

Selected Examples of Design Optimization Using RBOT and FaultTree+

M. D. Muhlheim and J. W. Cletcher, II; Oak Ridge National Laboratory; Oak Ridge, TN 37831

S. Flanagan and J. L. Hynek; Isograph Direct; Newport Beach, CA 92660

R. Stack; Dow Chemical; Hillsdale, MI 49242

Abstract

Probabilistic risk assessment (PRA) is an analytical method used to estimate the probability of failure of a system and to determine what the most likely contributors are to that failure. Space, nuclear, medical, and defense industries are among those that have used PRA methods for assessing risks and/or reducing the costs in designing, upgrading, manufacturing, assembling, and operating components, systems, or facilities. When applied at an early stage of a project, PRA can be a valuable design tool. Current PRAs, however, are generally performed to demonstrate safety and are often unsuited for applications aimed at making design or operating decisions. Unlike conventional PRA tools, users of *FaultTree+* have been developing programs that allow PRA analysts and designers to easily determine the probabilistic implications of different design configurations and operating conditions in various combinations to reduce, control, or eliminate risk by quantitatively identifying risk drivers as the design develops. A program being developed by the Oak Ridge National Laboratory (ORNL), coupled to *FaultTree+*, allows users to evaluate design changes; new modeling approaches, methods, or theories; modeling uncertainties and completeness; physical assumptions; and data changes at the component, cabinet, train, system, and facility level. Because each “new” plant configuration may or may not improve safety or may marginally improve safety at great cost or operational flexibility, all previous design alternatives are retained to maximize the benefits of a risk-based design. The power of the one-button architecture developed by ORNL becomes evident by the number of design alternatives that can be evaluated—for one design, 11 component choices in 2 safety systems yielded 160 design alternatives. More importantly, because of the ease in evaluating alternate component or system arrangements, dramatic increases in reliability were observed with atypical, unusual, or simply different design configurations compared to the designs using “proven” reliability design practices. In addition, the lessons learned can be counterintuitive and significant. For example, one of the design alternatives evaluated using the one-button architecture program revealed that in some instances, using more reliable components actually decreased the plant’s reliability. The impacts from external events, such as seismic or fire events at nuclear power plants, explosions on military craft, or large vibrations from launch vehicle liftoff, can be evaluated simultaneously with internal events using the one-button architecture. A chemical plant application by Dow Chemical also shows that fault tree development time can be reduced by coupling a common database with the basic events and subtree logic already available with *FaultTree+*. This allows chemical systems to be evaluated quickly without being labor intensive by leveraging prior studies and data. As exemplified by the reduction in risk and increase in safety, any new design or design upgrade would benefit greatly from using these cutting-edge risk tools.

Introduction

Probabilistic risk assessment (PRA) is an analytical method used to estimate the probability of failure of a system and to determine what the most likely contributors are to that failure. Space, nuclear, medical, and defense industries are among those that have used PRA methods for assessing risk; increasing safety margins and optimizing costs in the design, fabrication, construction, testing, and operation of components, systems, and facilities.

When applied at an early stage of a project, PRA can be a valuable design tool. Current PRAs however, are generally performed to demonstrate safety and are often unsuited for applications aimed at making design or operating decisions.¹ In making design decisions, if comparisons are made using simplified fault trees, the models may not accurately represent the system’s functioning or malfunctioning.² Valid design or operation comparisons require detailed assessments. Developing a detailed PRA during the design phase of a project is an iterative process where the models are developed at design “freeze” points. However, as the design matures, the PRA results continue to reflect a previous design and not the current design. An example of the process is

- development of a PRA model,
- use of the model to identify weaknesses,

- quantification of PRA benefits of alternate design and operational strategies, and
- adoption of selected design and operational improvements.

This process was followed by Westinghouse during the design of its AP600. As expected, the scope and detail of the AP600 PRA model increased as the plant design matured. Although the iterative process resulted in a number of design and operational improvements, the process spanned five stages and six revisions.^{3,4}

This iterative process can continue throughout the design cycle and into the certification process. For example, when considering the final design approval for the CE System 80+ reactor containment design, the Nuclear Regulatory Commission (NRC) requested that the designers evaluate design alternatives that would help mitigate the consequences of severe accidents.⁵ Sixty-three design alternatives were considered, and twenty-seven were quantified. This back-end approach is expensive and time-consuming. A much better approach would be to use a dynamic PRA coupled to the design to reduce, control, or eliminate risk by quantitatively identifying risk drivers as the design develops.

