Identifying Risk Drivers Early in a Design

Nuclear Facilities Safety Meeting

Michael D. Muhlheim, Ph.D.
Donald L. Williams, Jr.

February 2, 2006

OAK RIDGE NATIONAL LABORATORY
U. S. DEPARTMENT OF ENERGY

UT-BATTELLE

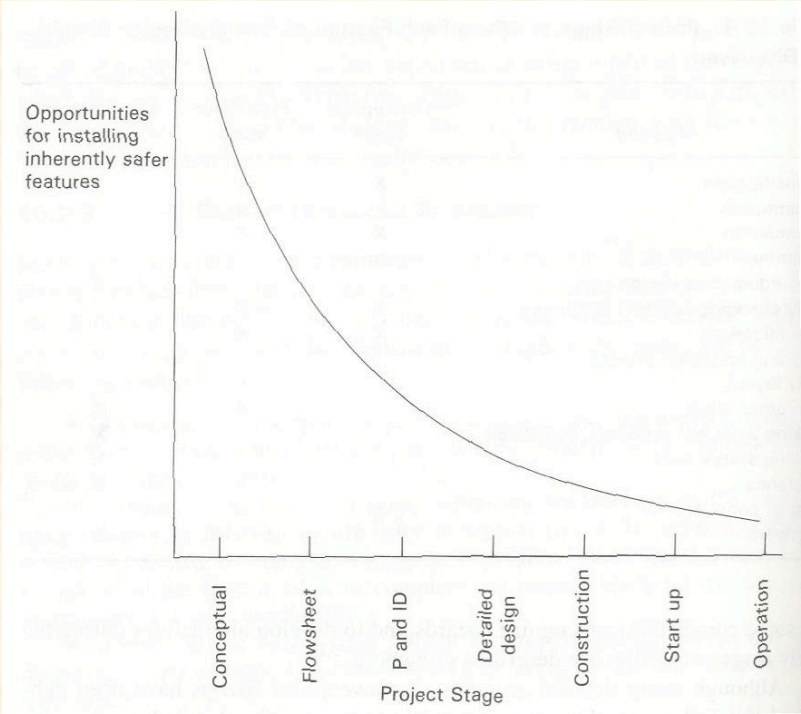
Preventing or Mitigating Undesirable Consequences of Postulated Accidents is One of the Most Important Cornerstones of Safe Operations at DOE Facilities

- The DOE complex contains some 34 sites with about 3500 nuclear facilities located in 13 states*
- Many facilities are old and deteriorating*
- DOE's nuclear facilities contain multiple hazards for workers, the public, and the environment*

*Source: *Improving Regulation of Safety at DOE Nuclear Facilities*

A Safety Analysis shall be Performed at the Earliest Practical Point in Conceptual or Preliminary Design (DOE O 420.1)

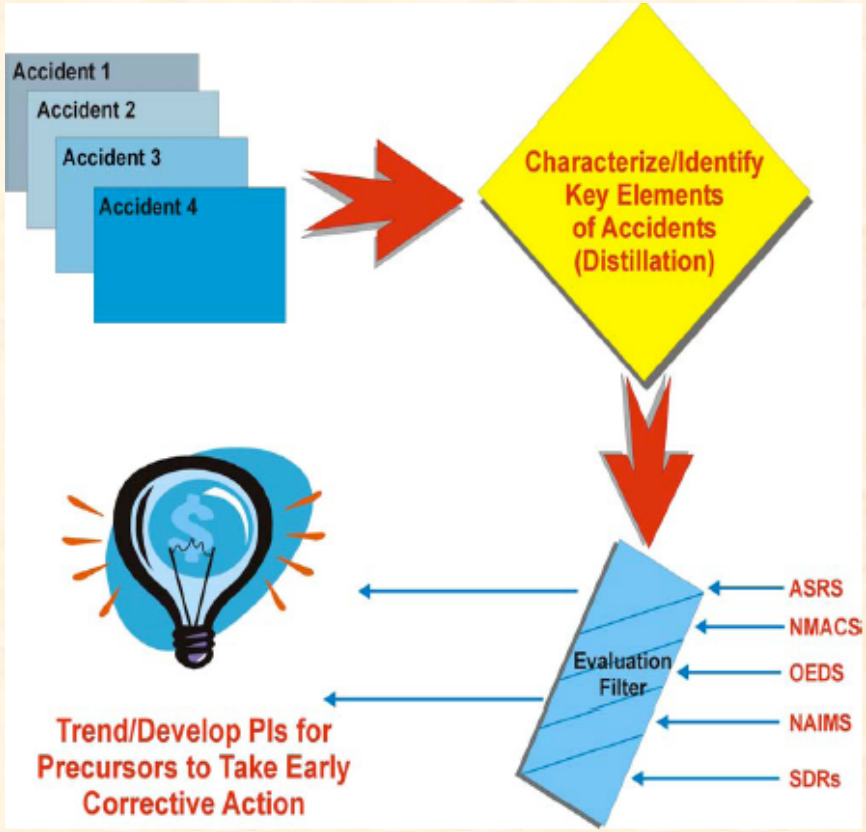
- If it costs $1 to fix a problem at the conceptual stage, it will cost
  - $10 at the flow sheet stage
  - $100 at the line diagram stage
  - $1,000 after the plant is built
  - > $10,000 to clean up the mess after an accident



Source: *Plant Design for Safety, a User-Friendly Approach*

Activities Considered Normal Before an Accident are Often Identified in Hindsight as "an Accident Waiting to Happen"

- Hazards analysis
- Accident analysis
- Lessons learned
- Performance indicators
- Root cause analysis
- Workshops, conferences
- Across industry



Decisions About Safety should be an Integral Part of 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.

