

Use of PRA Techniques to Optimize the Design of the IRIS Nuclear Power Plant

M. D. Muhlheim* and J. W. Cletcher, II¹

¹*Oak Ridge National Laboratory, 1060 Commerce Park, Oak Ridge, Tenn., 37830-6487*

True design optimization of a plant's inherent safety and performance characteristics results when a probabilistic risk assessment (PRA) is integrated with the plant-level design process. This is the approach being used throughout the design of the International Reactor Innovative and Secure (IRIS) nuclear power plant to maximize safety. A risk-based design optimization tool employing a "one-button" architecture is being developed by the Oak Ridge National Laboratory to evaluate design changes; new modeling approaches, methods, or theories; modeling uncertainties and completeness; physical assumptions; and data changes on component, cabinet, train, and system bases. Unlike current PRAs, the one-button architecture allows components, modules, and data to be interchanged at will with the probabilistic effect immediately apparent. 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, feedback on design alternatives is immediate, and true optimization and understanding can be achieved. Thus, for the first time, PRA analysts and designers can easily determine the probabilistic implications of different design configurations and operating conditions in various combinations for the entire range of initiating events. The power of the one-button architecture becomes evident by the number of design alternatives that can be evaluated. Component choices yielded 160 design alternatives. Surprisingly, the lessons learned can be counter-intuitive and significant. For example, one of the alternative designs for IRIS evaluated via this architecture revealed that because of common-cause failure probabilities, using the most reliable components actually decreased systems' reliability.

Keywords: PRA, advanced reactor designs, plant optimization, IRIS

I. Introduction

The International Reactor Innovative and Secure (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.¹

The designers of the IRIS plant are using a safety-by-design approach to cover all aspects of safety (e.g., internally, externally, and shutdown-initiated events) at the very beginning of the design process. The design of IRIS began using probabilistic risk assessment (PRA) very early in the design process at the conceptual phase.²

Typical optimization programs use PRAs to optimize plants on a system-by-system basis, one change at a time. Previous evaluations are discarded. Unfortunately, optimization requires evaluating different system and component configurations in various combinations for the entire range of initiating events. Thus, unlike current design optimization programs, the most effective PRA program should allow different types of plant systems and components, in different states, to be interchangeably evaluated. However, because each "new" plant configuration may or may not improve plant safety, all previous design alternatives should be retained to maximize the benefits of a risk-based design.

Current PRAs are generally first drawn up to demonstrate safety and are often unsuited for applications aimed at making design or operating decisions.³ For design work, comparisons are made between design alternatives using simplified models that can be used as the design progresses and later, the complex models that are developed at design freeze points (i.e., full-scope PRAs).

*Corresponding author, Tel: 865-574-0386, Fax: 865-574-8481, Email: muhlheimmd@ornl.gov

For example, during the design of the AP600, the iterative process for the PRA included

- \$ 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.

The scope and detail of the AP600 PRA model increased as the plant design matured. The iterative process (five stages and six revisions) resulted in a number of design and operational improvements.^{4,5}

By developing a program that allows designers to use the PRA to make design decisions regarding a plant's reliability, safety, and cost, designers can continuously perform trade-off studies to identify strengths and weaknesses. To create a tool that designers could use on a continuous basis rather than in stages

- \$ requires a risk-based design optimization tool that designers could (and would) actually use,
- \$ allows the designers to learn what makes a system reliable,
- \$ allows designers to observe how changes in one system affects other systems, and
- \$ provides immediate feedback on design alternatives.

The value of a system for easily and quickly evaluating design alternatives becomes apparent when considering the final design approval (FDA) review for the CE System 80+ reactor containment design. The NRC requested that the designers evaluate design alternatives that help mitigate the consequences of severe accidents.⁶ Sixty-three design alternatives were considered, and twenty-seven were quantified.

II. One-Button Architecture

The idea of mixing PRA and design is nothing new. Tools devoted to automatically constructing fault trees have been proposed by several researchers since the 1970s, but most of these tools (in particular, the first ones) were characterized by a drastic simplification of the system model to make the automatic treatment of the system description possible. According to Carpignano, simplified system models yield fault trees and models with low accuracy that do not accurately represent the systems functioning or malfunctioning.⁷ Thus, although the concept of automatic fault tree construction is over 30 years old, the fact that analysts and designers do not use it indicates its ineffectiveness. In reality, no matter how good the algorithm is for creating fault trees, this approach

will never be as good as a PRA analyst working directly with the designers!

