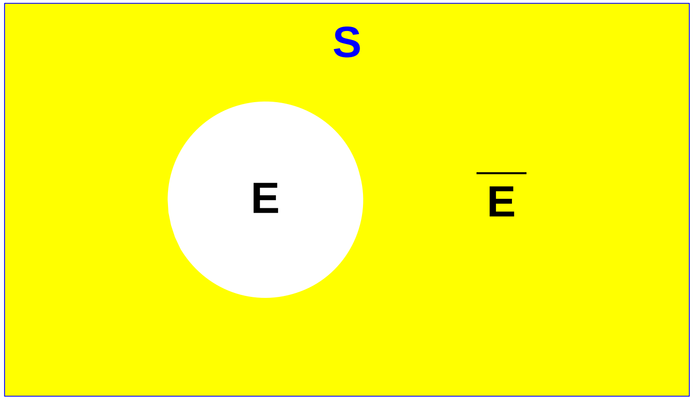
- ***MINIMAL CUT SET*:** **A cut set that does not contain another cut set as a subset.**

Indicator Variables

$$X_j = \begin{cases} 1, \text{ If } E_j \text{ is T} \\ 0, \text{ If } E_j \text{ is F} \end{cases}$$

Important Note: **$X^k = X$, k: 1, 2, …**

Venn Diagram



$$X_T = \phi(X_1, X_2, \ldots X_n) \equiv \phi(\underline{X})$$

$\phi(\underline{X})$ is the structure or switching function.

It maps an n-dimensional vector of 0s and 1s onto 0 or 1.

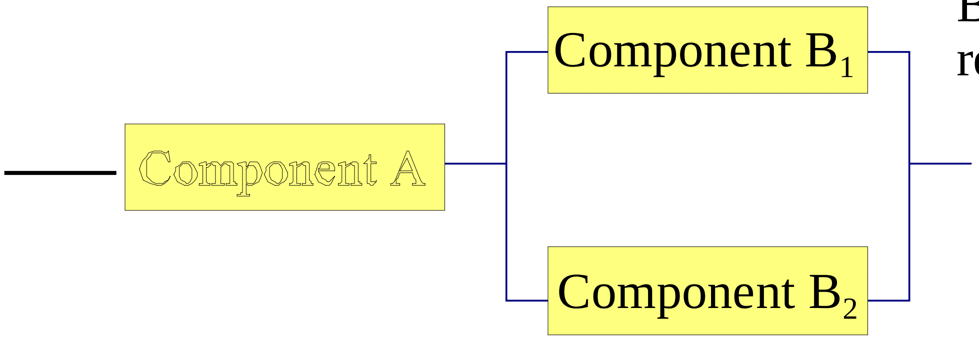
Disjunctive Normal Form:

$$\mathbf{X}_{\mathbf{T}} = 1 - \prod_{1}^{\mathbf{N}} (1 - \mathbf{M}_{\mathbf{i}}) \equiv \coprod_{1}^{\mathbf{N}} \mathbf{M}_{\mathbf{i}}$$

Sum-of-Products Form:

$$X_T = \sum_{i=1}^{N} M_i - \sum_{i=1}^{N-1} \sum_{j=i+1}^{N} M_i M_j + \ldots + (-1)^{N+1} \prod_{i=1}^{N} M_i$$

Dependent Failures: An Example



B_1 and B_2 are identical redundant components

MCS: $M_1 = \{X_A\}$ $M2 = \{X_{B1}, X_{B2}\}$

System Logic	$X_S = 1 - (1 - X_A)(1 - X_{B1}X_{B2}) =$ $= X_A + X_{B1}X_{B2} - X_A X_{B1} X_{B2}$
Failure Probability	$P(\text{fail}) = P(X_A) + P(X_{B1} X_{B2}) - P(X_A X_{B1} X_{B2})$

Example (cont'd)

- In general, we cannot assume independent failures of B_1 and B_2. This means that

$$P(X_{B1}\,X_{B2}) \geq P(X_{B1})\,P(X_{B2})$$

- How do we evaluate these dependencies?

Dependencies

- **Some dependencies are modeled explicitly, e.g., fires, missiles, earthquakes.**
- **After the explicit modeling, there is a class of causes of failure that are treated as a group. They are called *common-cause failures.***

Special Issue on Dependent Failure Analysis, *Reliability Engineering and System Safety,* vol. 34, no. 3, 1991.