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

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

- **Optimization also requires coordination between designers and analysts**

Many Times, what is Perceived to be True is Different from what is Actually True

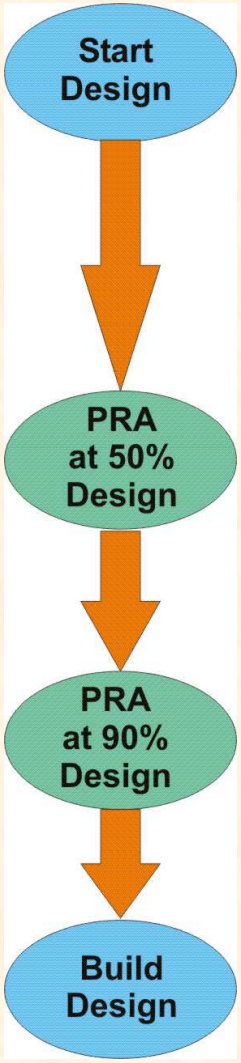
- It is more likely that you will be bitten by
  - a person
  - wild rat
  - squirrel

  than by a shark.

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

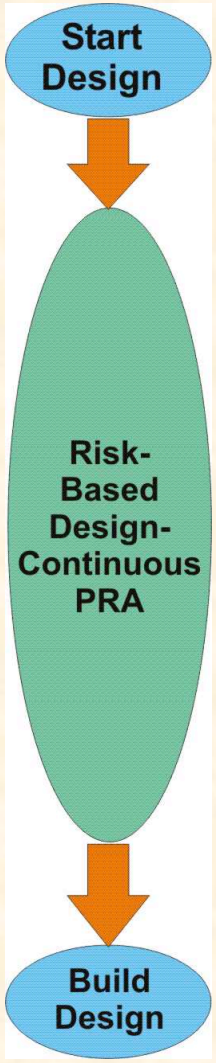
  than by a shark.

Source: Florida Museum of Natural History



The Safety Analyses are Typically Developed at Specific Design "Freeze Points"

ORNL's Risk-Based Design Optimization Tool (RBOT) Allows Designers to Reduce, Control, or Eliminate Risk by Quantitatively Identifying Risk Drivers as the Design Develops



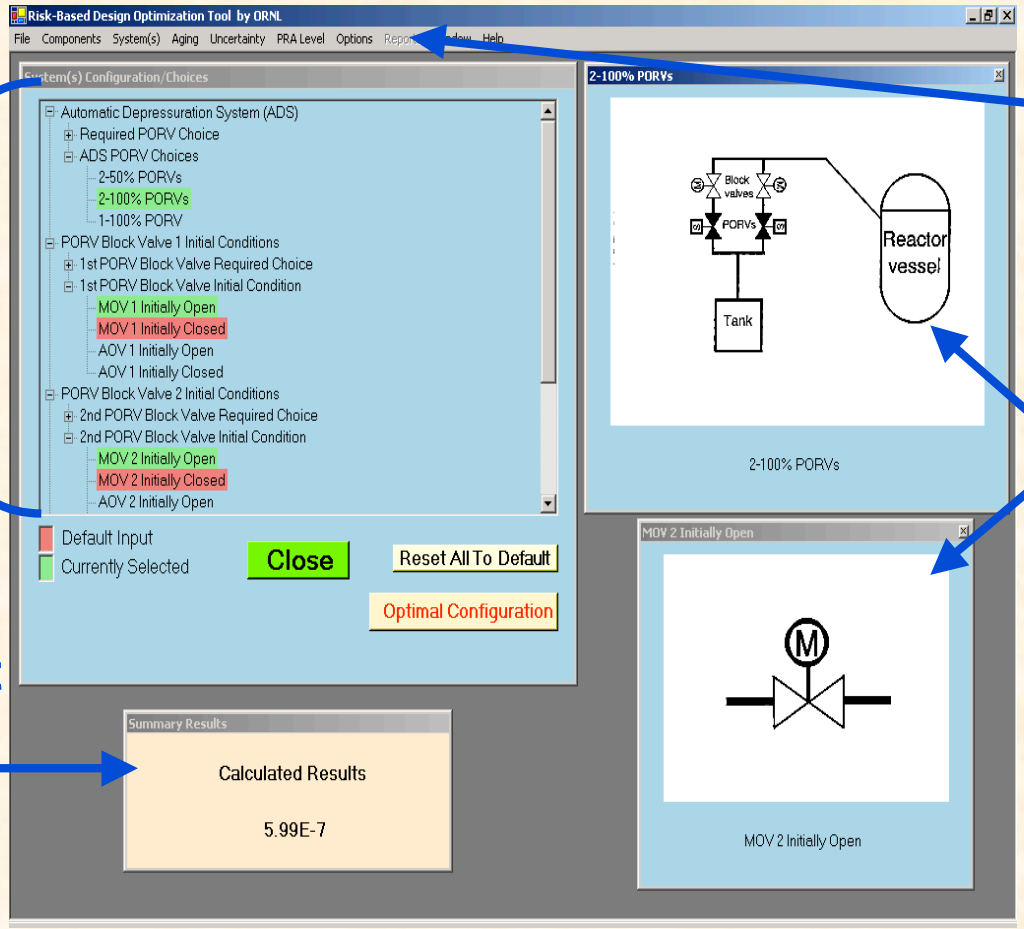
Any Fault Tree Created Using RBOT is the Same as that which would Result if those Choices were the Original Design