Westinghouse, in its design of the International Reactor Innovative and Secure (IRIS) plant, brought the use of a dynamic PRA to reality by using a safety-by-design approach to cover all aspects of safety at the very beginning of the design process.⁶ Rather than evaluate design alternatives on a system-by-system basis, one change at a time, and discarding previous evaluations, the different system and component configurations were evaluated in various combinations for the entire range of initiating events. Thus, unlike other design “optimization” programs, Westinghouse used its PRA program to evaluate different types of plant systems and components, in different operational states, that were interchangeably evaluated as the design progressed. Because each “new” plant configuration may or may not improve plant safety or may marginally improve safety at great cost or operational flexibility, all previous design alternatives were retained to maximize the benefits of a risk-based design. More importantly, because of the ease in evaluating alternate component or system arrangements, dramatic increases in reliability were observed with atypical, unusual, or simply different design configurations compared to the designs using “proven” reliability design practices. This contributed greatly in a two order-of-magnitude reduction in the base-case core damage frequency for IRIS. The design lessons learned from the dynamic PRA for IRIS were then applied by Westinghouse to the AP1000 even though it was undergoing design certification review by the NRC.⁷

Innovative Approaches to Probabilistically Evaluating Alternative Designs

As part of its safety-by-design approach and commitment to reduce the core damage frequency to as low as realistically possible for its IRIS plant, Westinghouse had many team members focused on safety and reliability. One of the team members was the Oak Ridge National Laboratory (ORNL); its task was to develop a one-button architecture that would allow components, modules, and data to be interchanged at will with the probabilistic effect immediately apparent. ORNL’s program, called risk-based design optimization tool (RBOT), is coupled to *FaultTree+* and allows users to evaluate design changes; new modeling approaches, methods, or theories; modeling uncertainties and completeness; physical assumptions; and data changes on component, cabinet, train, system, and facility bases.

With RBOT, changing the design is as simple as picking one of the design alternatives from a scroll-down menu (Fig. 1) that have been developed by PRA analysts. The default (base case design) and currently selected design options are highlighted; graphical displays provide additional indicators of the option(s) chosen. With the scroll-down menu, many design alternatives, including unconventional alternatives, can be easily evaluated. If additional

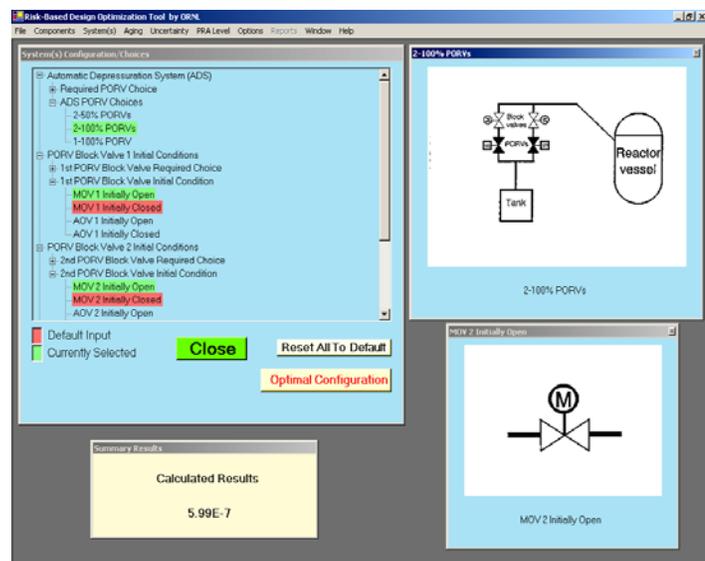


Fig. 1. ORNL’s RBOT allows users to choose design alternatives from a scroll-down menu.

design alternatives are desired and are not available in the scroll-down list of options modeled in RBOT, they can be easily created by a PRA analyst and added to the scroll-down list. The basic RBOT computer program in development automatically inserts the correct fault tree module(s) for the design configuration chosen into the PRA model in *FaultTree+*,⁸ maintains any links to event trees (if used), relinks the correct support systems, adjusts the common-cause failure probabilities on the train and system levels, and accounts for changes in recovery actions and human error probabilities. *FaultTree+* then recalculates the parameters of interest for the entire spectrum of initiating events, and transmits the results back to RBOT. The resulting fault tree is the same as that which would result if those choices were the original base case. Any or all of the design options can be made in any order using RBOT. Because all choices remain available, no information is lost and the design can be returned to any previous state.

Because all of the current and previous design, modeling, and data sets are available via the one-button architecture, the safety ramifications of design options are evaluated very early, feedback on design alternatives is immediate, and true optimization of the plant design can be achieved. Thus, even with complicated systems and alternatives, designers can not only observe if the system is more reliable, but can also understand *why* the system is better or worse.

Selected Examples of Design Optimization Using RBOT and *FaultTree+*

IRIS: The IRIS design is aimed at achieving four major objectives: proliferation resistance, enhanced safety, economic competitiveness, and reduced waste. The safety approach of Generation II reactors [current nuclear power plants (NPPs)] can be defined as coping with accidents/consequences by active means, while the improved approach of Generation III reactors (e.g., AP600) is coping by inherently safer passive means. The design of IRIS, a next-generation NPP, promotes safety to the next level through safety-by-design that eliminates most accident initiators while the consequences of other accidents are rendered acceptable.⁹

Figure 2 shows the safety systems for the IRIS reactor. The two systems that were evaluated using RBOT were the automatic depressurization system (ADS) and the emergency heat removal system (EHRS). The ADS is a pressure relief system with two parallel trains for blowing down into the suppression pool. There are four trains of emergency heat removal. The number of trains required for operation are dependent upon the initiating event and varies from 2–4. The EHRS is a natural circulation system that removes heat via the steam generator. The flow path is from the steam generator, to the refueling water storage tank, through a main and/or bypass leg, back to the steam generator.