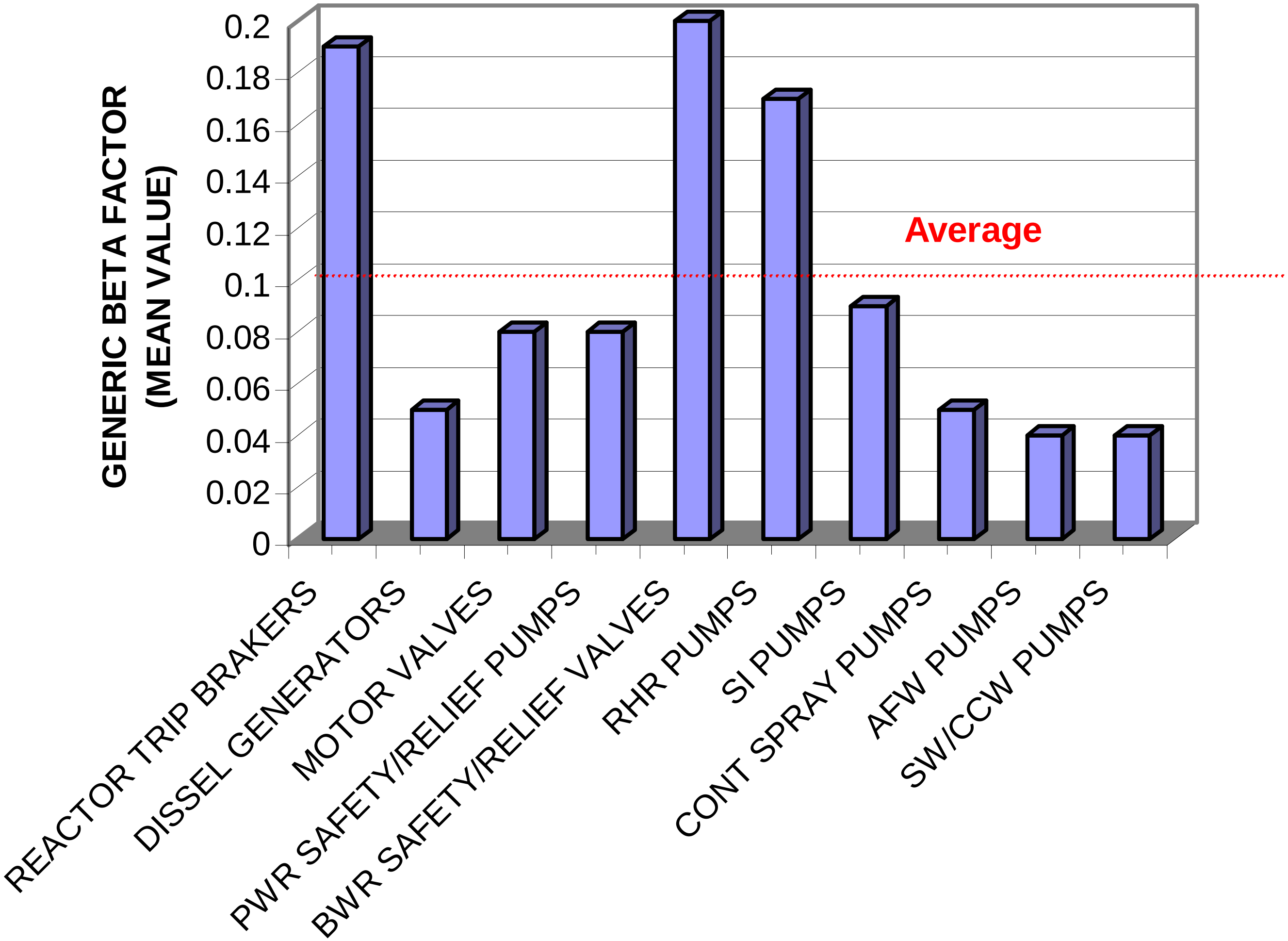
The Beta-Factor Model

- The β-factor model assumes that common-cause events always involve failure of all components of a common cause component group

- It further assumes that

$$\beta = \frac{\lambda_{\mathrm{CCF}}}{\lambda_{\mathrm{total}}}$$

Generic Beta Factors



Data Analysis

- **The process of collecting and analyzing information in order to estimate the parameters of the epistemic PRA models.**

- **Typical quantities of interest are:**
  - **Initiating Event Frequencies**
  - **Component Failure Frequencies**
  - **Component Test and Maintenance Unavailability**
  - **Common-Cause Failure Probabilities**
  - **Human Error Rates**

General Formulation

$$X_T = \varphi(X_1,\ldots X_n) \equiv \varphi(\underline{X})$$

$$\mathbf{X_T = 1 - \prod_{1}^{N} (1 - M_i) \equiv \coprod_{1}^{N} M_i}$$

$$X_T = \sum_{i=1}^{N} M_i - \sum_{i=1}^{N-1} \sum_{j=i+1}^{N} M_i M_j + \ldots + (-1)^{N+1} \prod_{i=1}^{N} M_i$$

X_T : the TOP event indicator variable (e.g., core melt, system failure)

M_i : the ith minimal cut set (for systems) or accident sequence (for core melt, containment failure, et al)

TOP-event Probability

$$P(X_T) = \sum_1^N P(M_i) + \ldots + (-1)^{N+1} P\left(\prod_1^N M_i\right)$$

$$P(X_T) \cong \sum_1^N P(M_i)$$

Rare-event approximation

The question is how to calculate the probability of M_i

$$P(M_i) = P(X_k^i \ldots X_m^i)$$

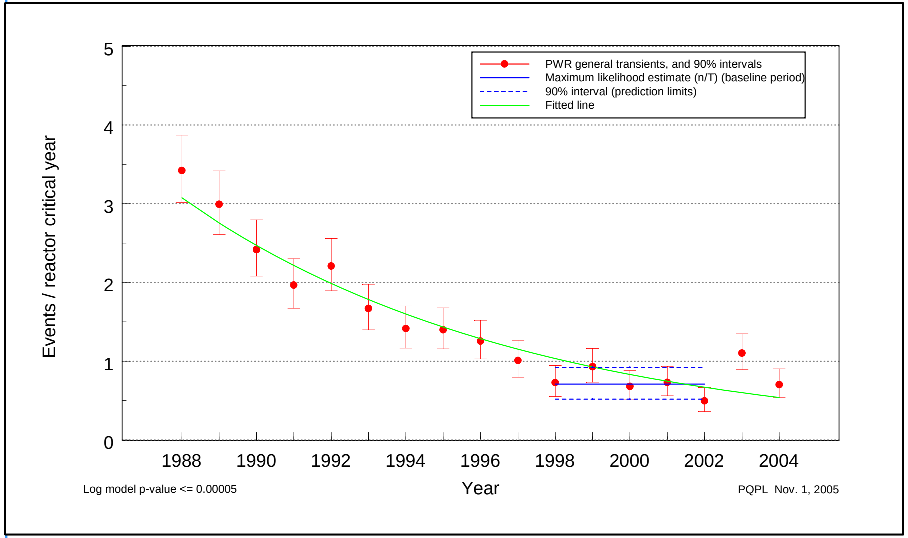
RISK-SIGNIFICANT INITIATING EVENTS

Risk-Significant Initiating Event	Period	Number of Events	Mean Frequency	Trend
General Transients	1998 – 2004	2120	7.57E-1	⬇
BWR General Transients	1997 – 2004	699	8.56E-1	⬇
PWR General Transients	1998 – 2004	1421	7.10E-1	⬇
Loss of Feedwater	1993 – 2004	188	9.32E-2	⬇
Loss of Heat Sink	1995 – 2004	259	1.24E-1	⬇
BWR Loss of Heat Sink	1996 – 2004	154	1.88E-1	⬇
PWR Loss of Heat Sink	1991 – 2004	105	9.23E-2	⬇
Loss of Instrument Air (BWR)	1994 – 2004	19	7.60E-3	⬇
Loss of Instrument Air (PWR)	1990 – 2004	17	1.19E-2	⬇
Loss of Vital AC Bus	1988 – 2004	43	2.98E-2	⬌
Loss of Vital DC Bus	1988 – 2004	3	2.35E-3	⬌
Stuck Open SRV (BWR)	1993 – 2004	14	2.07E-2	⬌
Stuck Open SRV (PWR)	1988 – 2004	2	2.30E-3	⬌
Steam Generator Tube Rupture	1988 – 2004	3	3.48E-3	⬌
Very Small LOCA	1988 – 2004	5	3.92E-3	⬌