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 chosen

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



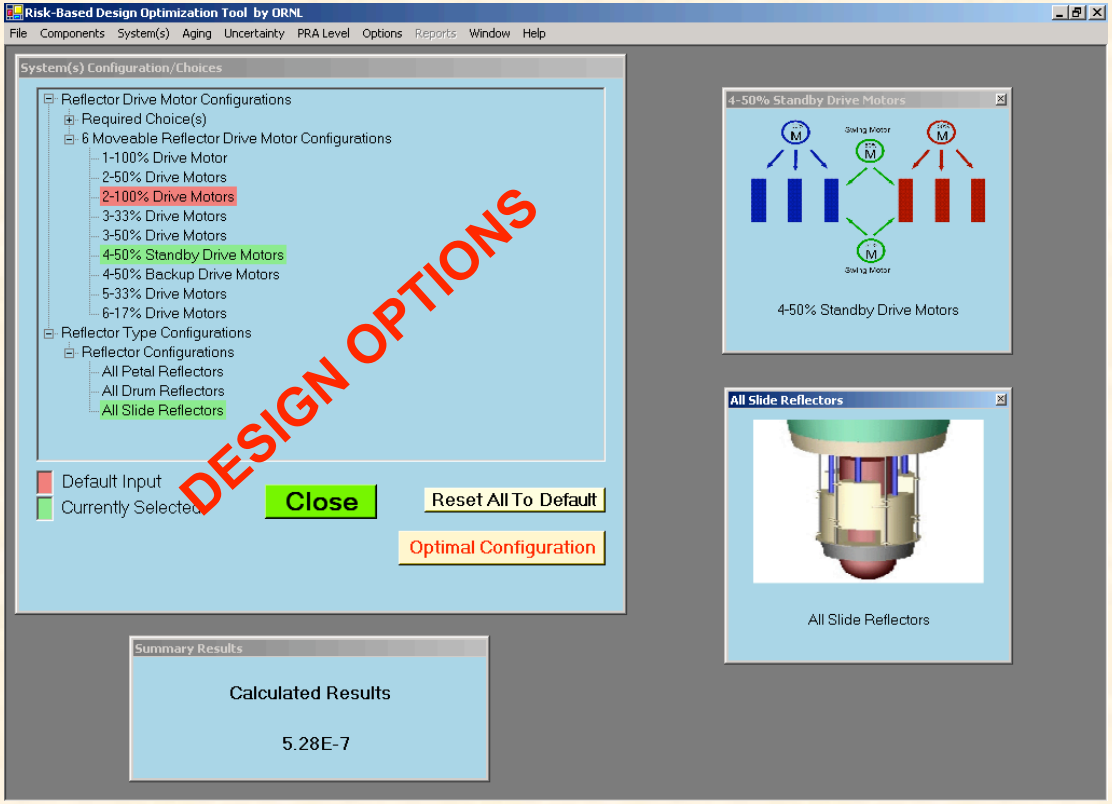
RBOT is Effective in Reducing Design Cycle Time and Improving System Reliability

Design Trades

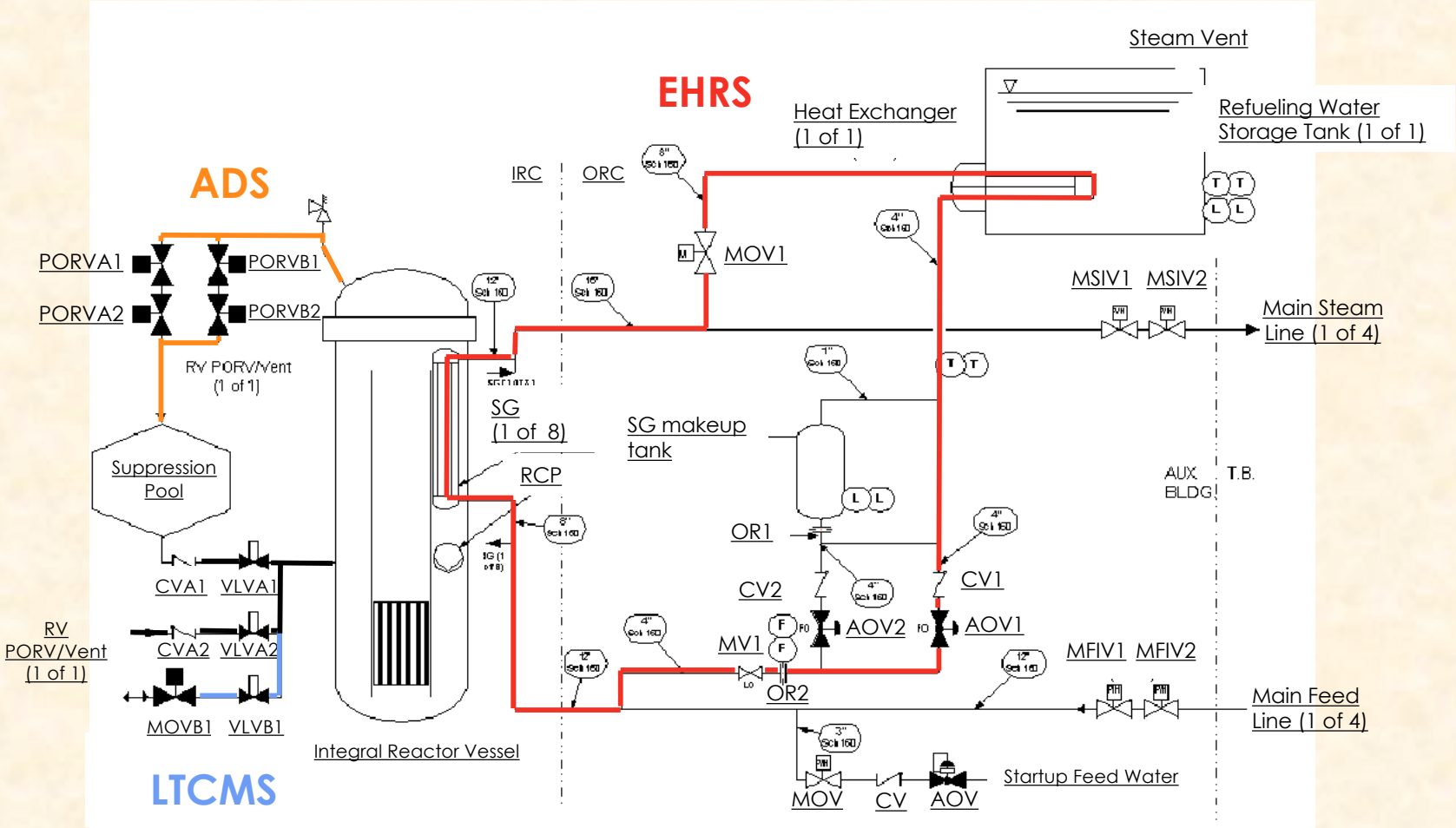
- Component choices
  - Type
  - Position
  - Failure data
- System architecture