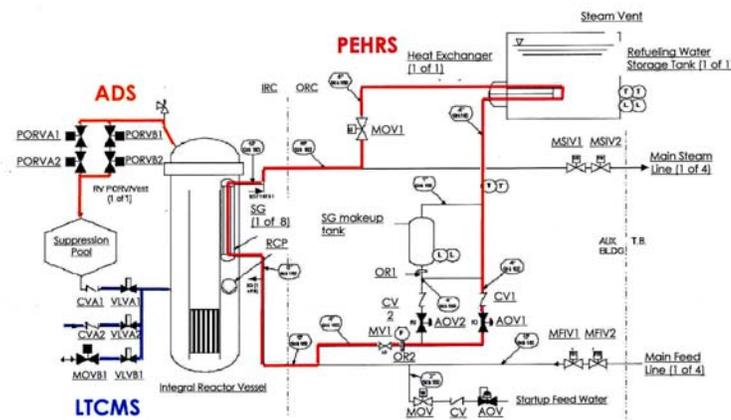


Fig. 2. Safety systems for the IRIS reactor. (PEHRS is the passive emergency heat removal system, ADS is automatic depressurization system, and LTCMS is the long-term core makeup system).

A collection of design alternatives for various systems for IRIS were identified through the review of current and Generation III NPP designs. For example, a review of operating NPPs showed that typical relief systems (similar to IRIS's ADS) consist of one or two trains. Generation III NPPs have more complex systems such as two trains with four stages of pressure relief. Further review shows that the block valves for the power-operated relief valves (PORVs) may be initially open or closed. (The block valves are used to prevent a loss-of-coolant accident given a stuck open PORV. However, a block valve that fails to open will prevent depressurization of the primary system. Thus, a trade-off exists between having the block valves open or closed.) When a system arrangement, component type, component position is chosen from the menu, RBOT automatically changes the fault tree in *FaultTree+* to reflect that choice. The following choices were made available in RBOT for optimizing the ADS:

- the choice of block valves and PORVs were air-operated valves (AOVs) and motor-operated valves (MOVs) (other type valves could have been added at any time),
- the initial position of the block valves (AOVs and MOVs) could be open or closed,

- the number of trains for pressure relief could be 1 or 2, and
- the capacity of each valve, whether AOV or MOV, could be 50% or 100% (i.e., able to accommodate 50% or 100% of the maximum steam flow required for successful depressurization of the primary system for the design basis accidents).

The base case level-1 PRA for IRIS evaluated using RBOT included 4 event trees with the following initiating events (IEs): a primary system loss-of-coolant accident, a steam generator tube rupture, a secondary system pipe break, and a loss of offsite power. The mitigating systems necessary to prevent core damage for these IEs are represented by 11 fault trees that cover subcriticality of the reactor, primary system depressurization, and long- and short-term heat removal. Choosing any of the options developed and made available via RBOT provides users with a PRA that is the same that would be developed if that were the base case model. Again, because all previous choices are still available, the design can be returned to any state, at any time, in any order.

In this example, the one-button architecture allowed designers to evaluate 40 unique design alternatives of the ADS for the 8 design choices given above. However, simply providing design alternatives is not beneficial unless various metrics of interest can be compared, improved, or optimized. Using this example, evaluating the failure modes for the different design options provides clues on how the system could be improved. By clicking a single “button” to change the design of the system, designers learned that for those events requiring pressure relief that

- with only one block valve, the initial position of the block valve does not matter—failures of the PORV(s) dominate the reliability of the system;
- 2 PORVs, each with a 50% capacity rating (i.e., 2–50% capacity), do not provide sufficient redundancy and are in fact worse than having just one PORV because the failure of either PORV/block valve arrangement causes the system to fail;
- true redundancy (2- vs 1-100% capacity valve) improves reliability by an order of magnitude and not the square of the PORV’s failure probability because of shared systems and components;
- for those events requiring pressure relief, it is 4–6 times better to have the block valve initially open, where it has to spuriously transfer to the closed position than to have it initially closed and having to open. (For many system arrangements, the dominant contributor to system failure is the CCF probability of the block valves to open. The simplest way to reduce the CCF probability of the block valves’ failing to open is to have the block valves already open.), and
- for the ADS, it is observed that having the block valves originally open improves system reliability 20% and reduces the core damage frequency 3.5%. Once this CCF probability of the block valves failing to open is eliminated, the type of block valve (e.g., MOV or AOV) is inconsequential.

The other safety system evaluated using RBOT was the EHRS. Identifying design alternatives for the EHRS was a challenge because it was already a pretty elegant system in its simplicity. The original design used natural circulation cooling (i.e., no pumps), and only 1 of the 2 AOVs needed to open to start the system. In fact, the designers purposefully used the most reliable valves they could—the AOVs. As such, identifying design alternatives for the EHRS was not originally considered because of the simplicity of the existing system design.