The objective is to have a baseline PRA of IRIS with a collection of alternative system designs, modeling approaches, modeling assumptions, physical assumptions, level of detail, and data to evaluate their importance. Optimization requires looking at different cases for different systems in various combinations. Because the goal during the design of IRIS is to use a safety-by-design approach, feedback from lessons learned must be easily incorporated into the models. Optimization also requires that many aspects and influences on safety must be evaluated *in toto*, not in isolation. To meet these needs, the Oak Ridge National Laboratory (ORNL) is developing a risk-based design optimization tool (RBOT) that uses a one-button architecture to more easily evaluate the risk impacts from different combinations of design alternatives, modeling techniques, data sets, and external events.

The one-button architecture is designed to evaluate combinations of design and event options through sets of fault tree modules in a dynamic PRA. Changing the design is as simple as picking a design alternative from a scroll-down menu (Fig. 1). The RBOT computer program automatically inserts the correct fault tree module(s) into the PRA model in *FaultTree+*,⁸ re-links the correct support systems, adjusts the common-cause failure probabilities, and recalculates the parameters of interest. If additional design alternatives are desired and are not available in the scroll-down list of options, they can be easily created and added by a PRA analyst. 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.

The parameters available for optimizing the design are described below.

1. Reliability

The IRIS project is being managed with the philosophy of designing reliability into the plant at the earliest possible stage of development. Designing for reliability is the most economically sound approach to take. This approach differs from the numerous design optimization and improvement programs traditionally used in the commercial nuclear industry that have employed PRAs to optimize plants on a system-by-system basis. Optimization requires evaluating different system configurations in various combinations for the entire range of initiating events. The most effective PRA program would allow the designers to assess the impact of various design options themselves without having to become PRA experts. For example, consider each of the following arrangements for

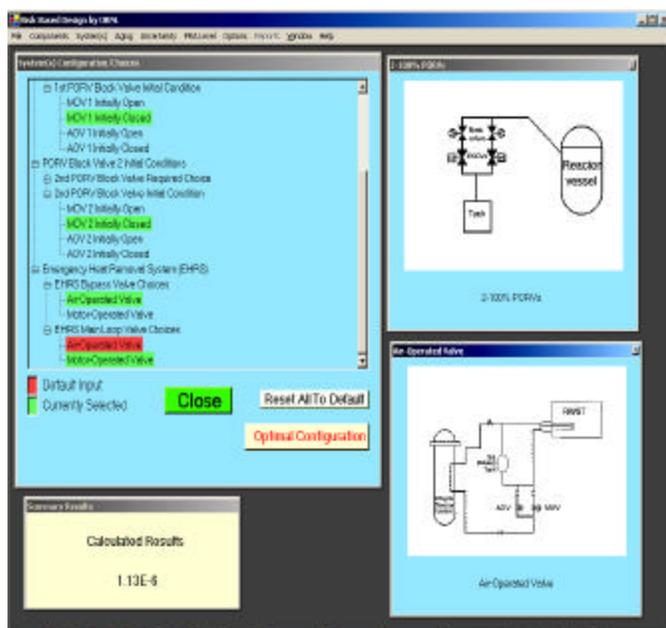


Fig. 1 One-button architecture for PRA evaluations.

auxiliary feedwater (AFW) systems that exist at various nuclear power plants:

- \$ Beaver Valley: 2B50% capacity motor-driven pumps (MDPs) and 1B100% capacity turbine-driven pump (TDP);
- \$ ANO 1: one MDP and one TDP (both 100% capacity pumps);
- \$ Braidwood: one MDP and one diesel-driven pump (both 100% capacity pumps).

Which of these is better for an AFW system? How do the various support systems affect the reliability of the system? Are different valve types or system components important contributors to system failure? Do test and maintenance activities for different components affect the availability of the system? How would you rank the alternate system designs? How many alternate system designs should be evaluated? A review of historical data⁹ shows that diversity of the AFW pumps results in the smallest system unreliability and that cross-ties between trains has a minimal effect on system reliability because pump failures are the most likely causes of system failures. The best arrangement for AFW systems based on historical data, and confirmed using RBOT, is 2 MDPs and 1 TDP, followed closely by 1 MDP and 2 TDPs.

PRA's performed in isolation (i.e., one change at a time) result in numerous system designs, none of which are guaranteed optimal. However, the one-button architecture used for IRIS allows designers to evaluate the benefits

(and costs) of different types and capacities of components (e.g., pumps and valves) and various systems arrangements, including cross-ties between system trains. These choices allow designers, and not just the PRA analysts, to evaluate alternatives probabilistically, identify the dominant failure modes, and focus on reducing the calculated core damage frequency (CDF) by concentrating on its dominant contributors.