Figures of Merit

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

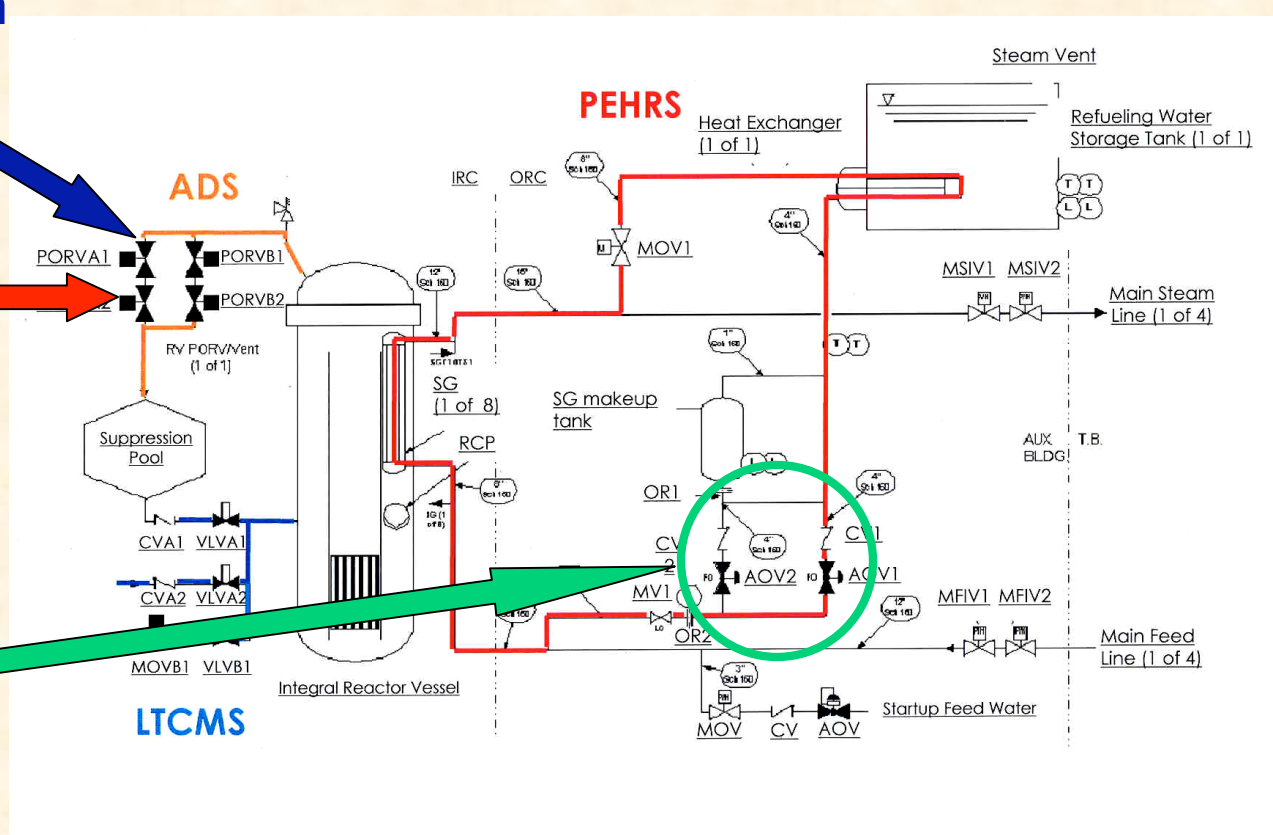


RBOT was Used to Identify the Optimal Designs of the IRIS Safety Systems

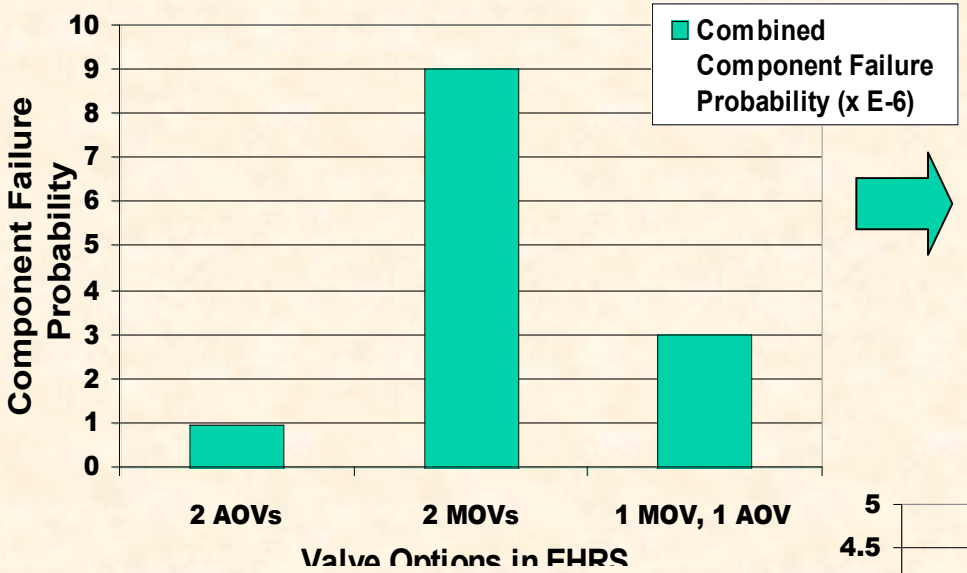


The 11 Component Choices Yield 160 Design Alternatives

- **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**

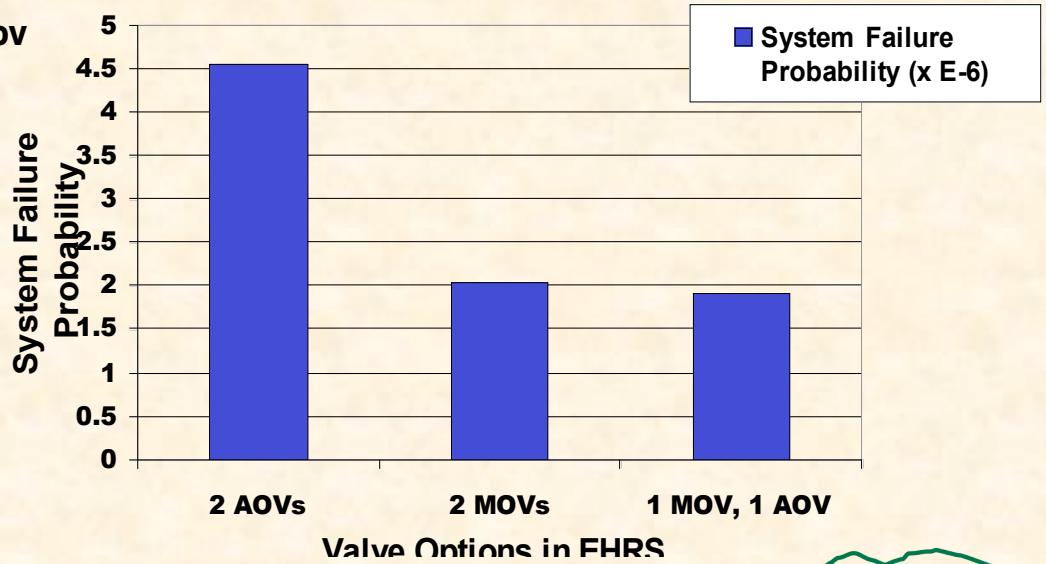


"Logical" Decisions for Optimization may be Wrong