With RBOT, the number of trains in a system, or even component type or position—alternatives that would not normally be evaluated—were evaluated because of the ease of changing out components, adding trains, etc. This is contrary to typical alternatives that focus on big changes such as number of trains and cross-ties between trains (although these can also be easily evaluated using RBOT).

Because AOVs have the best reliability characteristics for active valves, it was expected that their use would result in the most reliable system. With the ease of evaluating different components and their arrangement, RBOT was used to change one or both of the AOVs to MOVs for each train of the EHRS. Changes automatically made by RBOT to the *FaultTree+* model for the valve options included

- changing the selected component(s) from AOV to MOV (or vice-versa if changing from MOV to AOV),
- changing the support system for those components from instrument air to electric power (or vice-versa if changing back to AOVs),
- changing the CCF probabilities on the train level, and

- changing the CCF probability on the system level (4 trains).

Surprisingly, using the “better” valves actually made the system (and thus the plant) worse. Using the more unreliable MOVs actually improved system performance. This is because the CCF probability for the AOVs failing to open is larger than that for the MOVs, and the CCF probability of the valves was the largest contributor to system failure. Although the MOVs significantly improved the system, using a mix of AOVs and MOVs provided the most reliable system. In fact, a mixed-valve system improved system reliability by 42%; the core damage frequency was reduced by 23%.

Surprisingly, the relatively few component choices for the ADS and EHRS resulted in a very large number of design alternatives. The 11 component choices—component type, position, and capacity—resulted in 160 design alternatives. The one-button architecture allowed all of these alternatives to be evaluated probabilistically with ease and provided designers with insights into system behavior.

With the wealth of information available through the one-button architecture, design alternatives can now begin to consider production, operation, and maintenance costs. For example, if the use of a mixed-valve system significantly increases operation and maintenance costs, a decision could be made to maintain all MOVs in the EHRS because system unreliability would not increase appreciably. Thus, for the first time, plant reliability and other attributes, such as cost, can be optimized simultaneously.

Reflector Control Segments for a Space Reactor: Because of renewed interest in space reactor power systems, ORNL used its RBOT program to evaluate the reliability of design alternatives for the reflector controls of an SP-100 type reactor (Fig. 3). The SP-100 was being developed using a lithium-cooled fast spectrum fission reactor with uranium nitride fuel that would have produced 100 kW of electricity. Three mission profiles were under consideration:¹⁰

1. a high-altitude (>300-year orbital lifetime) mission, launched by a Titan IV launch vehicle, boosted by chemical upper stages into its operational orbit;
2. an interplanetary nuclear electric propulsion mission, started directly from a Shuttle parking orbit; and
3. a low-altitude (50-year orbital lifetime) mission, launched by the Shuttle and boosted by a chemical stage to its operational orbit, with subsequent disposal boost after operation.

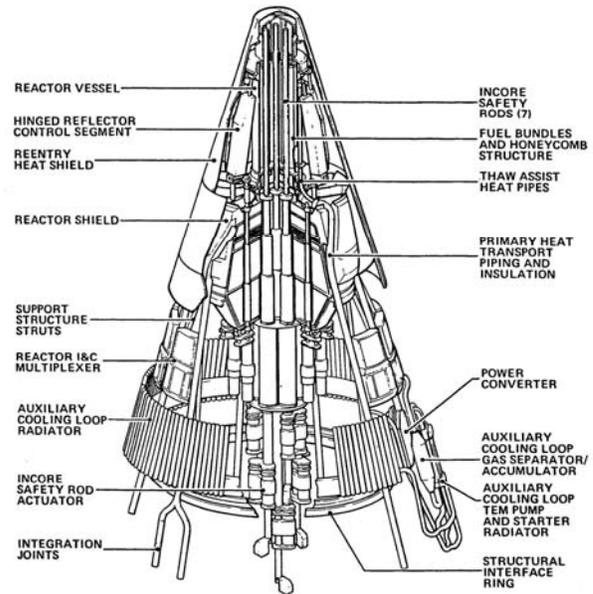


Fig. 3. SP-100 reactor power assembly.

Reactivity of the reactor was to be controlled by 12 reflector elements, with additional shutdown margin provided by 7 internal safety rods. To operate successfully, four of the six movable reflector elements in the reflector control system had to move to ensure startup and shutdown (after the safety rods are withdrawn). Three types of reflectors are typically considered for space reactors—petal, drum, and slide reflectors. Petal reflectors are hinged reflectors, drum reflectors rotate, and slide reflectors move up and down. When the reflectors are in their “in” position, they surround the reactor core and reflect the neutrons back into the core, thereby sustaining the chain reaction. Nine motor/reflector arrangements were evaluated using RBOT that ranged from one motor moving all six reflectors to six motors, one for each reflector. The motor-reflector arrangements evaluated were:

