Design Optimization Using RBOT and FaultTree+

International System Safety Conference

San Diego, CA

Michael D. Muhlheim, Ph.D.

Oak Ridge National Laboratory

August 2005

Coauthors

Joseph W. Cletcher, II
Oak Ridge National Laboratory

Jeremy L. Hynek
Isograph, Inc.

Stephen Flanagan, Ph.D
Isograph Ltd.

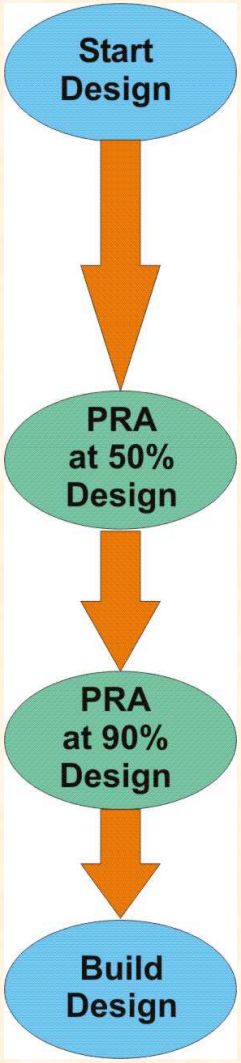
Robert Stack
Dow Chemical

Many Decisions About Safety Have to be Made Early in the Design

- Safety is sometimes viewed as a coat of paint —something to be added to the finished design rather than an integral part of the design.

- Hazards or operating problems not identified until late in the design typically result in complex add-on equipment.

OLD Method



In a Typical Design Process, the Probabilistic Risk Assessments (PRAs) are Developed at Specific "Freeze Points" of the Design

- The PRA for the AP600 spanned five stages and six revisions
- During final design approval of the CE80+, 63 design alternatives were considered, and 27 were quantified

Change—change—who wants change? Things are bad enough as they are. (*Lord Salisbury*)

- **Optimization requires early coordination between designers and PRA practitioners**

- **Optimization also requires the willingness to evaluate atypical, unusual, or simply different design configurations compared to "proven" practices**

Many Times, What Is Perceived To Be True Is Different From What Is Actually True

- It is more likely that you will be bitten by
  - a person
  - wild rat
  - squirrel

  than by a shark.

- It is more likely that you will be fatally injured by
  - a dog
  - snake
  - mountain lion

  than by a shark.

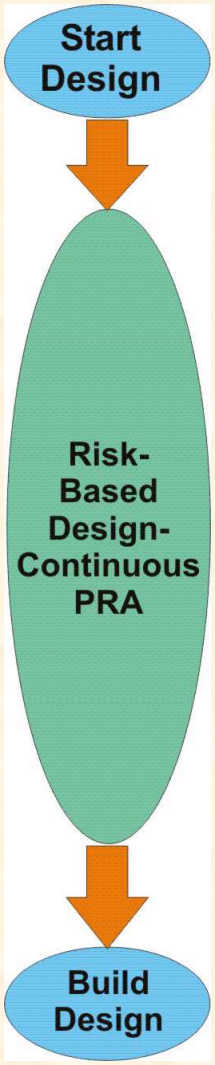
Source: Florida Museum of Natural History

A Risk-Based Design Reduces, Controls, or Eliminates Risk by Quantitatively Identifying Risk Drivers as the Design Develops

- Westinghouse used a "safety-by-design" approach at the very beginning of the design process for its IRIS Plant

- Using ORNL's Risk-Based Design Optimization Tool (RBOT), different types of plant systems and components, in different operational states, were evaluated interchangeably as the design progressed

NEW Method



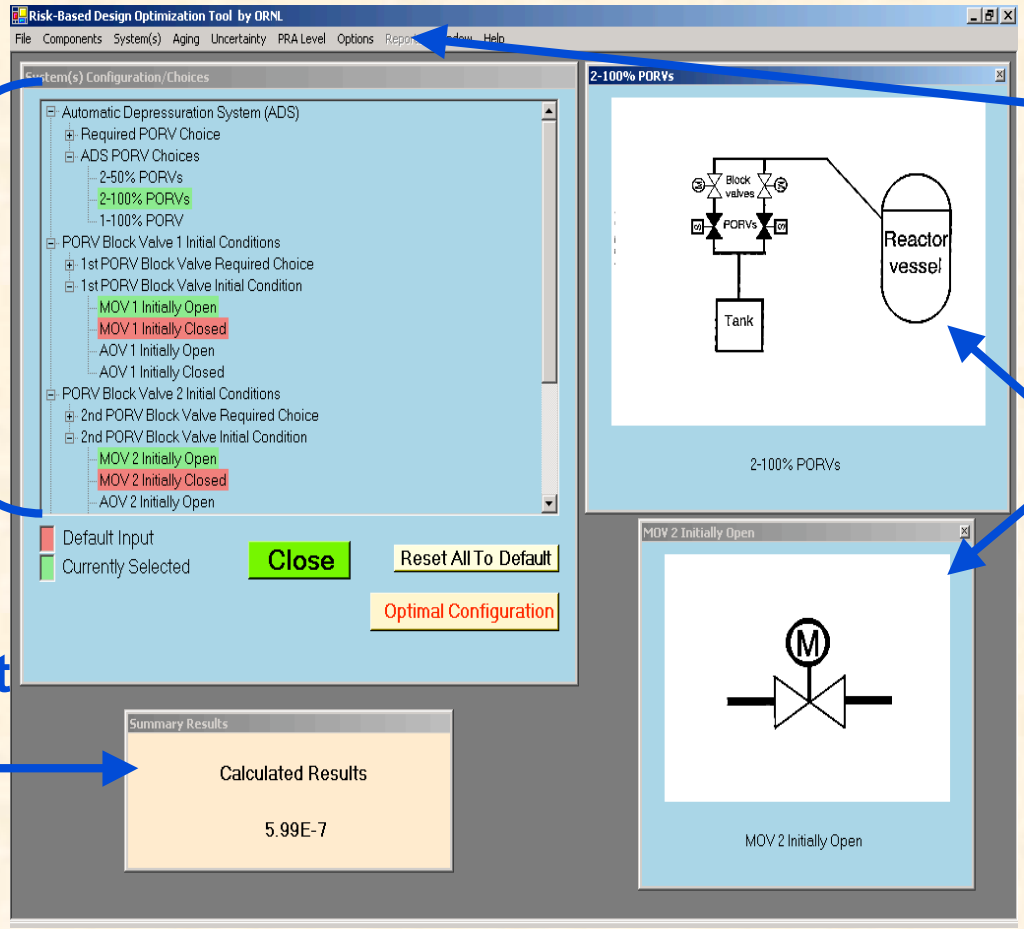
Any Fault Tree Created Using RBOT Is the Same as That Which Would Result if Those Choices Were the Original Design

Design alternatives are provided in a scroll-down menu

Other options are available

Graphical displays of the design options selected from the scroll-down menu provide confirmation of design choices