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

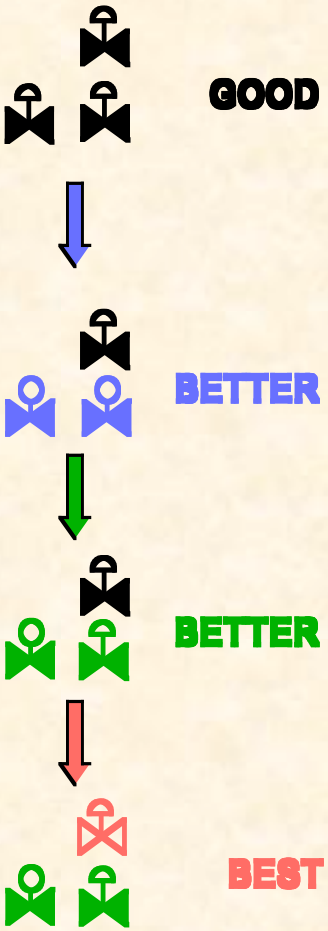
The use of the most reliable valves resulted in the most unreliable system!



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 the System can be Improved

BASE CASE
ADS block valves closed
Valves in EHRS are AOVs



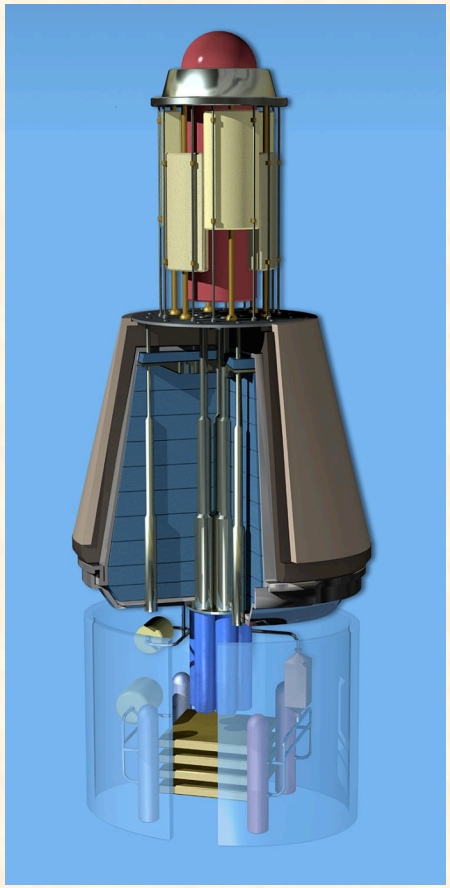
Valves in EHRS changed to MOVs
CCF of valves reduced by a factor of 20!