- 1–100% motor: one motor operates all six reflectors,
- 2–50% motors: two motors where each motor operates a bank of three reflectors, one motor is a swing motor that can operate either bank of three reflectors,
- 2–100% motors: each motor can operate all six reflectors (i.e., 100% backup),
- 3–33% motors: each motor operates a bank of two reflectors,

- 3–50% motors: two motors where each motor operates a bank of three reflectors, one motor is a swing motor that can operate either bank of three reflectors,
- 4–50% motors: two motors where each motor operates a bank of three reflectors, two backup motors that can operate one bank of reflectors,
- 4–50% motors: two motors where each motor operates a bank of three reflectors, two swing motors that can operate either bank of reflectors,
- 5–33% motors: three motors that each operate a bank of two reflectors, two swing motors that each can operate one of two banks of reflectors, and
- 6–17% motors: six motors that each operate one reflector.

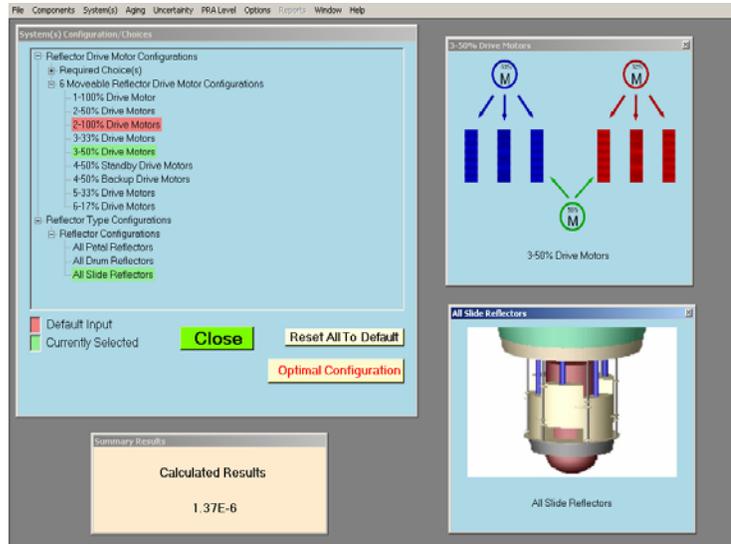


Fig. 4. Example of design alternatives for a space reactor power system’s reflector control system.

Because RBOT allows changes to be made easily, all of the motor-reflector arrangements given above were evaluated with the “click of a button” (Fig. 4). Surprisingly, the five-motor configuration was the optimal system configuration. A review of why five motors is the best arrangement for six movable reflectors shows that in the five-motor configuration, four motors must fail for the system to fail (Fig. 5). A similar review of the other reflector motor options clearly shows that any of the other design options require fewer reflector motors to fail for the system to fail. For example, a system with six reflector drive motors—one for each reflector—requires three motors to fail for the system to fail (Fig. 6).

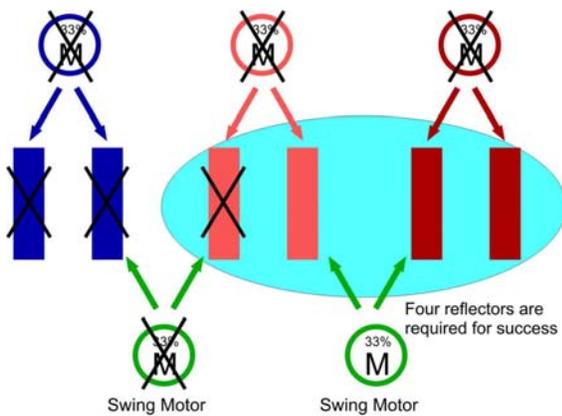


Fig. 5. The five-motor option for the reflector drive system requires the most motors to fail (four) for the system to fail.

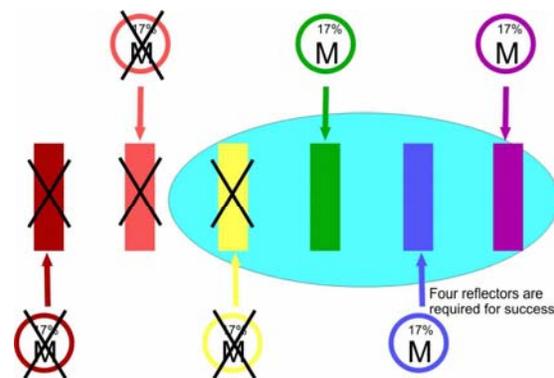


Fig. 6. Any motor option other than the five-motor option for the reflector drive system requires three or fewer motors to fail for the system to fail.

Chemical/Petrochemical Industry Example: In the chemical and petrochemical industry, fault tree analysis is used as a tool for improving new system design, for evaluating design upgrades for existing systems, and determining if systems meet established safety and reliability targets. Work processes such as Six Sigma can use fault tree tools to model the process to assess its safety and reliability capabilities and achieve breakthroughs in new designs. Using *Fault Tree+* with a selection of fault tree modules that represent current best designs for these systems, models of a new design including these standard subsystems can be quickly evaluated.