Metric of interest relayed from *FaultTree*+ back to RBOT



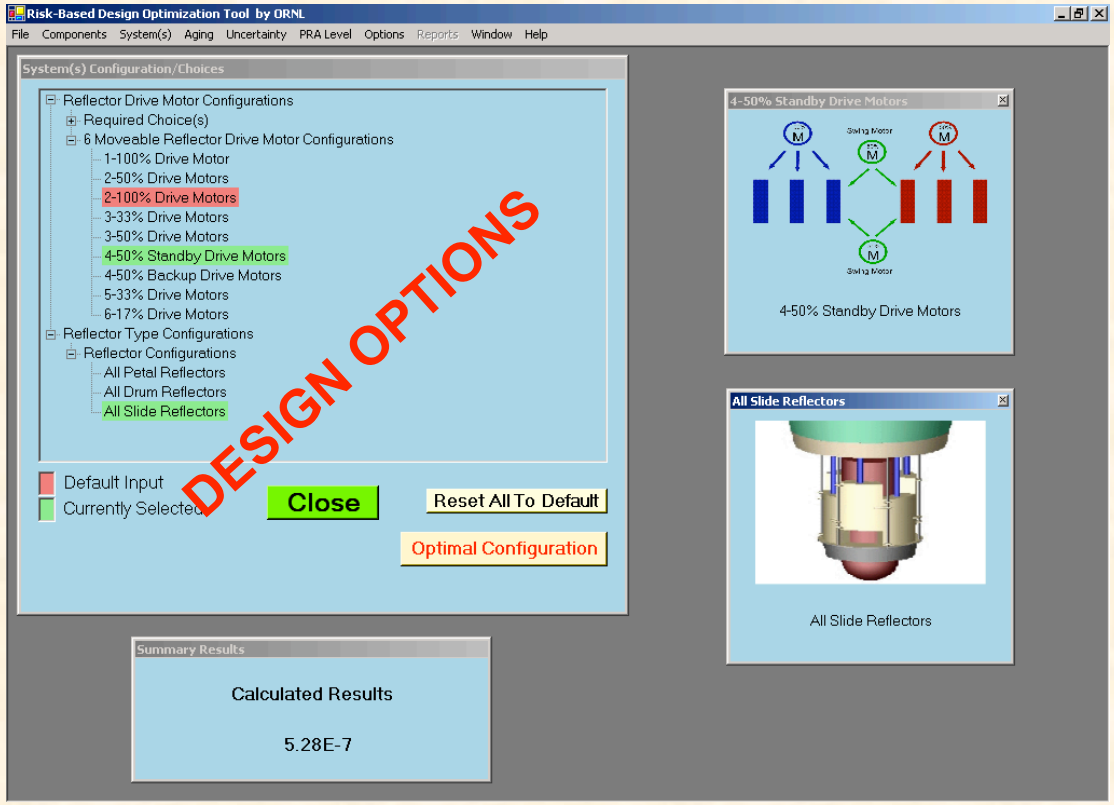
RBOT is Effective in Reducing Design Cycle Time and Improving System Reliability

Design Trades

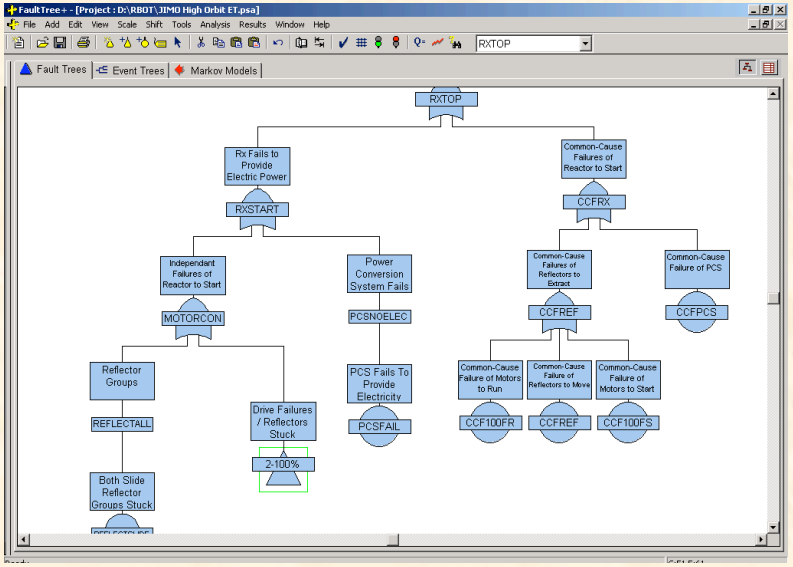
- Component choices
  - Type
  - Position
  - Failure data
- System architecture

Figures of Merit

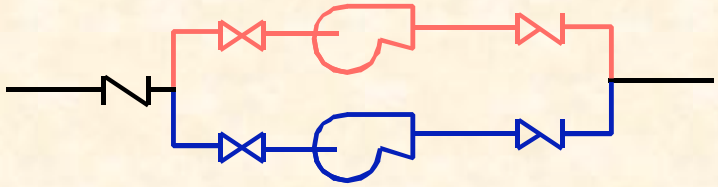
- Aging
- Reliability
- Cost vs reliability
- Uncertainties and sensitivity



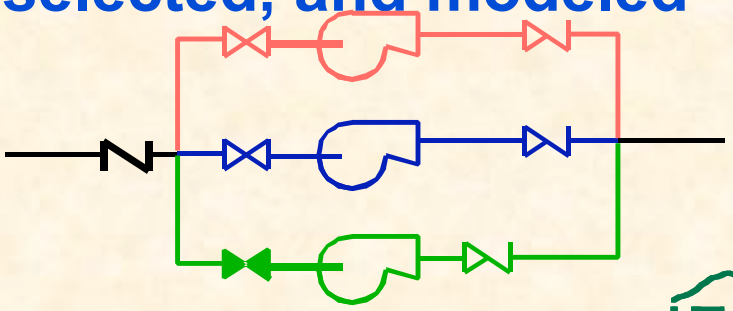
The PRA Analysis Using RBOT Starts the Same as Current Analyses



- **PRA analyst**
  - **Develops PRA model of the original design using *FaultTree+***

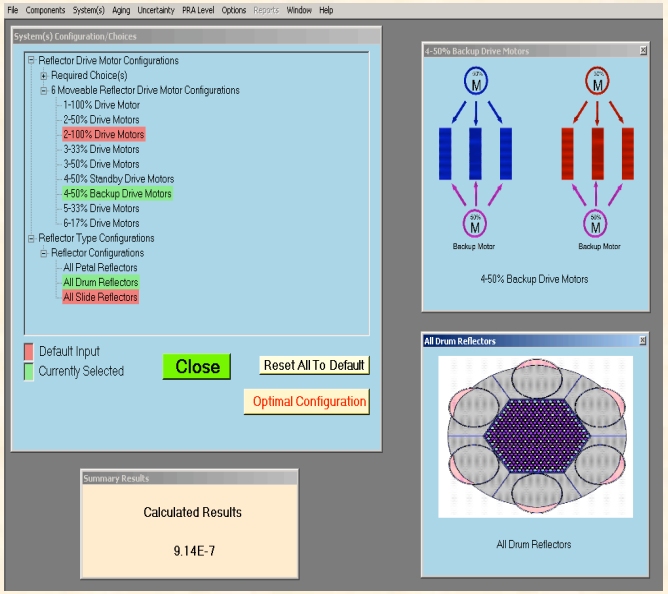


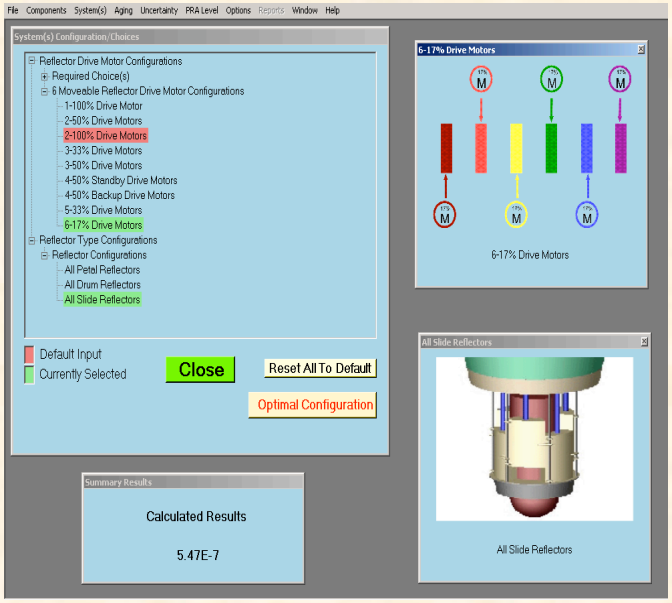
  - **Potential design alternatives are identified, selected, and modeled**



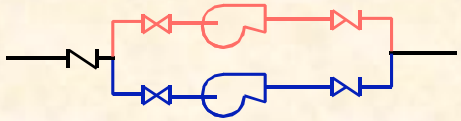
Once Loaded into RBOT, Any or All of the Design Options Can Be Made in ANY Order