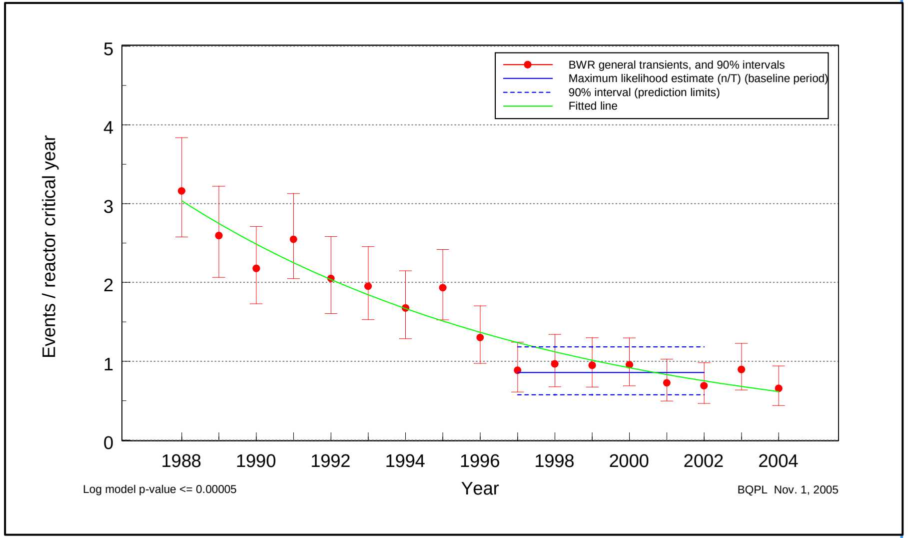
Courtesy of P. Baranowsky. Used with permission.

INITIATING EVENT TRENDS

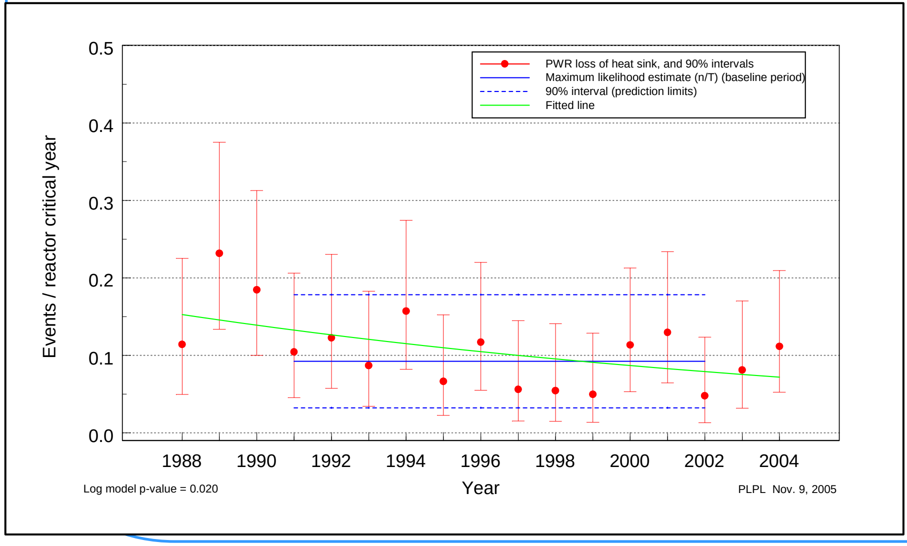
PWR General Transients



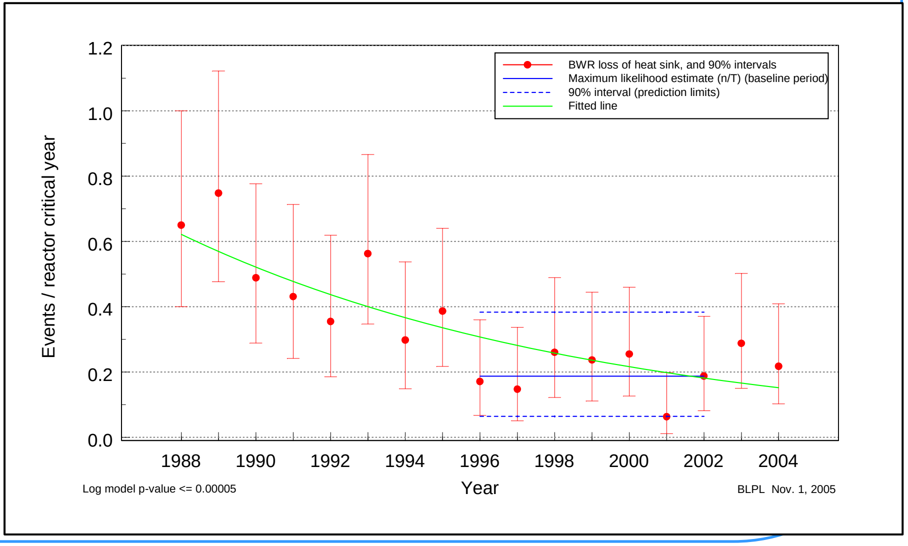
BWR General Transients



PWR Loss of Heat Sink



BWR Loss of Heat Sink



Courtesy of P. Baranowsky. Used with permission.