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

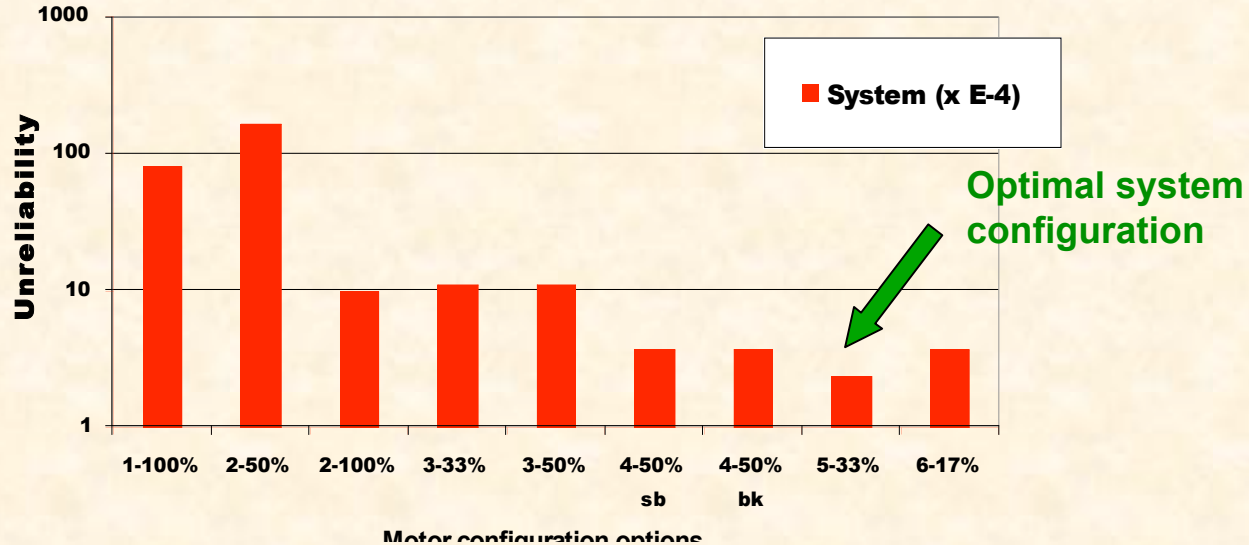
ADS block valves changed to open
CCF of block valves no longer a contributor!

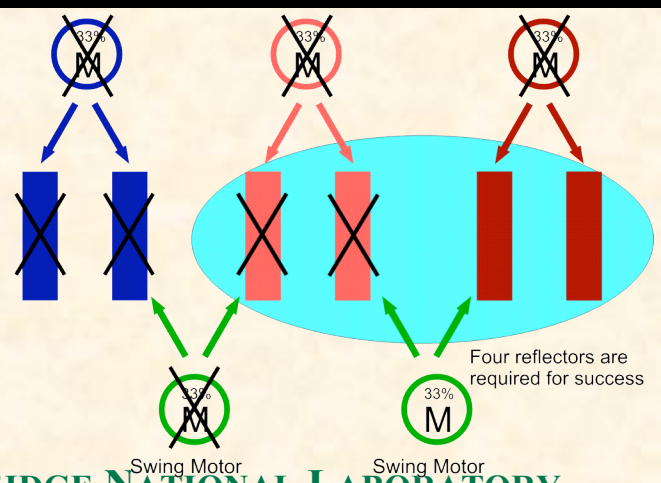
Consider the Following Example of Optimizing the Number of Reflector Drive Motors on an SP-100 Type Reactor

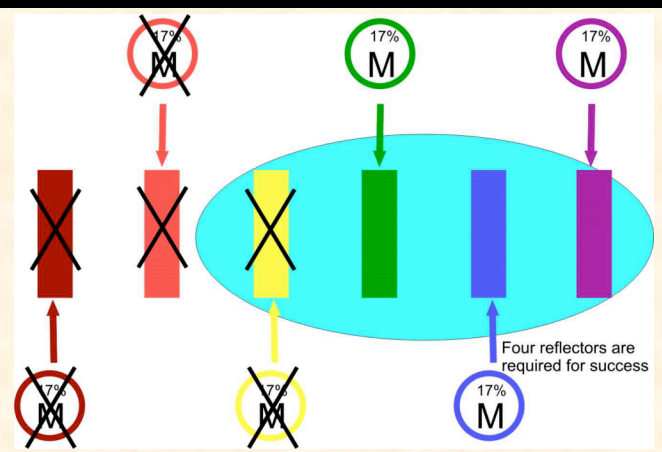
For the space reactor to achieve a critical state, 4 of the 6 reflectors must move to their "in" position.