- User
  - Selects design alternative(s) for review from scroll-down menu
  - Can optimize on train, system, or plant

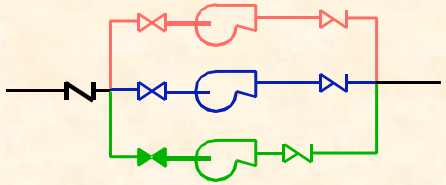


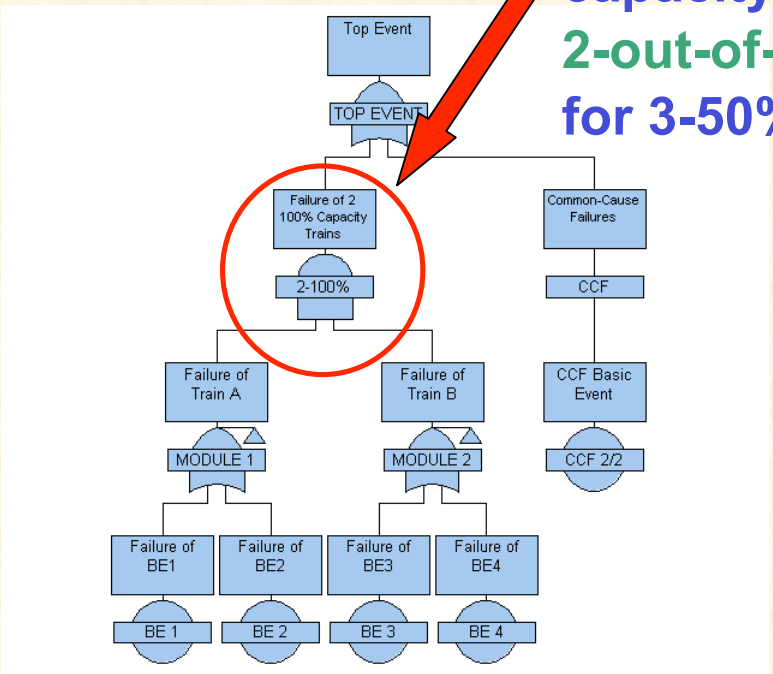


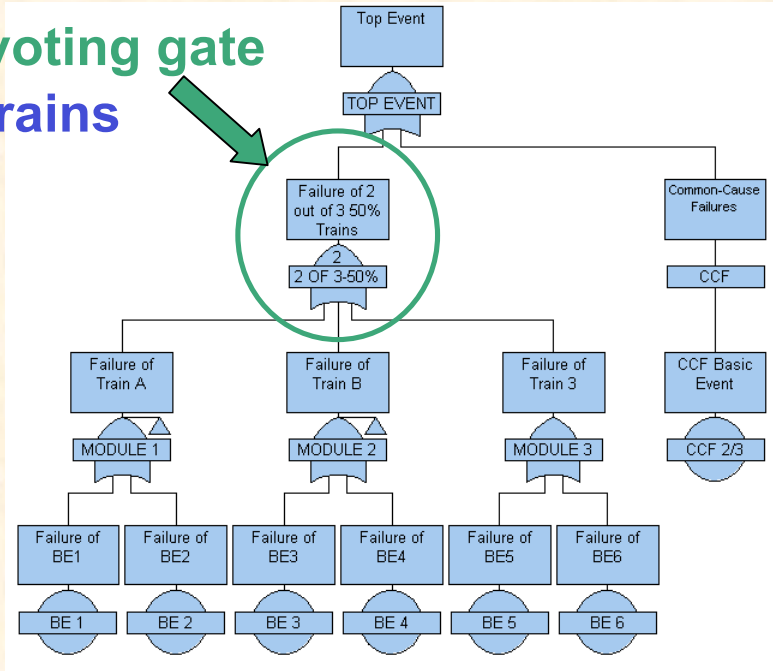
For the Option Chosen, RBOT Automatically Changes the Gates to Reflect the Correct Fault Logic



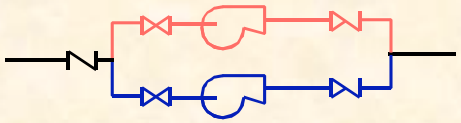
Gate changed from AND gate for 2-100% capacity trains to 2-out-of-3 voting gate for 3-50% trains