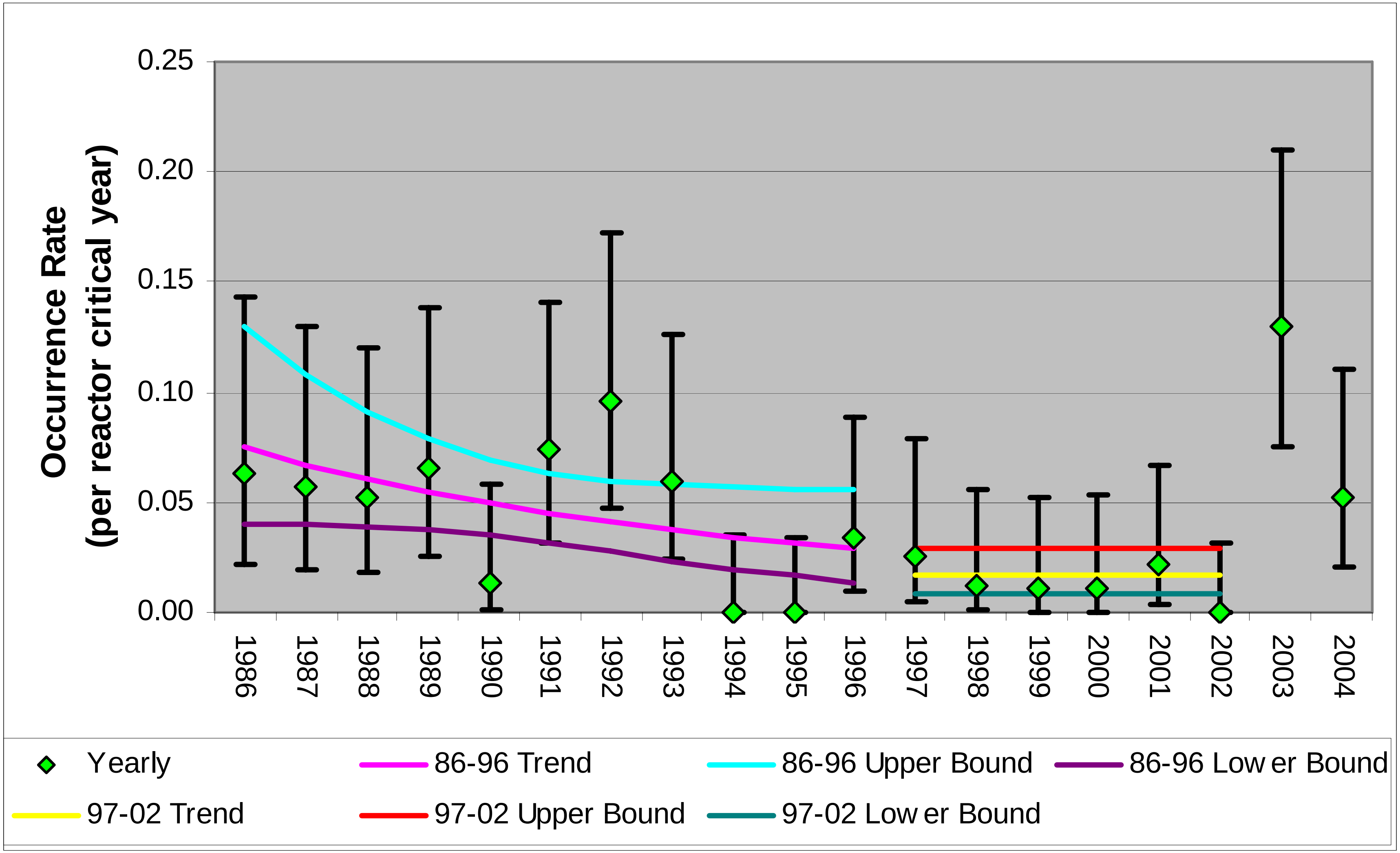
INITIATING EVENTS INSIGHTS

- **Most initiating events have decreased in frequency over past 10 years.**
- **Combined initiating event frequencies are 4 to 5 times lower than values used in NUREG-1150 and IPEs.**
- **General transients constitute majority of initiating events; more severe challenges to plant safety systems are about one-quarter of events.**

P. Baranowsky, RIODM Lecture, MIT, 2006

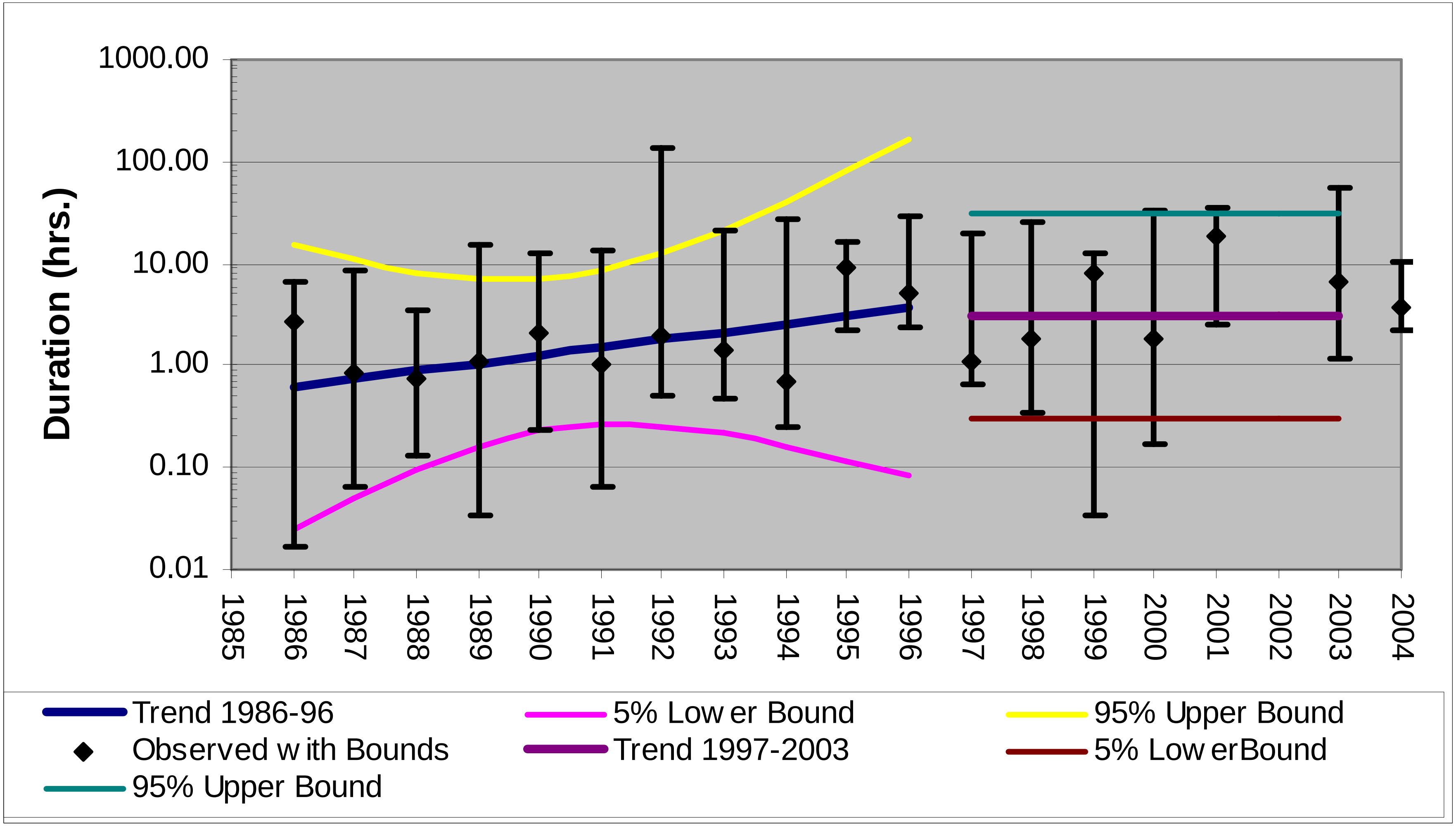
Courtesy of P. Baranowsky. Used with permission.