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

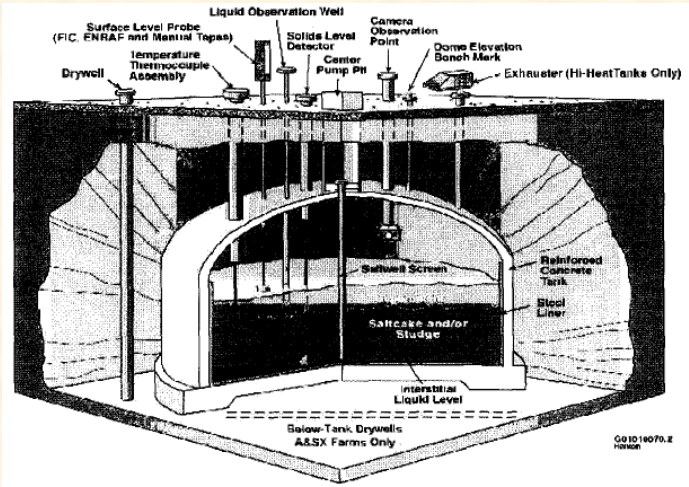


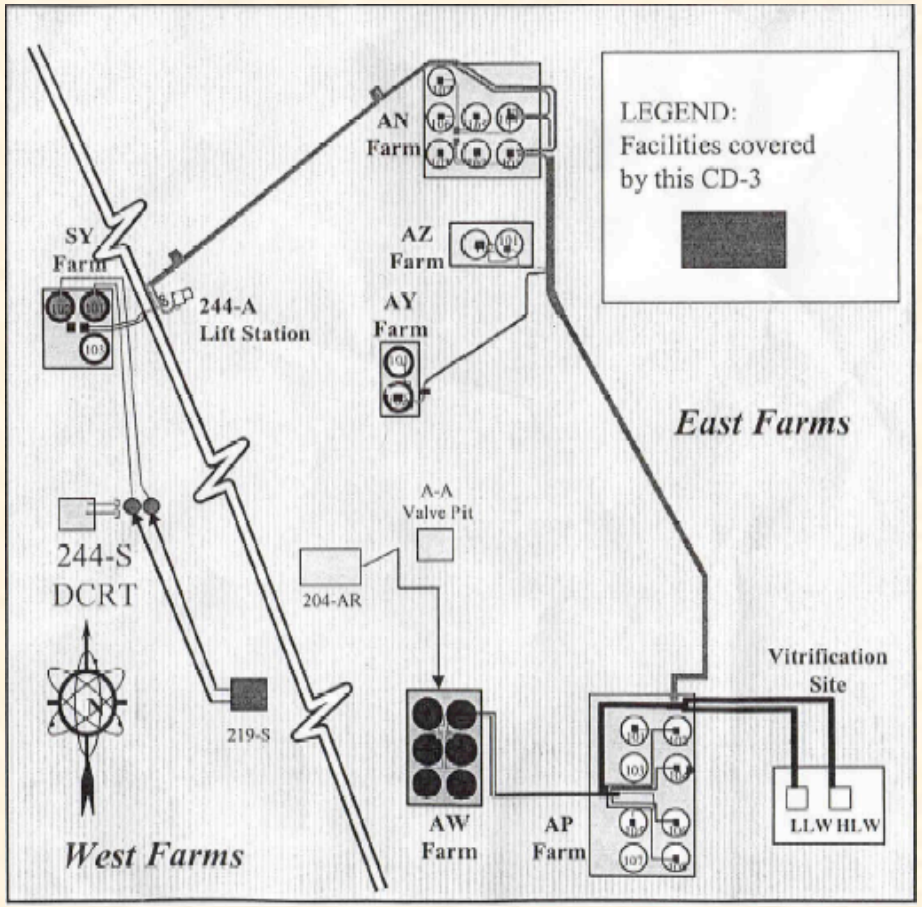




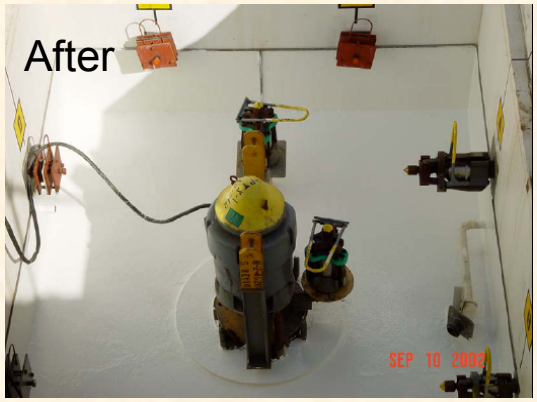
RBOT can be Used to Evaluate the Safety Performance, Good Practices, and Lessons Learned at DOE Facilities

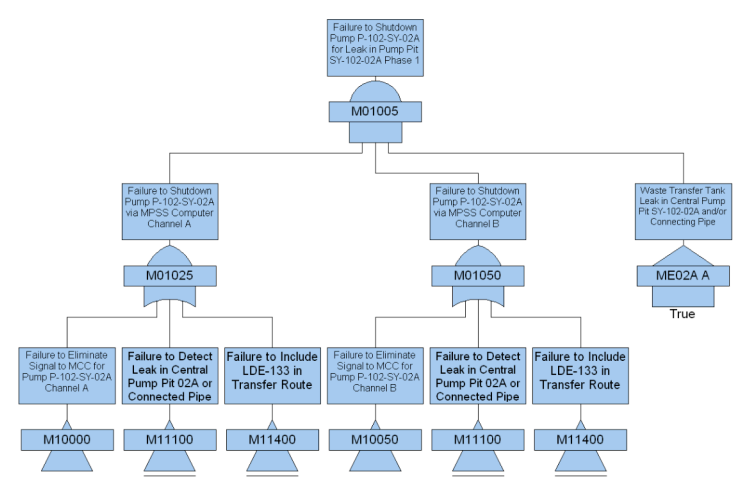
The master pump shut-down system at Hanford is undergoing a 2-phase upgrade for transferring waste between tanks