2. Passive Safety

Early PRA's 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.¹⁰ 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.

Designers and PRA analysts evaluating new designs for inherently safe reactors must evaluate the physical phenomena that make the passive safety features effective. Evaluations should include

- \$ determining and modeling how the safety functions of the passive processes could be interrupted (e.g., is external cooling of low points in a natural circulation loop possible?);¹⁰
- \$ identifying and probabilistically quantifying the uncertainties in the physics of heat transfer in passive systems (e.g., in a passive system, corrosion within pipes might prevent natural convection from reaching the designed operation point); and
- \$ evaluating and modeling the transition period between the point at which the passive systems are "spent," such as an injection tank becoming empty, and the start of active systems.

Designers must be aware that passivity by itself is not synonymous with improved safety and reliability.¹¹ Two conclusions from the Korean Next Generation Reactor (KNGR) PRA were that safety injection tanks had no considerable effects in reducing the CDF, while the reactor cavity flooding system and catalytic hydrogen igniters were important contributors to accident mitigation and to containment protection after core damage occurs. (IRIS does not have an emergency core cooling system, has reactor cavity flooding capability, and has an inert containment.)

The one-button architecture supports these new modeling approaches by providing designers with a probabilistic evaluation of physical phenomena and

uncertainties for various passive designs coupled with active systems. In addition, the one-button architecture supports not only the standard binary approach or failed, which may not be adequate for passive systems but can support modules for degraded conditions.

3. Internal and External Events

During the initial design stages, design activities typically focus on internally-initiated events such as loss-of-coolant accidents (LOCAs), operational transients, and anticipated transient without scram (ATWS) events. Because internal events are better understood and easier to evaluate, significant effort and experience has identified many initiators of internal events. For example, the AP600 PRA evaluates 26 initiating events in three classes: LOCA, transient, and ATWS. Eight of which contribute >94% of the internally initiated CDF.

Focusing on reducing the internally initiated CDF could have minimal impact on the total CDF. Externally initiated events are often significant contributors to a plant's total CDF.¹² 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 internal-events CDF. 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.

It is also important to evaluate the shutdown risk early in the design phase because some passive safety systems may not be available or may be ineffective during shutdown. The risk while a plant is shut down may exceed the risk during normal operations.

The one-button architecture for IRIS is ideal for evaluating the risk from shutdown and seismic events early in the design. For example, consider evaluating a seismic event using the one-button architecture. The one-button architecture globally changes the data to reflect that off-site power is unavailable because of an earthquake, no off-site power recovery is assumed for up to 24 h after the occurrence of an earthquake, all components not qualified for the seismic event fail, and normal failure rates apply for seismically qualified components.¹³ Fragility curves are used to refine CDF estimates for the external events.

4. Aging

Aging concerns are not limited to active components. New concerns with respect to aging arise because of the reliance on passive safety systems. Influences such as 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.¹⁴ This is particularly important for IRIS, which has a 48-month minimum maintenance interval.

Through the use of the one-button architecture, designers can now observe the effects of aging of systems and components by adjusting the failure probability (based on aging-related studies) and providing a priority ranking of aged structures/passive components to determine their risk significance. 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 (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).

5. Failure Data, Human Error Probabilities, and Uncertainties

Component failure data, recovery probabilities, and human error probabilities can vary greatly. For example, a review of data from several NPP IPEs showed that the failure probability for a spuriously operating block valve differs between plants by a factor of over 10,000. Further complicating the issue is that in practice, most PRAs do not provide much information regarding the failure of passive components.

The one-button architecture for IRIS is set up to evaluate not only model changes but also data changes. Further, changes can be individual or global. With a click of a button, designers can change data from different plants to high, low, and average values from a collection of IPEs and back to IRIS-specific data. Data for individual components can also be changed via the one-button architecture. This allows designers to observe the sensitivity of system reliability to the data and to identify latent design weaknesses by using favorable or conservative failure and recovery data. Similarly, IRIS designers can take equipment out of service and observe the impact of this action on the CDF. Further, there is the benefit from being able to globally change the human error probabilities to 0 or 1 for comparison with the base-case CDF to evaluate the plant's sensitivity to operator actions.