ANNUAL LOOP FREQUENCY TREND



Courtesy of P. Baranowsky. Used with permission.

ANNUAL LOOP DURATION TREND



Department of Nuclear Science and Engineering

Courtesy of P. Baranowsky. Used with permission.

LOOP FREQUENCY INSIGHTS

- Overall LOOP frequency during critical operation has decreased over the years (from 0.12/ry to 0.036/ry)
- Average LOOP duration has increased over the years:
  - Statistically significant increasing trend for 1986–1996
  - Essentially constant over 1997–2004
- 24 LOOP events between 1997 and 2004; 19 during the “summer” period
- No grid-related LOOP events between 1997 and 2002; 13 in 2003 and 2004
- Decrease in plant-centered and switchyard-centered LOOP events; grid events are starting to dominate

Courtesy of P. Baranowsky. Used with permission.

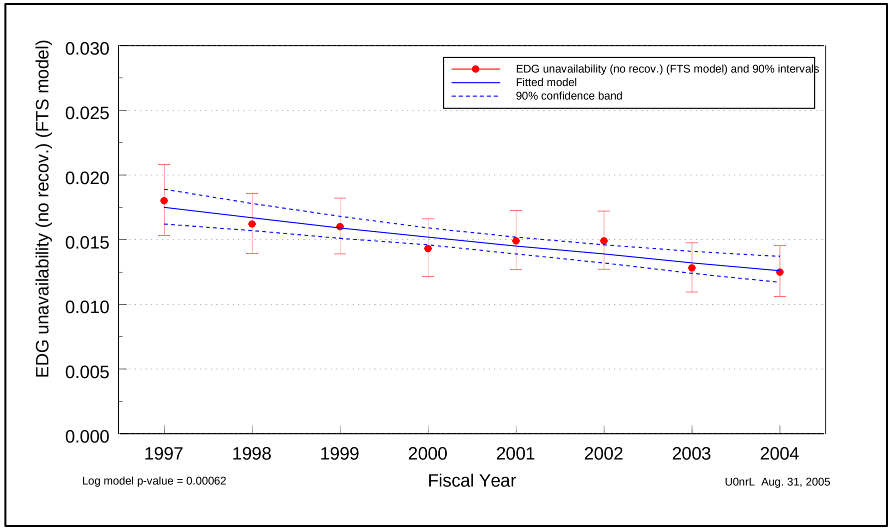
SYSTEM RELIABILITY STUDY RESULTS

STUDY	MEAN UNRELIABILITY	UNPLANNED DEMAND TREND	FAILURE RATE TREND	UNRELIABILITY TREND
AFW (1987–2004)	5.19E-4	↓	↓	↔
EDG (1997–2004)	2.18E-2	N/A	N/A	↔
HPCI (1987–2004)	6.25E-2	↓	↓	↓
HPCS (1987–2004)	9.48E-2	↓	↔	↔
HPI (1987–2004)	1.09E-3	↓	↓	↔
IC (1987–2004)	2.77E-2	↓	↓	↔
RCIC (1987–2004)	5.18E-2	↓	↓	↔

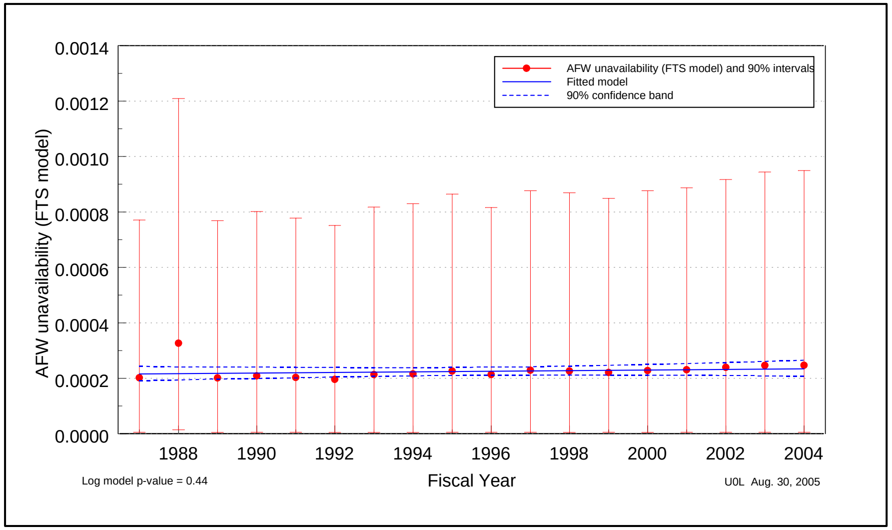
Courtesy of P. Baranowsky. Used with permission.