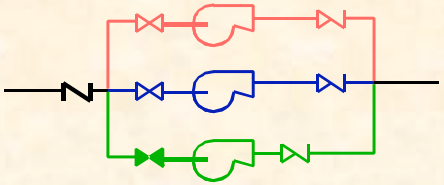


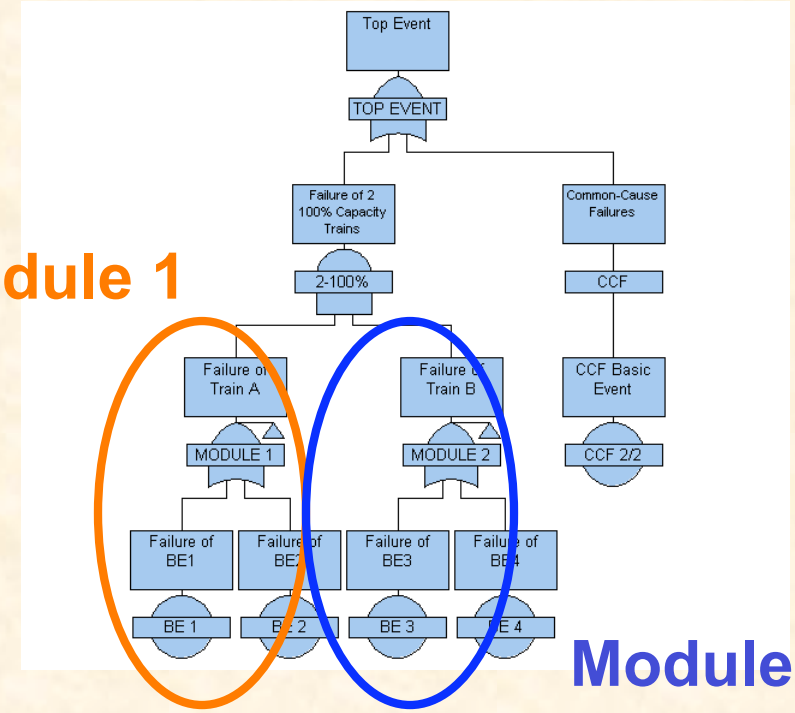


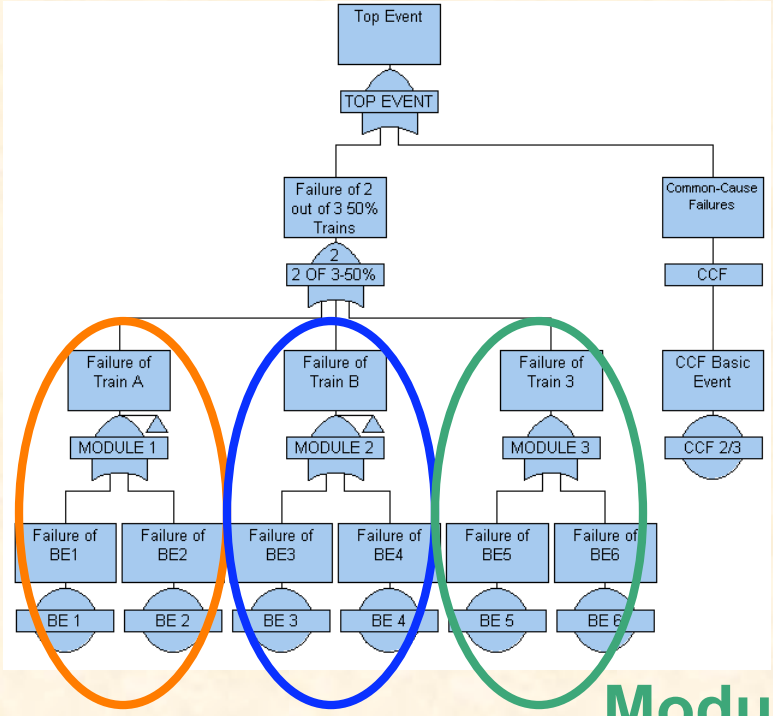


RBOT Inserts the Correct Fault Tree Modules into the PRA Model in *FaultTree+*







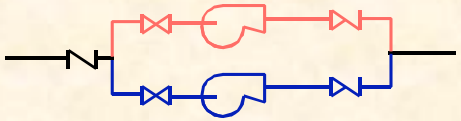


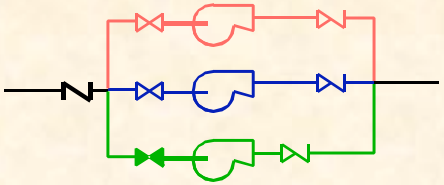
Module 1

Module 2

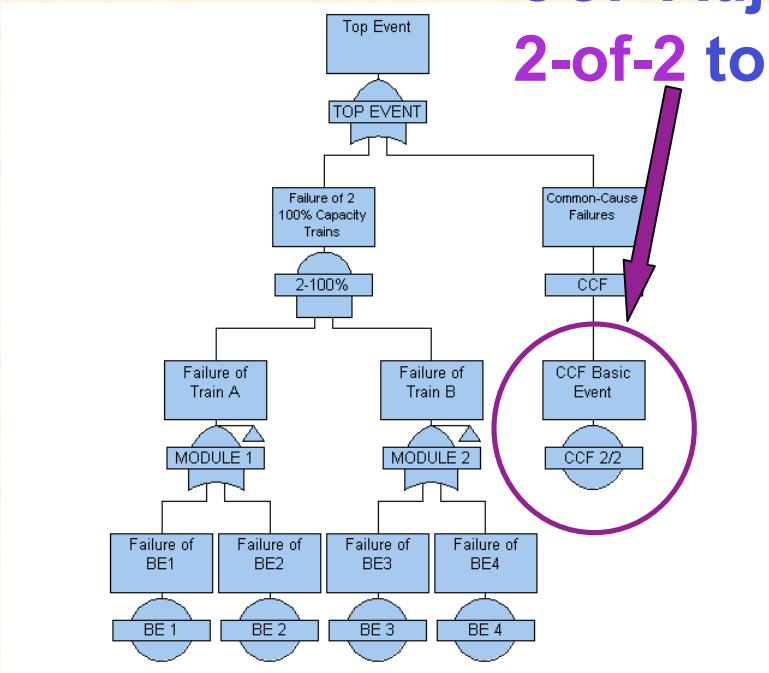
Module 3

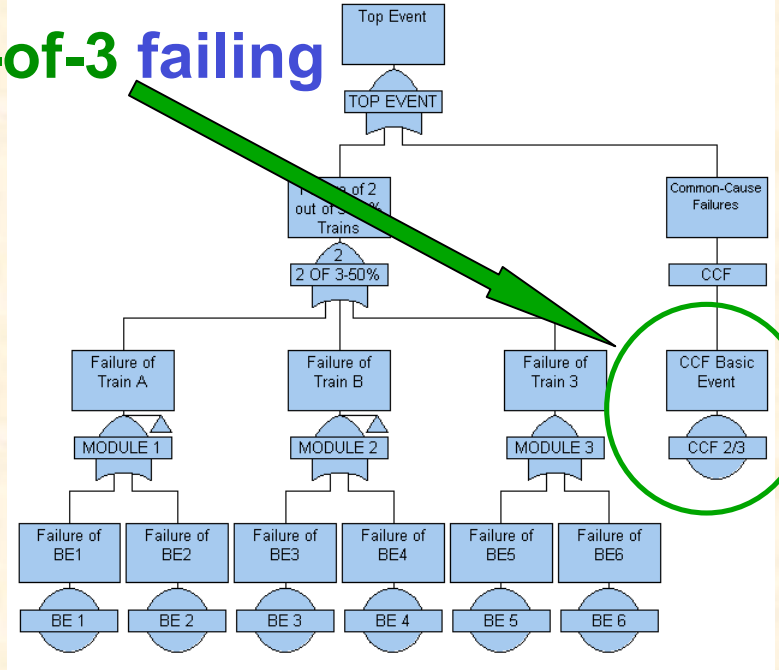
RBOT Also Accounts for Changes in Recovery Actions, Human Error, and Common-Cause Failure (CCF) Probabilities





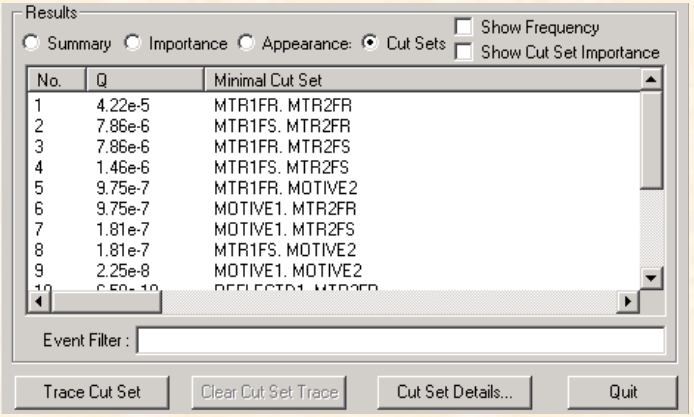
CCF Adjusted from
2-of-2 to 2-of-3 failing