III. Risk-Based Design Optimization

1. Design Alternatives

Optimization requires evaluating different system configurations in various combinations for the entire range of initiating events. 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 shows that typical relief systems [similar to IRIS's automatic depressurization system (ADS)] are 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. By providing choices for component type (air-operated or motor-operated valves), initial valve position (open or closed), number of trains (1 or 2), and valve capacity (50% or 100%), the one-button architecture allows designers to evaluate 40 unique design alternatives. Evaluating the failure modes then provides clues on how the system can be improved.

Using this example, by clicking a single "button" to change the design of the system, designers can learn 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 dominate the reliability of the system;
- \$ 2B50% capacity PORVs 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 (2B vs. 1B100% 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; and
- \$ for those events requiring pressure relief, it is four to six 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.

2. Design Alternatives for IRIS ADS / Emergency Heat Removal System (EHRS) Design

The next test for the one-button architecture was to evaluate a more complex example that allows designers to change component types and configurations in multiple systems. Not only must all of this information automatically adjust to the option chosen, but common-cause failure (CCF) data and support systems must be updated. The one-button architecture in RBOT automatically corrects the CCF probabilities and realigns the correct support system(s) for the different components in the *FaultTree+* models. 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.

Fig. 2 shows the safety systems for the IRIS reactor. A total of eleven design alternatives were provided for the ADS and the [P]EHRS. Alternatives for the ADS include the type of block valves [air-operated valves (AOVs), motor-operated valves (MOVs), or both] and their initial position (open or closed), the number of trains, and the capacity of the relief valves (50% or 100%). Alternatives for the EHRS include the type of valves that must open on either the main or the bypass lines (AOVs, MOVs, or both) to initiate the system. Support systems changes required (based on the options chosen) include actuation signals, electric power, and instrument air. Required CCF probability changes are based on the initial position of the valves and the valve combinations chosen. The resulting 11 choices provide 160 unique design alternatives! The architecture meets the necessary condition that the order in which the design choices are made is irrelevant [i.e., the answer (CDF) is invariant].

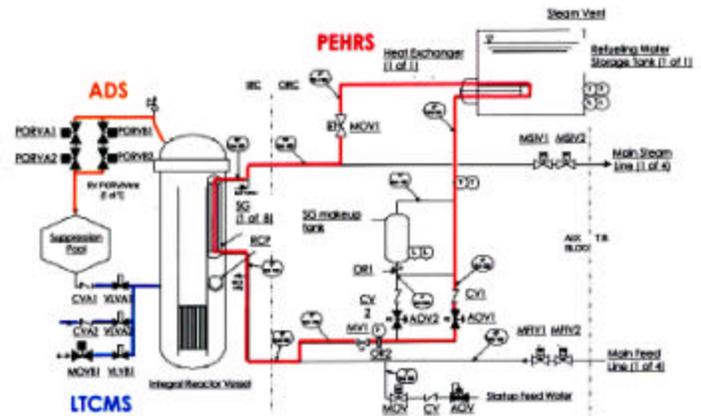


Fig. 2 IRIS safety systems. [ADS is the automatic depressurization system, PEHRS is the passive emergency heat removal system, and LTCMS is the long-term core makeup system.]

With the use of the one-button architecture, the impact of different components and system arrangements is readily apparent to designers. If a designer chooses a system arrangement with both PORV block valves closed and both trains 100%, (s)he will note that the dominant contributor to system failure is the CCF probability of the block valves to open. By knowing the largest contributor to system failure, a designer can now begin to evaluate design alternatives. The simplest way to reduce the CCF probability of the block valves' failing to open is to have the block valves already open. The penalty for this would

be an inadvertent opening of a PORV. Because all initiating events are considered in the trade-off studies, any gains or losses are net gains or losses. Thus, for the ADS, it is observed that having the block valves originally open improves system reliability 20% and reduces the CDF 3.5% (Fig. 3). Once this CCF probability is reduced, the type of block valve (e.g., MOV or AOV) is inconsequential.