PWR SYSTEM RELIABILITY STUDIES

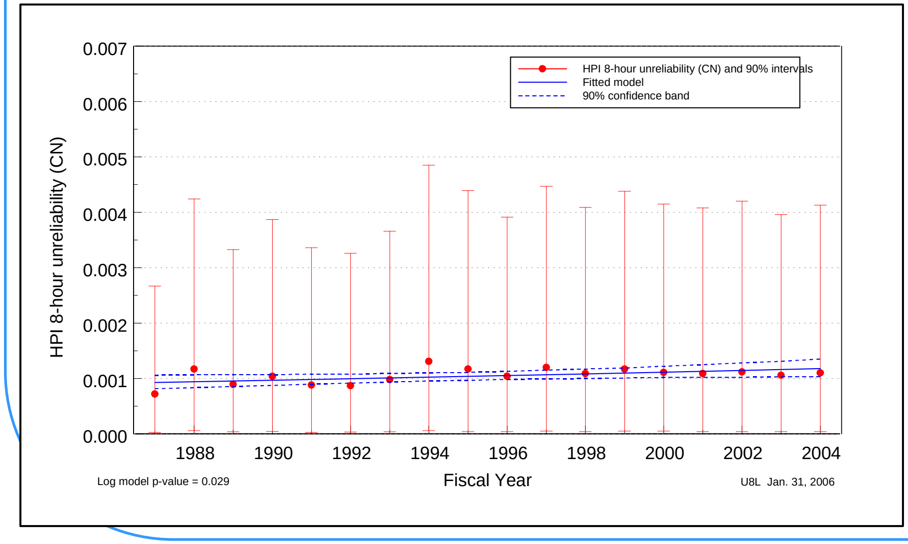
EDG Unavailability (FTS)



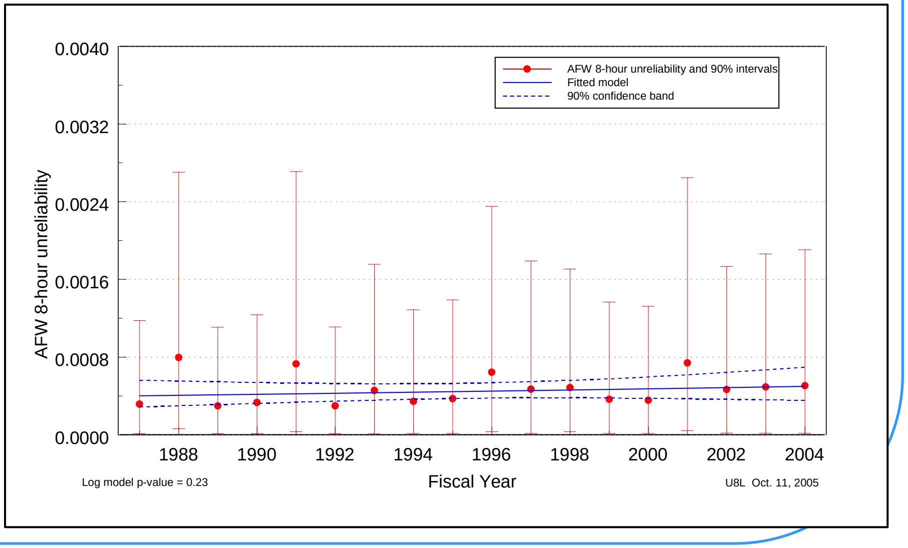
AFW Unavailability (FTS)



HPI Unreliability (8 hr mission)



AFW Unreliability (8 hr mission)



Courtesy of P. Baranowsky. Used with permission.

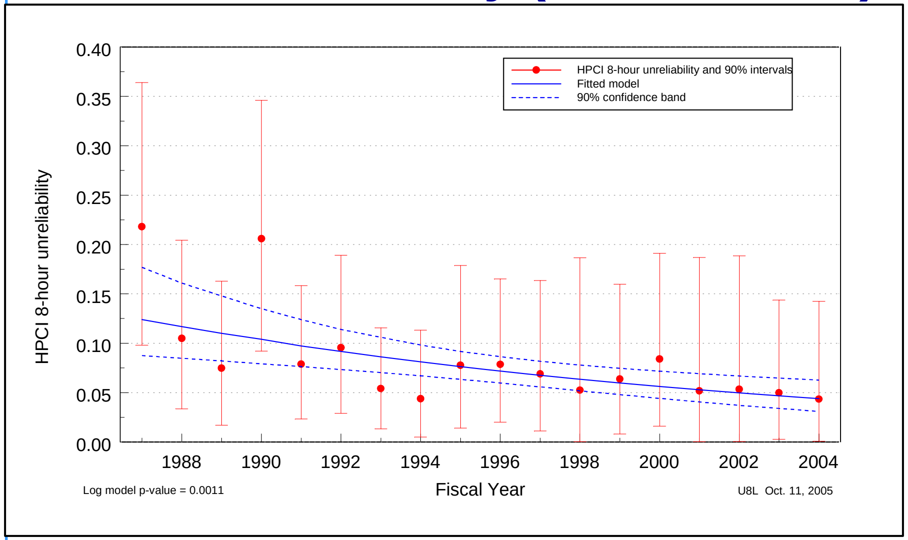
PWR SYSTEM INSIGHTS

- **EDG**
  - **EDG start reliability much improved over past 10 years.**
  - **Failure-to-run rates lower than in most PRAs.**
- **AFW**
  - **Industry average reliability consistent with or better than Station Blackout and ATWS rulemaking.**
  - **Wide variation in plant specific AFW reliability primarily due to configuration.**
  - **Failure of suction source identified as a contributor (not directly modeled in some PRAs).**
- **HPI**
  - **Wide variation in plant specific HPI reliability due to configuration.**
  - **Various pump failures are the dominant failure contributor.**

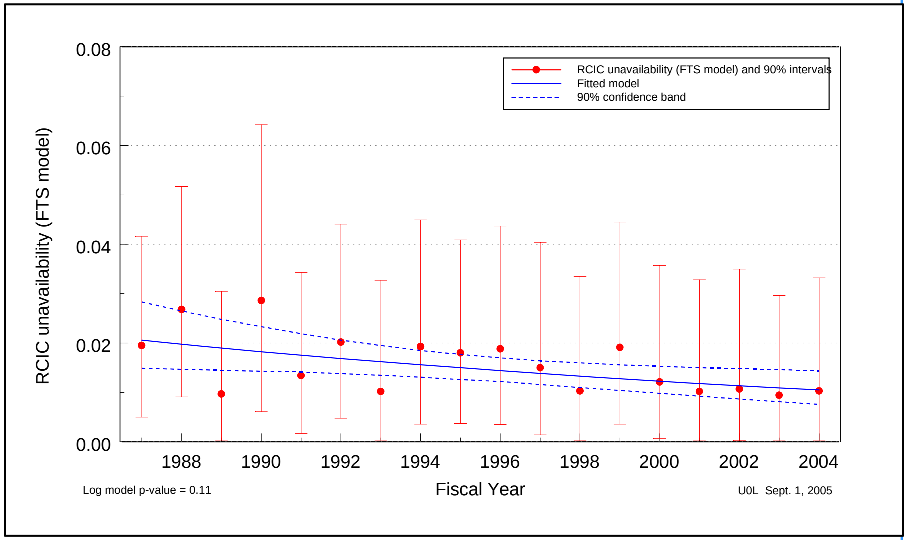
Courtesy of P. Baranowsky. Used with permission.