A simple generic example—a high integrity isolation system involving the use of three valves in series—is used to show how different design options and assumptions provide different results. The design options are to use a control valve (CV), an MOV, or an AOV that fails closed in any combination except that only zero or one CV may be used for any option. This results in seven possible options (ten if there was no restriction on the CV usage) from this simple example (Table 1).

Table 1 Seven design options using zero or one CV

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	AOV	AOV	AOV
				7	MOV	MOV	MOV

Using a graphical interface to model and change out the valves, each of the design options can be quickly checked (Fig. 7). Because library models and data are used, a high level of expertise with the fault tree details is not required. For the example valve options given in Table 1, the data in Table 2 were used to evaluate which valve arrangement given in Table 1 would be the best performing isolation system (the mean time to repair for all seven options was 0.01 years with a test interval of 1 year).

The values for the failure rates and beta factors can be changed to check the sensitivity of the results. This can be done by having alternate values in the library that can be used in the fault tree models. Another variable that can be easily checked is extending the test interval while still meeting the safety targets. If a safety target of 1.0×10^{-5} or less was specified, only three of the configurations would meet the target (Table 3). The common-cause failure contribution (%CCF) is a major factor in all the cases evaluated. These results agree with the IRIS example provided above.

Table 2 Data for valve design options for graphical interface library^a

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

^aNote these values are used for illustration purposes only and should not be taken as actual data.

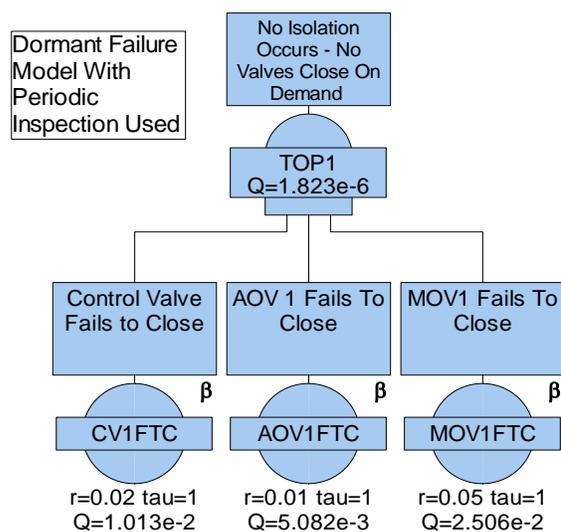


Fig. 7. One of seven *FaultTree+* library models available to the graphical interface in the sample problem.

Table 3 Results for the seven available design options in the graphical interface library

Design option	Unavailability	Contributor to CCF (%)
1	1.82×10^{-6}	70
2	1.16×10^{-5}	44
3	5.46×10^{-6}	94
4	1.34×10^{-5}	95
5	5.80×10^{-6}	44
6	5.08×10^{-4}	99+
7	5.17×10^{-4}	97

The emphasis of this paper is on the ease of use and time savings that can be achieved using the *FaultTree+* program with risk-based design optimization. With the short design timelines in the chemical tool makes what was previously impossible to be possible—design optimization from a safety perspective. In the interest of doing more fault tree studies with less resources, and being better, faster, and less expensive, this is clearly a 21st century analysis method.

Other Uses of a Dynamic Fault Tree

Focusing on reducing the likelihood of internally initiated events could have minimal impact on the overall reliability characteristics of a facility. For example, externally initiated events are often significant contributors to an NPP core damage frequency (CDF).¹¹ Individual plant examinations (IPEs) for current-generation NPPs have shown that the CDF from seismic events are of similar magnitude to or even larger than the CDF from internally-initiated events and that 70% of the plants that performed IPEs proposed plant improvements based on their seismic analysis. In addition, 25% of the IPE external events submittals reported that the CDF from fire exceeds the CDF from internal events. Although none of the 70 IPEs for external events (IPEEE) submittals identified any high wind, flood, or other external-event-related vulnerabilities, one plant lowered its flood CDF by three orders of magnitude by improving door-penetration seals. Without considering external events from a scoping perspective to identify unique vulnerabilities, significantly reducing the CDF from internally initiated events may result in only marginally reducing the overall CDF.

RBOT can be expanded to simultaneously evaluate external events, such as seismic, during the design phase by choosing via the one-button architecture a database whereby all seismically qualified components fail at their nominal failure rate while those not qualified are assumed to be failed. A fire or flood analysis would insert a database whereby all components affected by the fire or flood are assumed to be failed and the other components fail at their nominal failure rate. The same process would be used to evaluate rocket launches and their payloads. Military planes, ships, and armored vehicles can be evaluated for maneuverability or fire power by having an impact or explosion fail equipment and support systems in the vicinity of the anomaly. Similar to a seismic analysis, all other equipment fails at its nominal failure rate. Recovery actions to restore vital functions could be evaluated for impacts in different areas. The click on one of the menu options returns the analysis to its original state.