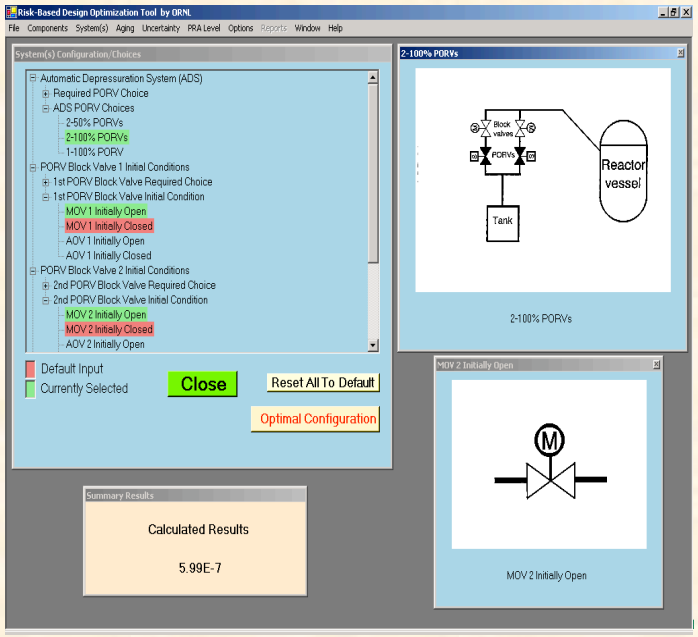




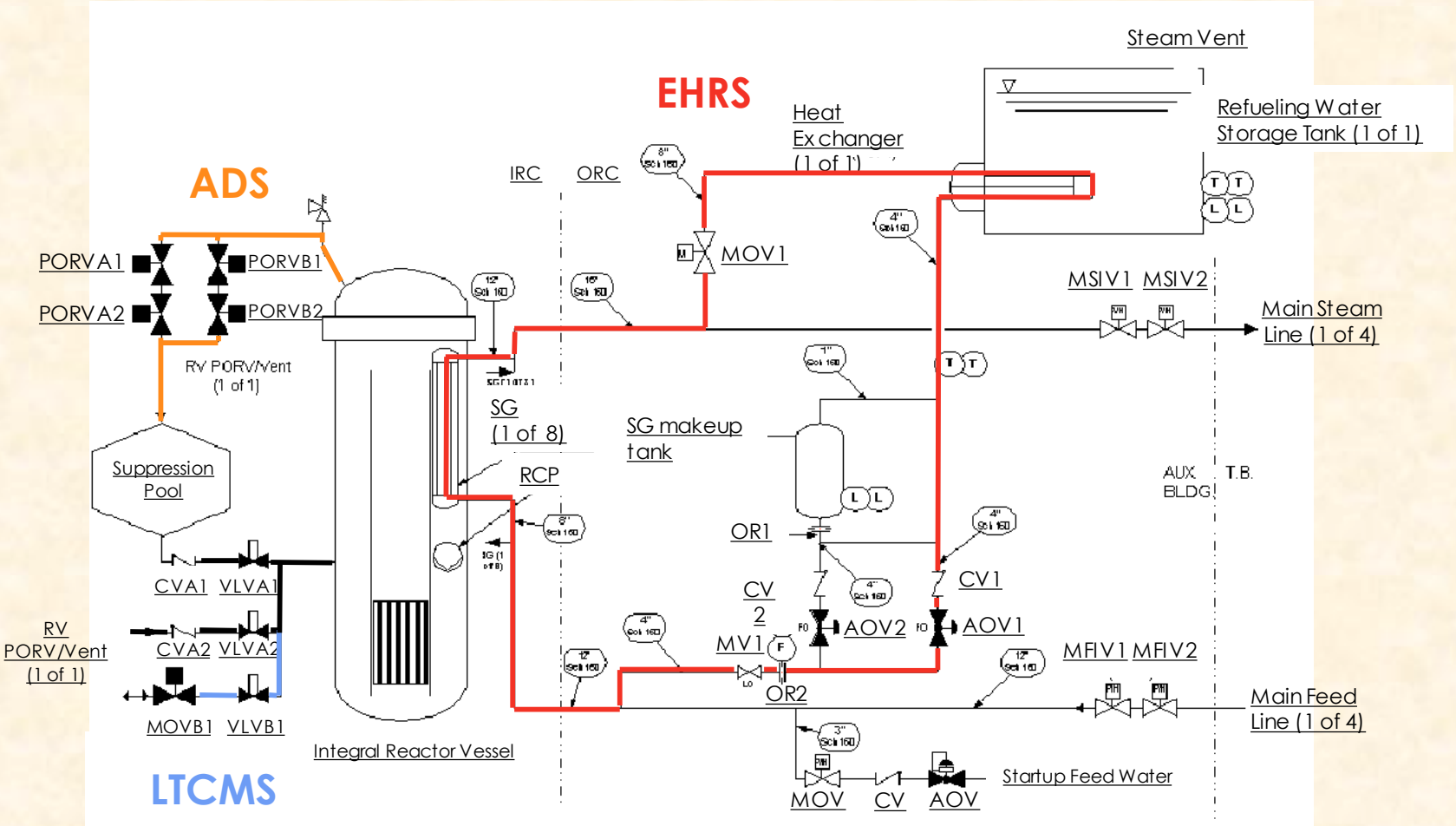
All of the Results from *FaultTree+* are Still Available via RBOT

- *FaultTree*+
  - Recalculates fault tree parameters
  - Transmits the results back to RBOT
- RBOT
  - Provides graphical display
  - Provides numeric display



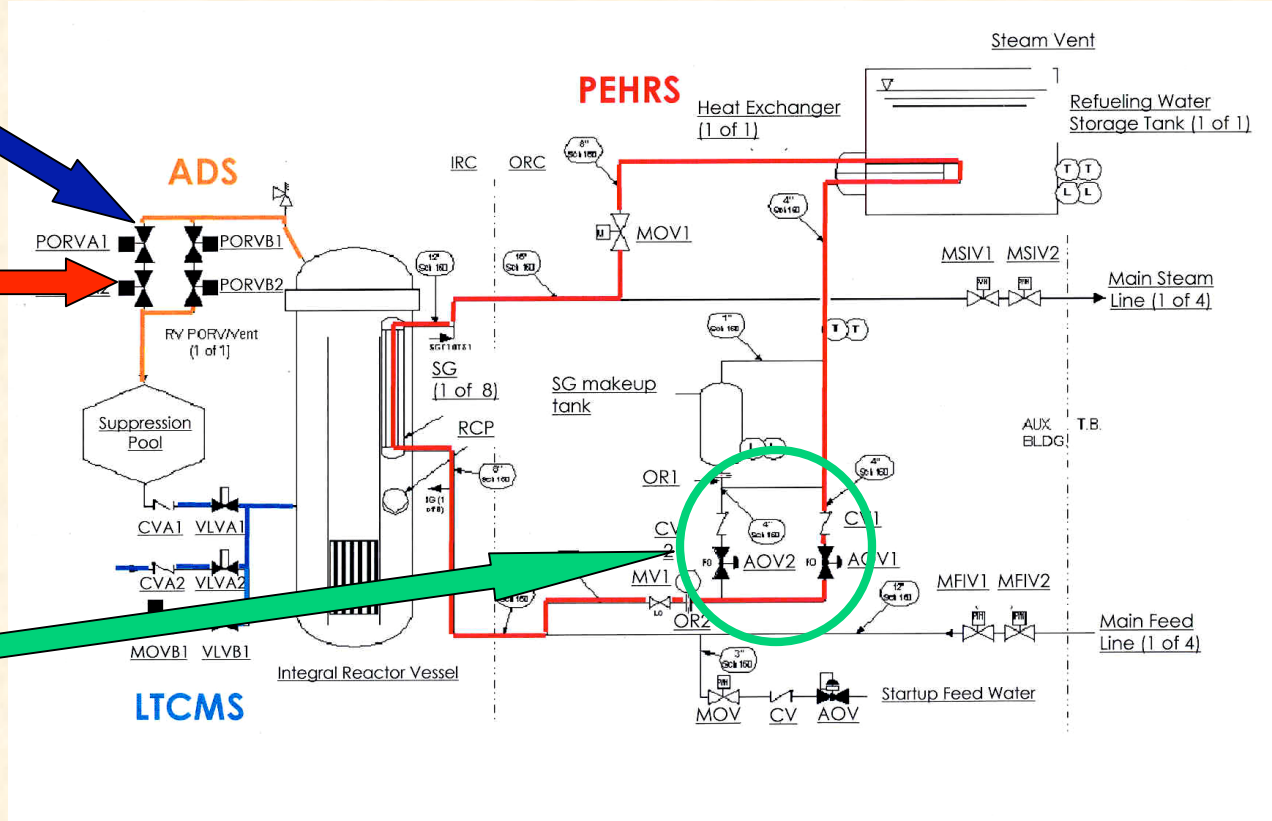


RBOT Was Used to Identify the Optimal Designs of the IRIS Safety Systems

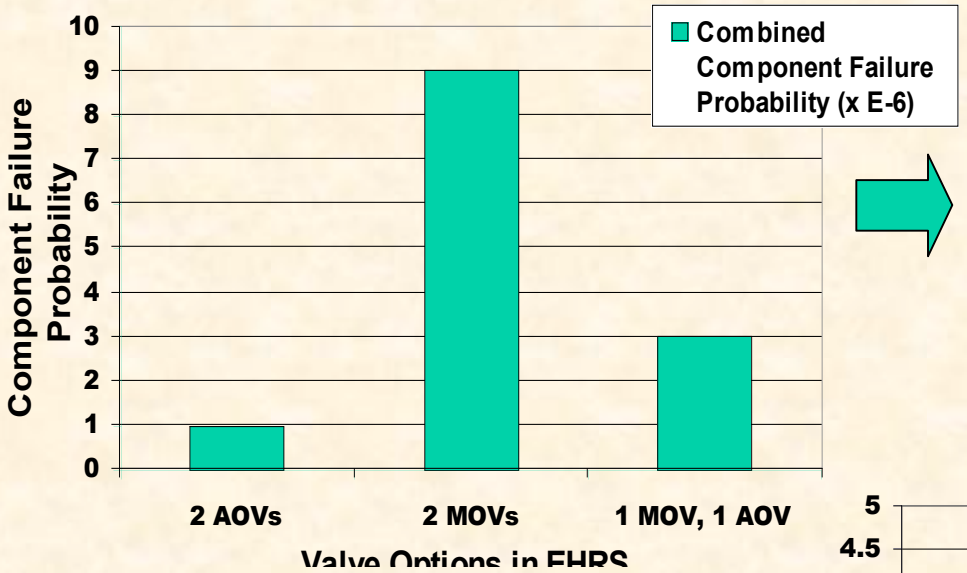


The 11 Component Choices Yield 160 Design Alternatives

- Block valve position and type
- Number and capacity of relief valves (RVs) in the Automatic Depressurization System (ADS) (1-100%, 2-50%, 2-100% RVs)
- Type of valves in Emergency Heat Removal System (EHRS) main and bypass lines