BWR SYSTEM RELIABILITY STUDIES

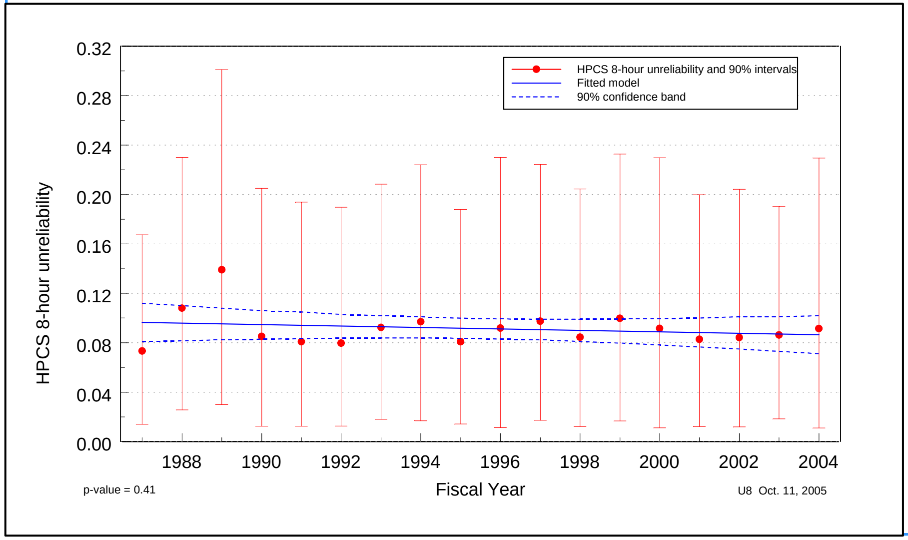
HPCI Unreliability (8 hr mission)



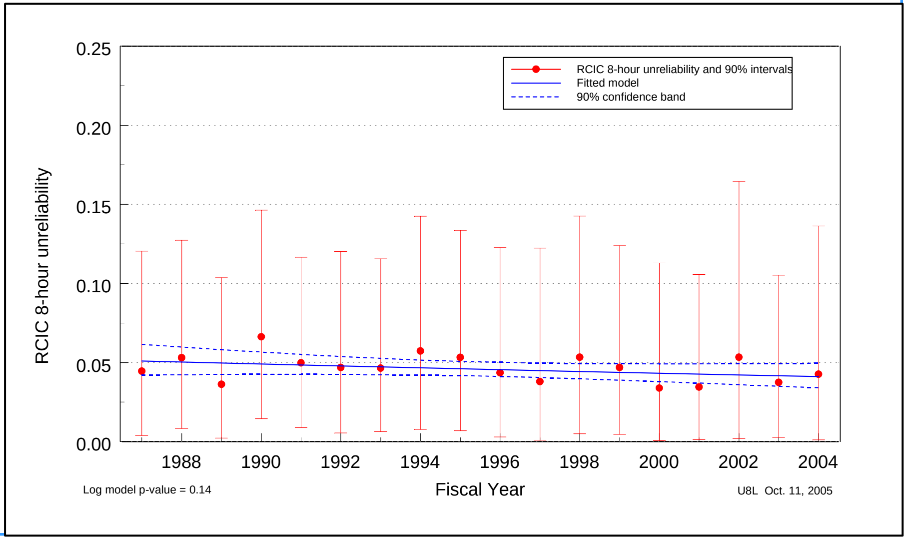
RCIC Unavailability (FTS)



HPCS Unreliability (8 hr mission)



RCIC Unreliability (8 hr mission)



Courtesy of P. Baranowsky. Used with permission.

BWR SYSTEM INSIGHTS

- HPCI
  - Industry-wide unreliability shows a statistically significant decreasing trend.
  - Dominant Failure: failure of the injection valve to reopen during level cycling.
- HPCS
  - Industry average unreliability indicates a constant trend.
  - Dominant Failure: failure of the injection valve to open during initial injection.
- RCIC
  - Industry average unreliability indicates a constant trend.
  - Dominant Failure: failure of the injection valve to reopen during level cycling.