Through the use of the one-button architecture, designers can now observe the effects of aging of systems and components by choosing the option where the failure probabilities are adjusted based on aging-related studies. The information available to RBOT from *FaultTree+* provides users with a priority ranking of aged structures/passive components to determine their risk significance. Aging concerns are not limited to active components. New concerns with respect to aging arise because of the reliance on passive safety systems. For example, influences such as age-related corrosion within piping could prevent natural circulation cooling in passive systems. In general, a system's operational mode is a factor influencing aging-related component failures because components in some standby systems display high aging fractions.¹² This is particularly important for spacecraft where maintenance is not feasible. The goal is not just to design a reliable system for today, but to design a system that will be reliable for the duration of the plant fuel cycle or mission length (i.e., 4 years). Those components with a high risk significance are targets for exploring other design alternatives. Thus, by incorporating this information into the PRA models, designers can evaluate how aging components affect system and plant reliability (e.g., at 1, 2, and 4 years).

Human errors and recovery actions also contribute significantly in accident sequences—both in accidents occurring and in minimizing their consequences. The impact of operators can be assessed by selecting from the menu a database that sets all human error probabilities to zero or one for a comparison with the base case. As always, the analysis can be returned to its original case via the one-button architecture.

Early PRAs excluded failures of passive equipment such as pipes, wiring, and multiple check valves from the quantitative analyses because they generally represented a very small contribution to system failure.¹² Because the CDFs for next-generation NPPs (such as IRIS) should be one to two orders of magnitude lower than those for current-generation NPPs, passive failures may now be measurable contributors to the CDF. Conversely, if a passive system requires some active component for initiation, the exclusion of passive components may be realistic because the failure probability of the active component will dominate the system failure probability.

Conclusions

The risk-based tool RBOT has shown that a few component choices (11) yields many design alternatives (160) for consideration. Through the use of RBOT it was also learned that the “logical” design decision for optimization may in fact be the wrong decision. However, because no one actually evaluates these decisions, no one knows that the decision was wrong. For example, removing MOVs from consideration because their failure probability is two to three times that of AOVs¹³⁻¹⁶ would be wrong. A more detailed evaluation shows that the CCF probability for two AOVs is typically

greater than that for two MOVs.^{13–15, 17} Because CCFs dominate the failure modes of reliable systems, using the more “unreliable” valves results in a more “reliable” system. It was also learned that four out of six makes five. That is, the best arrangement for moving four out of six reflectors is using five motors. By maintaining all of the current and previous design, modeling, and data sets via the one-button architecture, the safety ramifications of design options are evaluated, feedback on design alternatives is immediate, and true optimization and understanding can be achieved. These insights and lessons learned helped the IRIS design team and PRA team to achieve a two order-of-magnitude reduction in the base case core damage frequency.

Easily replaceable modules means that reviewers can assess new modeling approaches (e.g., working, failed, degraded); development and testing of new methods such as incorporating digital system failure or degradation of passive systems into a PRA; modeling uncertainties resulting from different modeling approaches, different modeling assumptions, different physical assumptions, and/or different levels of detail; and the sensitivity of assumptions, models, and data on the risk metrics of interest. More than one risk metric can be evaluated at a time such as internal and external events, reliability and cost, reliability and mass, reliability and ease of maintenance or operations. The power of RBOT coupled to *FaultTree+* is that all of the design options are simultaneously available allowing internally and externally generated events to be evaluated at the same time. Any new design or design upgrade would benefit greatly from using these cutting-edge risk tools.

Acknowledgment

Much of this work performed by ORNL was performed under funding provided by ORNL’s Laboratory Director’s Research and Development Program. ORNL is managed and operated by UT-Battelle, LLC, for the U.S. Department of Energy under contract DE-AC05-00OR22725.