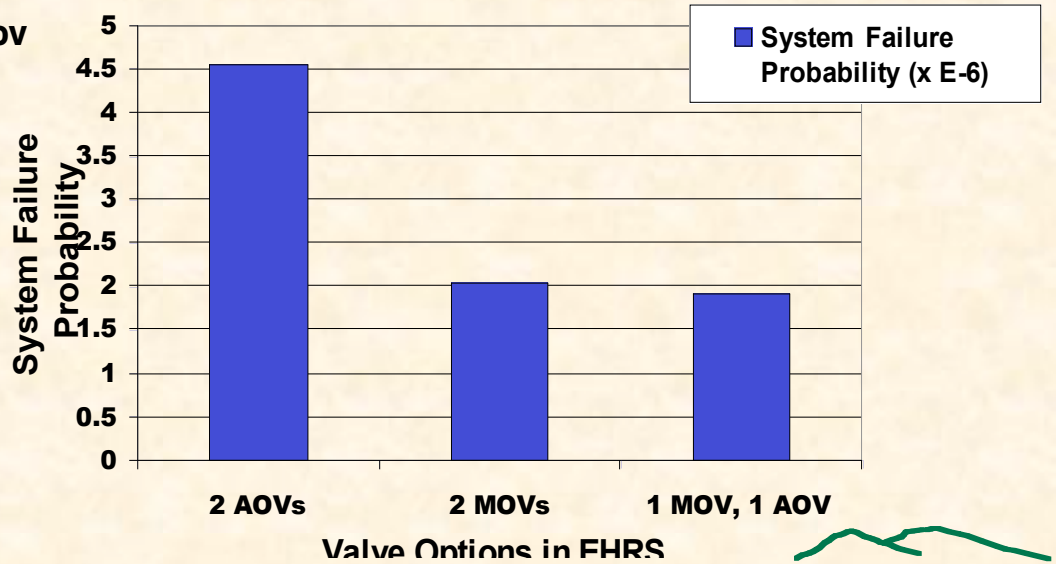


"Logical" Decisions for Optimization May Be Wrong



The air-operated valves (AOVs) are significantly more reliable than the motor-operated valves (MOVs).

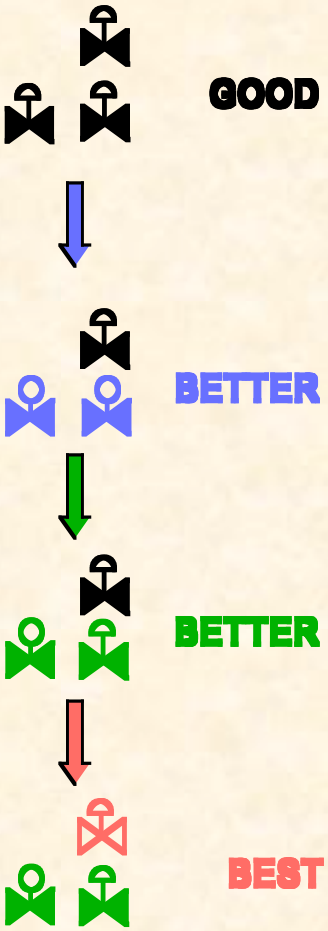
The use of the most reliable valves resulted in the most unreliable system!



The MOV / AOV valve option is only slightly better than the 2 MOV option because the common-cause failure of the check valves is the dominant contributor to system failure.

Failure Modes Provide Clues on How System Can Be Improved

BASE CASE
ADS block valves closed
Valves in EHRS are AOVs



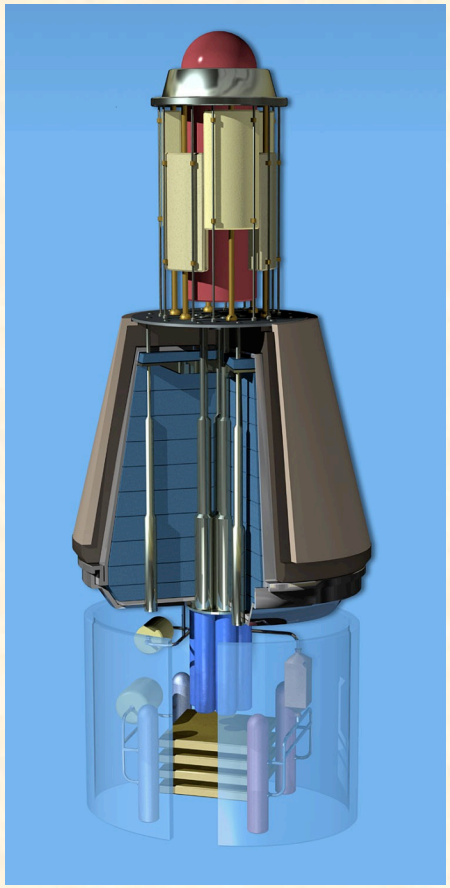
Valves in EHRS changed to MOVs
CCF of valves reduced by a factor of 20!

Valves in EHRS changed to AOVs / MOVs
CCF of valves no longer a contributor!

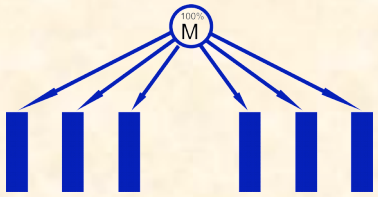
ADS block valves changed to open
CCF of block valves no longer a contributor!

Consider the Following Example of Optimizing the Number of Reflector Drive Motors on an SP-100 Type Reactor

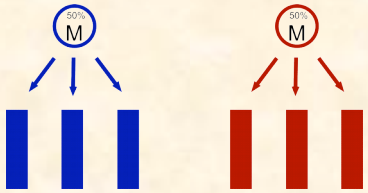
For the space reactor to achieve a critical state, 4 of the 6 reflectors must move to their "in" position.



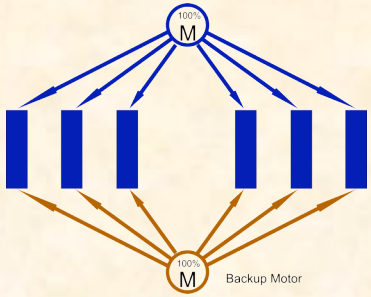
Because of the Ease of Evaluating Different Design Options, Nine Reflector Drive Motor Options Were Evaluated Using RBOT