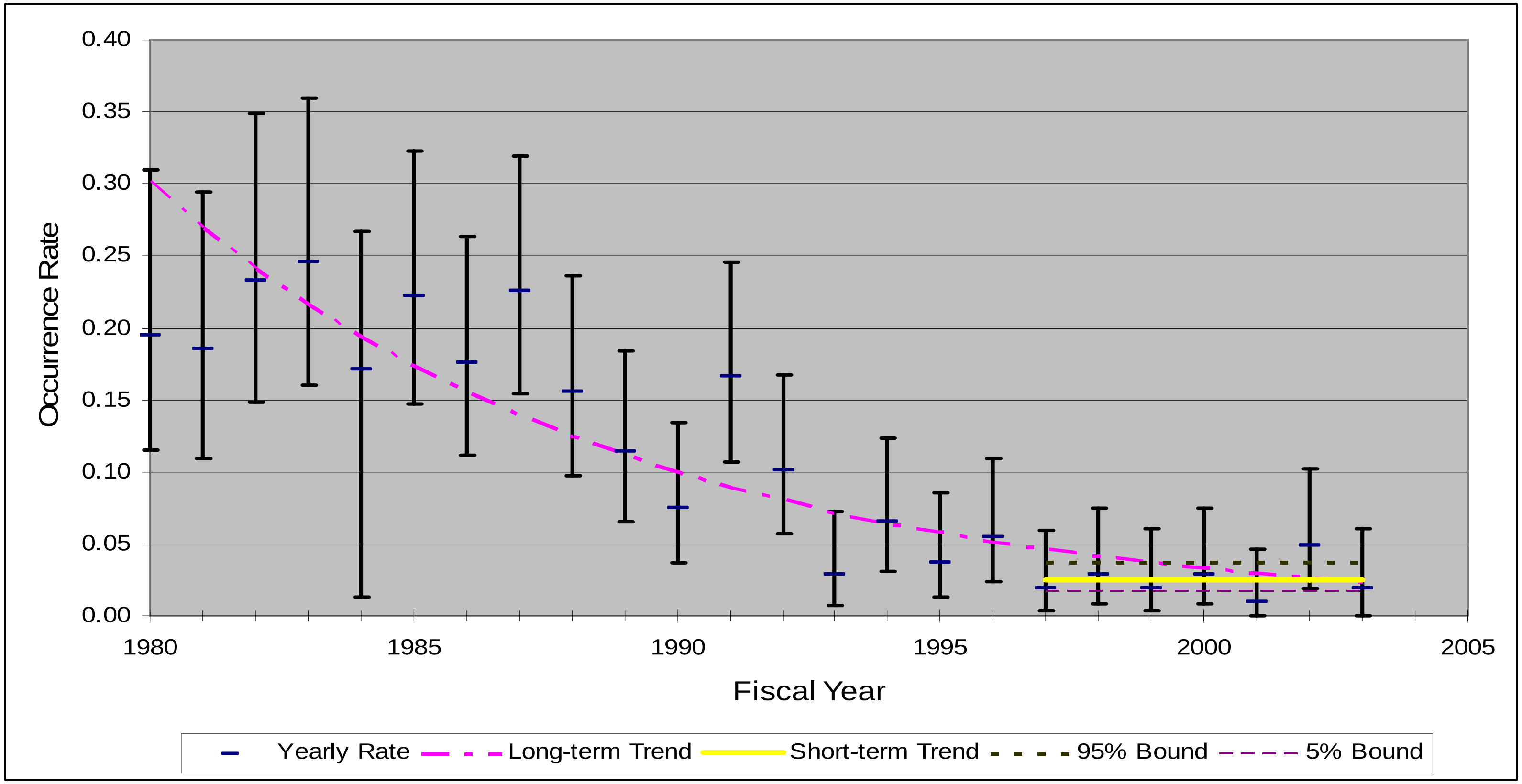
Courtesy of P. Baranowsky. Used with permission.

COMMON-CAUSE FAILURE (CCF) EVENTS

- Criteria for a CCF Event:
  - Two or more components fail or are degraded at the same plant and in the same system.
  - Component failures occur within a selected period of time such that success of the PRA mission would be uncertain.
  - Component failures result from a single shared cause and are linked by a coupling mechanism such that other components in the group are susceptible to the same cause and failure mode.
  - Equipment failures are not caused by the failure of equipment outside the established component boundary.

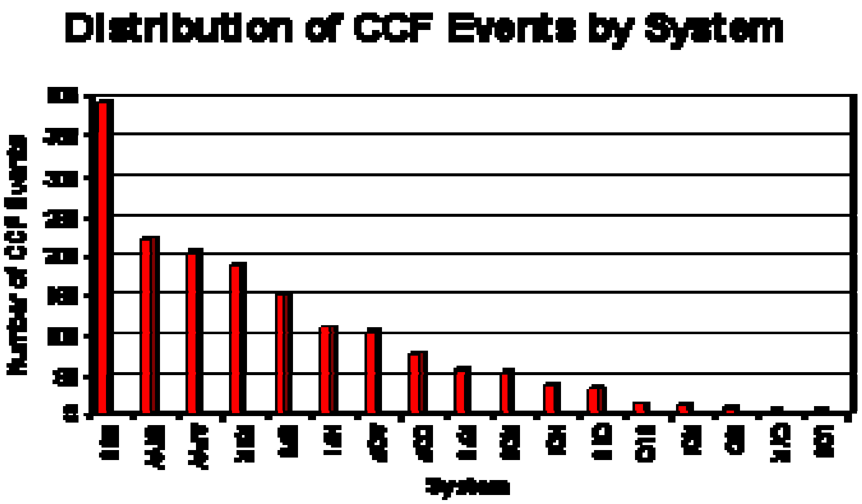
Courtesy of P. Baranowsky. Used with permission.

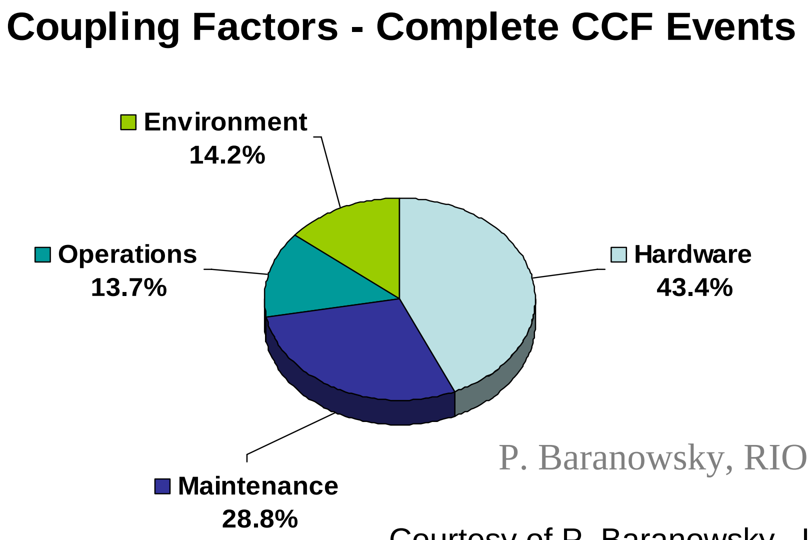
CCF OCCURRENCE RATE



P. Baranowsky, RIODM Lecture, MIT, 2006

Courtesy of P. Baranowsky. Used with permission.





P. Baranowsky, RIODM Lecture, MIT, 2006

Courtesy of P. Baranowsky. Used with permission.