References

1. A. D. Chambardel and L. Mange, “Completeness and Complexity of PSAs: Do They Need It?” *Proc. Probabilistic Safety Assessment and Management II, San Diego, California, March 20–25, 1994*.
2. A. Carpignano, “Use of System Simulation to Support Automated Fault Tree Construction,” *Proc. Probabilistic Safety Assessment and Management II, San Diego, California, March 20–25, 1994*.
3. C. Haag et al., “The Use of PRA in Designing the Westinghouse AP600 Plant,” *Proc. Int. Topical Meeting on Probabilistic Safety Assessment PSA 96: Moving Toward Risk-Based Regulation, Park City, Utah, September 29–October 3, 1996*, American Nuclear Society.
4. AP600 PRA, Revision 6, Section 59.2, “Use of PRA in the Design Process,” Westinghouse, November 15, 1995.
5. R. E. Schneider, M. C. Jacob, and D. J. Finnicum, “Applications of Level 2 PSA Results and Insights in the System 80+ Reactor Containment Design,” *Proc. Int. Topical Meeting on Probabilistic Safety Assessment PSA 96: Moving Toward Risk-Based Regulation, Park City, Utah, September 29–October 3, 1996*, American Nuclear Society.
6. Y. O. Mizuno and L. E. Conway, “Preliminary Probabilistic Safety Assessment of the IRIS Plant,” *Proc. ICONE10, 10th Int. Conf. on Nuclear Engineering, April 14–17, 2002*.
7. T. Hayes, “APP1000 Plant Overview,” IEEE Subcommittee on Qualification (SC-2), Clearwater, FL, November 10–11, 2003.
8. Isograph Reliability Software, *FaultTree+ V10*, 1986-2003.
9. M. D. Carelli and B. Petrovic, “Next Generation Advanced Reactor,” *Nucl. Plant J.*, May–June 2001.
10. D. R. Damon et al., *SP-100 Mission Risk Analysis, Volume I—Main Report*, GESR-00849, GE Aerospace, SP-100 Programs, San Jose Operations, San Jose, CA, August 1989.
11. *Perspectives Gained from the Individual Plant Examination of External Events (IPEEE) Program*, NUREG-1742, U.S. Nuclear Regulatory Commission, April 2002.
12. B. M. Meale and D. G. Satterwhite, *An Aging Failure Survey of Light Water Reactor Safety Systems and Components*, NUREG/CR-4747, U. S. Nuclear Regulatory Commission, July 1987.
13. *Simplified Passive Advanced Light Water Reactor Plant Program, AP600 Probabilistic Risk Assessment*, Rev. 7, Westinghouse Electric Corporation, June 28, 1996.
14. R. E. Ginna *Probabilistic Risk Assessment Project, Report to the Nuclear Regulatory Commission in Response to Generic Letter 88-20*, Rochester Gas and Electric Corporation, February 28, 1994.
15. R. E. Jaquith et al., *Probabilistic Risk Assessment for the System80+ Standard Design*, Rev. 1, DCTR-RS-02, ABB Combustion Engineering Nuclear Power, Windsor, Connecticut, March 1993.

16. R. J. Belles, J. W. Cletcher, D. A. Copinger, B. W. Dolan, J. W. Minarick, and M. D. Muhlheim, *Precursors to Potential Severe Core Damage Accidents, 1997: A Status Report*, NUREG/CR-4674, U.S. Nuclear Regulatory Commission, December 1998.
17. F. M. Marshall et al., *Common-Cause Failure Parameter Estimations*, NUREG/CR-5497, U.S. Nuclear Regulatory Commission, October 1998.

Bibliography

M. D. Muhlheim, Ph.D., Oak Ridge National Laboratory, P.O. Box 2008, Oak Ridge, TN 37831, USA, telephone – (865) 574-0386, facsimile – (865) 574-0386, e-mail – muhlheimmd@ornl.gov.

Dr. Muhlheim has a Ph.D. in nuclear engineering from the University of Tennessee. Dr. Muhlheim has performed all types of qualitative and quantitative risk or safety assessments for DOE, NRC, NASA, JPL, and commercial clients for nuclear, chemical, and space-related facilities.

J. W. Cletcher, III, Oak Ridge National Laboratory, P.O. Box 2008, Oak Ridge, TN 37831, USA, telephone – (865) 574-3236, facsimile – (865) 574-0386, e-mail – cletcherjw@ornl.gov.

Mr. Cletcher has a BS in engineering science from the Tennessee Technological University. Mr. Cletcher has been providing engineering support to the ORNL since 1984 through JBF Associates, Inc., PAI, Inc., and, most recently, UT Battelle. He has over 25-years experience in the nuclear industry and is a licensed engineer in TN and NY.

S. Flanagan, Ph. D., Isograph Direct, The Malt Building, Wilderspool Park, Greenalls Ave, Warrington, WA4 6HL, UK, telephone – +44 (0) 1925 437000, facsimile – +44 (0) 1925 437010, e-mail – steveflanagan@isograph.com.

Dr. Flanagan received a BSc in Physics and a Ph. D. in Nuclear Physics from the University of Manchester, UK. During the last 30 years he has worked on safety and reliability in the nuclear power, defense, and other industries. In 1986 he jointly founded Isograph, a developer of software tools for safety and reliability engineers.

J. L. Hynek, Isograph Direct, 4695 MacArthur Court, 11th floor, Newport Beach, CA 92660, USA, telephone – (949) 798-6114, facsimile – (949) 798-5531, e-mail – jhynek@isographdirect.com.

Mr. Hynek received a double BA from the University of Utah where he studied Business and Japanese. Over the last 5 years he has worked for Isograph Inc. in North America, and is currently the Sales Manager of Isograph's Newport Beach, California office.

R. Stack, Dow Chemical, 190 Uran St., Hillsdale, MI 49242, USA, telephone – (517) 439-4405, facsimile – (517) 439-5108, e-mail – stackrj@dow.com.

Mr. Stack has a BS ChE from the University of Massachusetts and an MBA from Quincy University. He is currently a process safety subject matter expert for Dow Chemical. Previously with Dow Chemical, Mr. Stack was a process safety engineer for Dow Automotive and a risk analysis in the Dow Chemical Process Safety Technology Center. Prior to joining Dow Chemical, Mr. Stack performed process safety, risk, and reliability analyses for Union Carbide, NUS Corporation, and American Cyanamid.