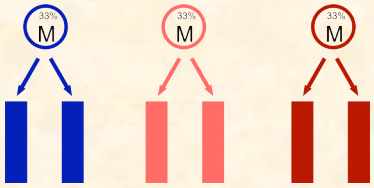
1-100%



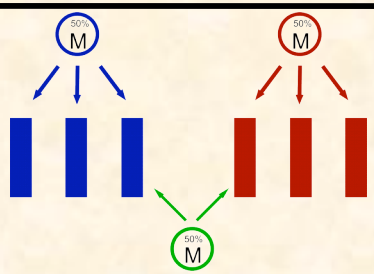
2-50%



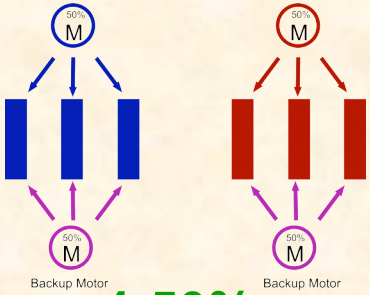
2-100%



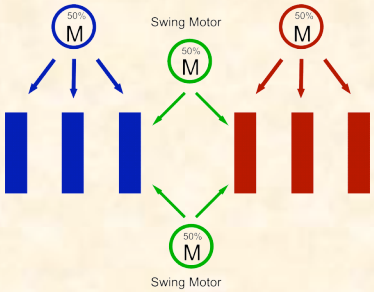
3-33%



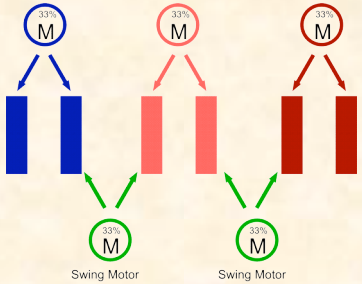
3-50%



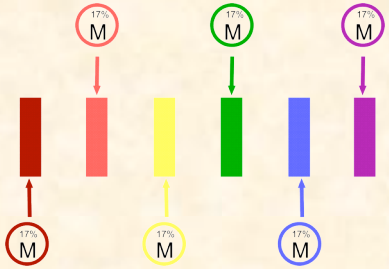
4-50%



4-50%

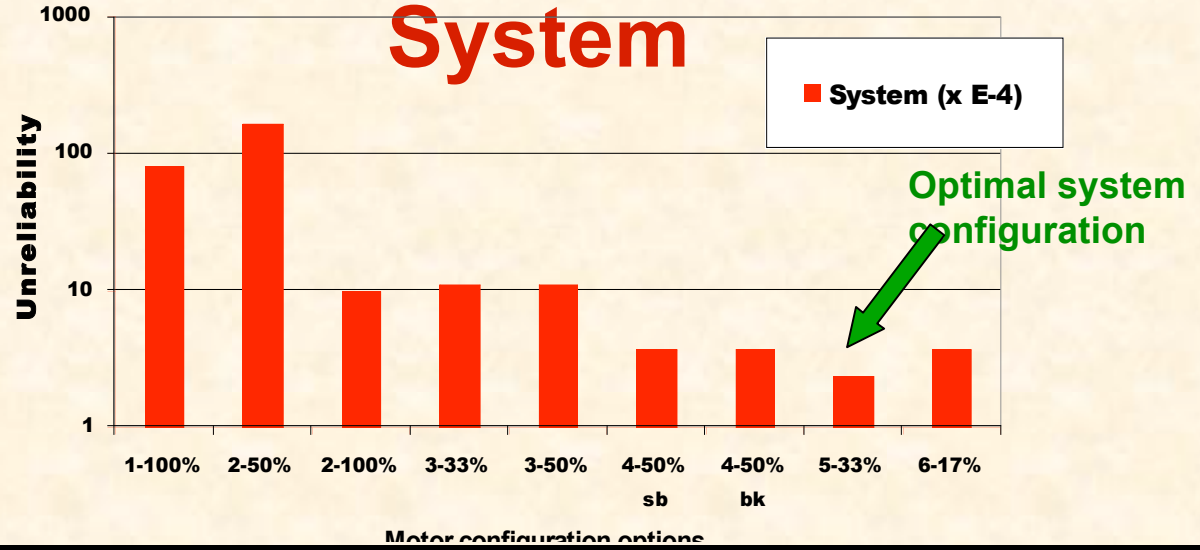


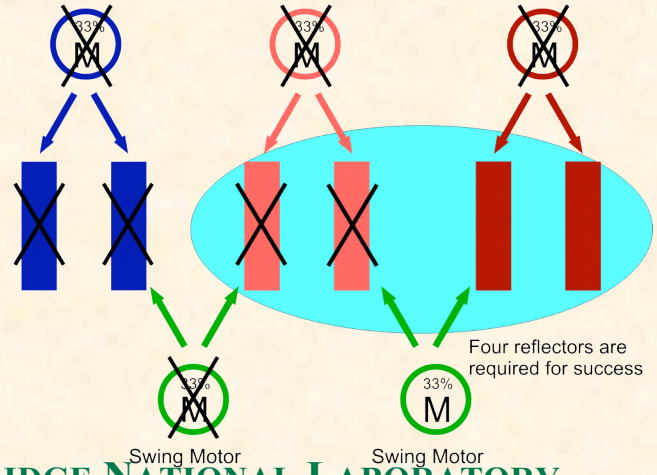
5-33%

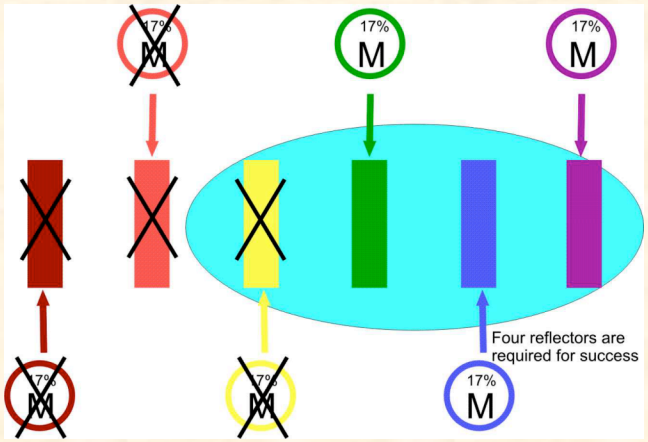


6-17%

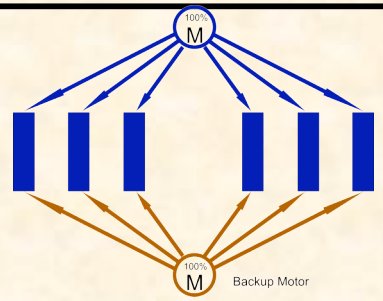
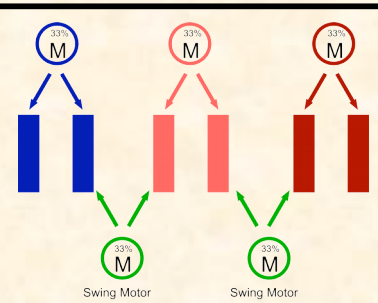
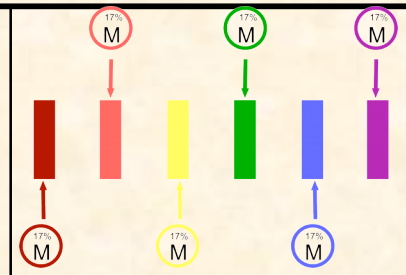
A Risk-Based Analysis Shows that 5 Motors Are Optimal for the "4-out-of-6" System



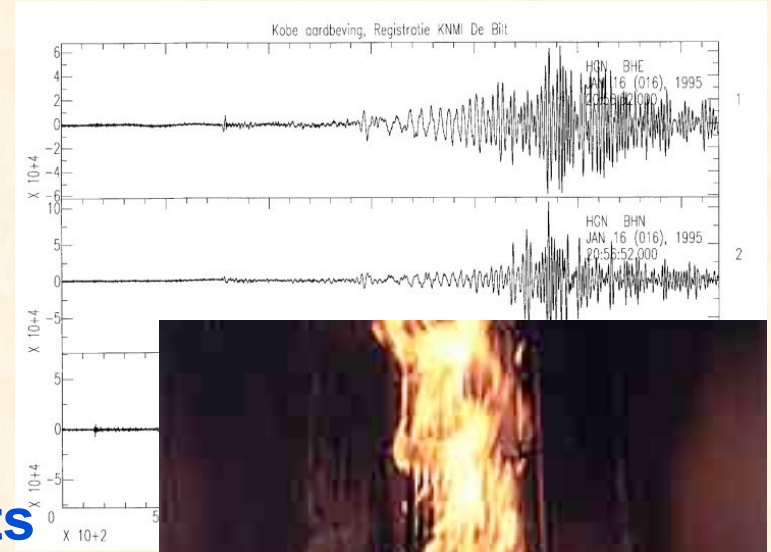




A 2-100% Capacity Reflector Motor Drive System, Although not the Most Reliable, has Advantages in Simplicity, Mass, and Cost

	 **2-100%**	 **5-33%**	 **6-17%**
Reliability	**3x worse than 5-33%** **2x worse than 6-17%**	**Most reliable architecture**	**About the same as 5-33%**
Simplicity	**Simple design with switching for backup motor**	**Complex design with swing motors**	**Simplest design**
Reactivity Control	**All Sliders move at same time**	**Banks of Sliders move at a time**	**Each Slider moves individually**
Mass	**Lightest of 3 architectures**	**3x that of 2-100%**	**3x that of 2-100%**
Cost	**Fewest parts, lowest cost**	**Most expensive**	**About as expensive as 5-33%**
Fault tolerance	**1**	**3**	**2**