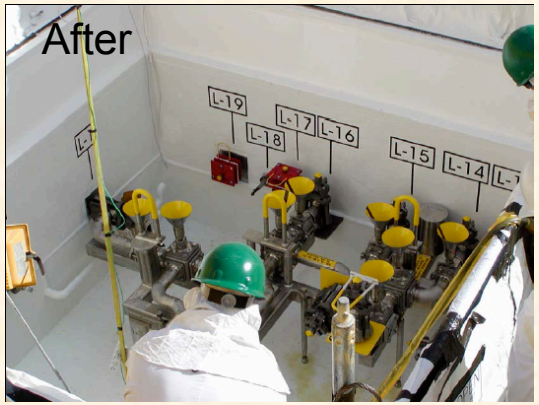




A Risk Assessment of the Master Pump Shutdown System Identified the Failure to Stop the Transfer Pump Given a Leak as the Most Likely Cause of System Failure (Phase 1)



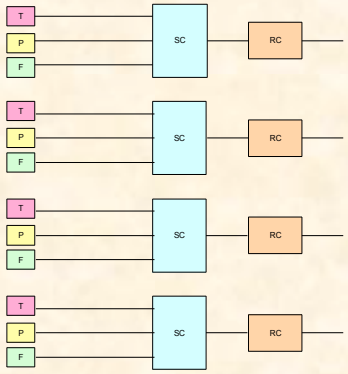




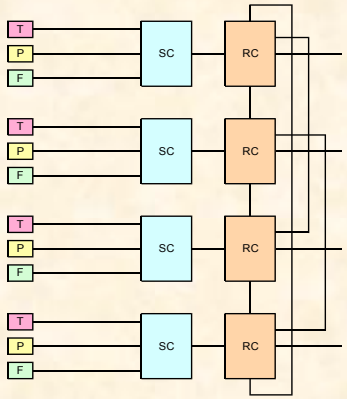
Source: *Failure and Reliability Analysis for the Master Pump Shutdown System*

RBOT Allows Alternative System Architectures to be Analyzed Against a Baseline Design

- Alternative methods to stopping a pump given a leak
  - Redundant relay contacts in series
  - Timer in relay circuit
  - Independent signal from redundant leak detection method
  - Independent sensor inputs with cross-linked controllers
- Redundant leak detection methods to consider
  - Flow meters on the incoming and outgoing transfer lines
  - Gamma radiation probes in pump pits
  - Interstitial monitoring between the inner and outer shell of the double-walled tanks and pipes
  - Vapor monitoring in the soil
  - Visual surveillance (human and/or video)



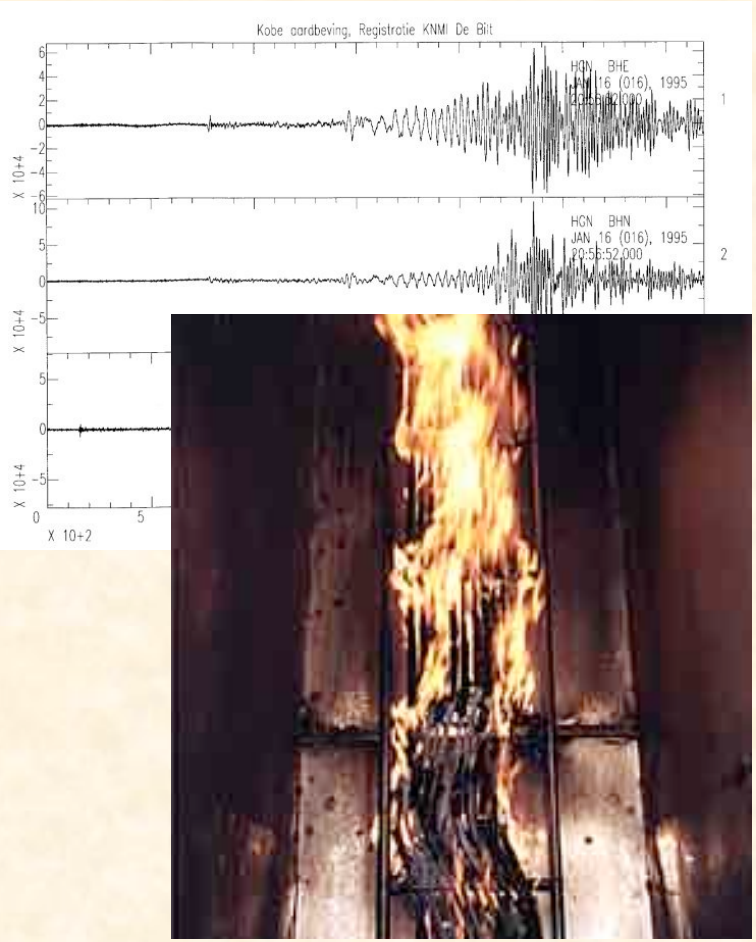
Independent sensor inputs and control outputs



Independent sensor inputs to cross-linked controllers

RBOT can be Expanded to Simultaneously Evaluate External Events as the Design Progresses

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.



Any New Design or Design Upgrade would Benefit Greatly from Using RBOT

- 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 have achieved tangible risk reduction results in the designs of commercial and DOE-sponsored nuclear systems.
- Watch for sharks, but understand that other less obvious risks may be lurking just beneath the surface!