RBOT Can Be Expanded to Simultaneously Evaluate External Events During the Design Phase

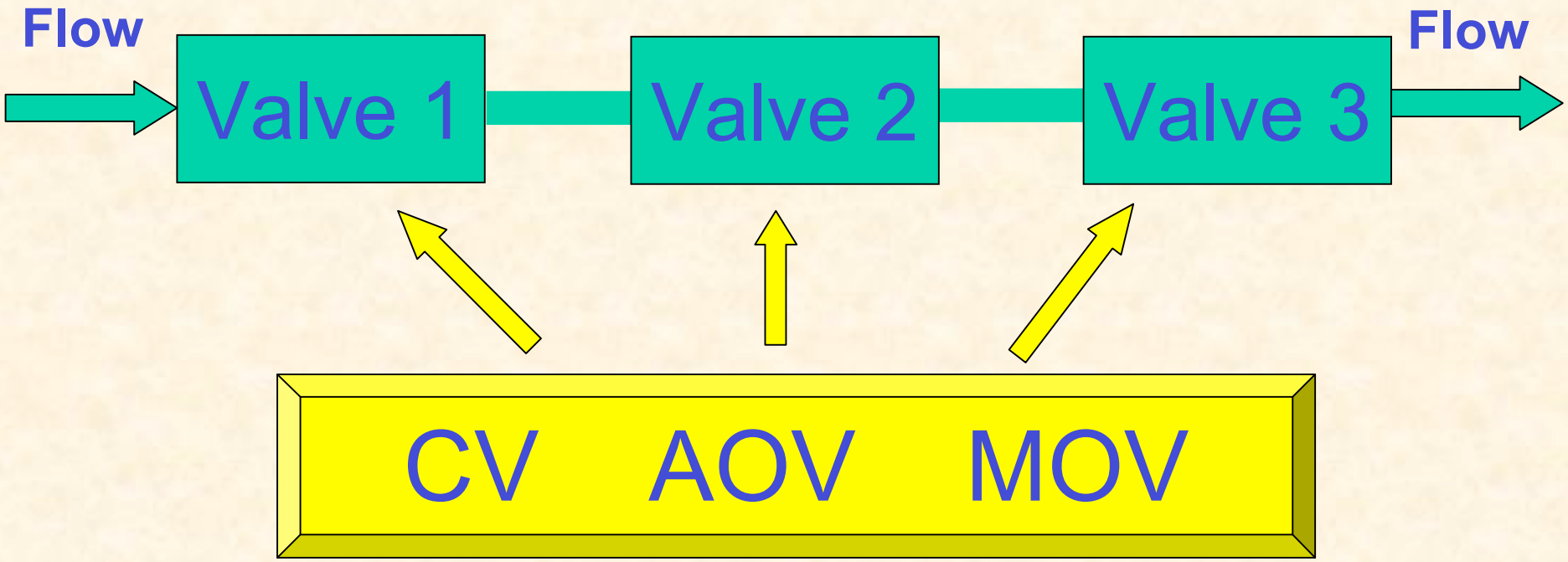


A fire, flood, or seismic analysis inserts a database whereby all components affected (or nonqualified) are assumed to be failed; the other components fail at their nominal failure rate.

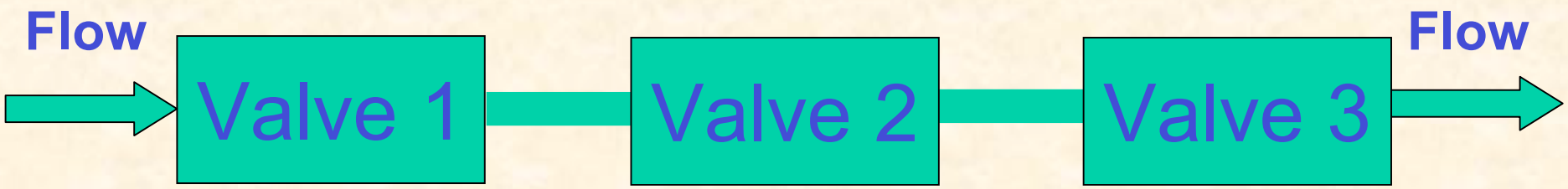
Similarly, maneuverability or fire power for ships, armored vehicles, etc. can be evaluated by inserting a series of databases whereby equipment and support systems in the vicinity of an anomaly are assumed to be failed.

Consider Optimizing an Isolation System with Choices of Control Valves (CVs), Motor-Operated Valves (MOVs), and Air-Operated Valves (AOVs)

- At least one valve must close for the successful isolation of the system

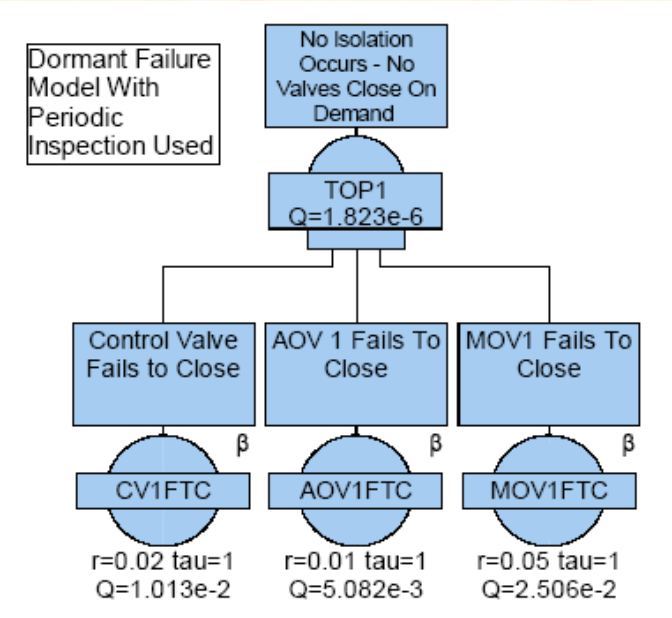


Valves May Be Used in Any Combination Except That Only Zero or One CV May Be Used for Any Option; This Results in Seven Possible Valve Combinations



Valve options using one CV				Valve options without using a CV			
Option	Valve 1	Valve 2	Valve 3	Option	Valve 1	Valve 2	Valve 3
1	CV	MOV	AOV	4	AOV	AOV	AOV
2	CV	MOV	MOV	5	AOV	MOV	MOV
3	CV	AOV	AOV	6	MOV	AOV	AOV
				7	MOV	MOV	MOV

Using a Graphical Interface with *FaultTree*+ Allows Users to Model, Change, and Evaluate the Design Options Quickly



Valve	Failure rate (per year)	Beta factor (failure to close)
MOV	0.04	0.02
AOV	0.01	0.10
CV	0.02	0.05
CV to AOV or MOV	CCF	0.01
AOV to MOV	CCF	0.01

These values are used for illustration purposes only.

Option 1 of the 7 *FaultTree*+ library models available to the graphical interface in the sample problem

Alternate Values for the Failure Rates and Beta Factors Can Be Added to the Library to Evaluate the Sensitivity of the Results

Any New Design or Design Upgrade Would Benefit Greatly From Using RBOT and *FaultTree*+

- RBOT allows hundreds of design alternatives to be easily evaluated and compared.
- Logical decisions for optimizing a system—without actually evaluating it—may in fact be the wrong decision.
- Insights and lessons learned from RBOT helped the IRIS design / PRA team achieve a 2 order-of-magnitude reduction in the base case core damage frequency. (While undergoing design certification by the NRC, the AP1000 design changed based upon insights and lessons learned from IRIS.)

For information about RBOT contact

Mike Muhlheim
865-574-0386
muhlheimmd@ornl.gov

For information about *FaultTree*+ contact

Jeremy Hynek
949-798-6114
jhynek@isographdirect.com