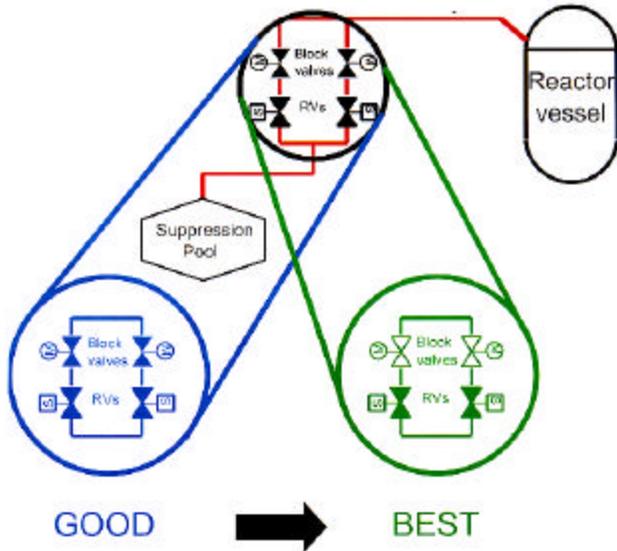


Fig. 3 One-button architecture providing design alternatives for the ADS.

By applying similar options to the EHRS and having the results immediately available, designers would notice that a system with all AOVs was the most unreliable. Although using MOVs significantly improved the system, using a mix of AOVs and MOVs provides the most reliable system (Fig. 4). In fact, a mixed-valve system improves system reliability by 42%; the CDF is reduced by 23% (Fig. 5). With the results immediately available, designers would learn that with a mixed-valve EHRS, the dominant failure modes are the CCF of the check valves (~95%) and the rupture of the refueling water storage tank (RWST) (~5%). (The CCF probability of the AOVs and MOVs in a mixed valve system is a minor contributor to system unreliability.) The designers' next step would be to try to reduce the CCF probability of the check valves. A review of the AP600 PRA¹⁵ shows the difficulty designers face in this task. About 21.5% of the internally initiated CDF for the AP600 involves an initiating event and the CCF of some check valves; another 10.9% of the CDF involves an initiating event, the CCF of some check valves, and another independent hardware failure. Thus, by knowing

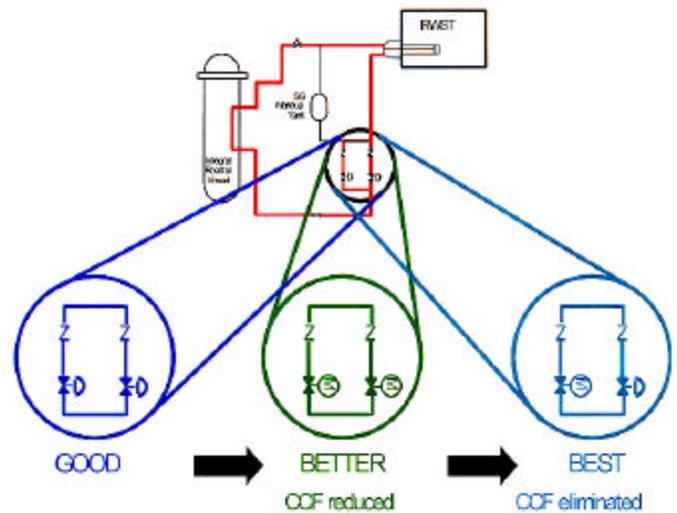


Fig. 4 One-button architecture providing design alternatives for the EHRS.

why and how the system fails, a designer would learn that for this system, further improvements in the system's reliability will be difficult because check valves are needed to prevent reverse flow.

With the wealth of information available to designers through the one-button architecture, they can now evaluate the numerous design alternatives and 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 reliability does not decrease appreciably (Fig. 5). Thus, for the first time, plant reliability and cost attributes can be optimized simultaneously.

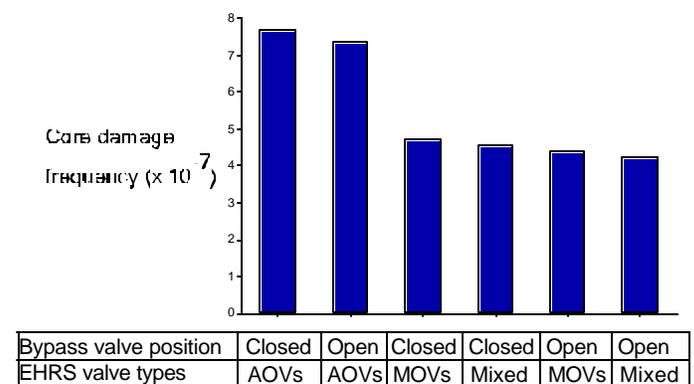


Fig. 5 System failure probability based on PORV block valve position and EHRS valve type.

3. Lessons Learned

A significant observation is that relatively few component choices result in a very large number of design alternatives. The 11 component choices for the ADS and EHRs (type, position, capacity) resulted in 160 design alternatives. The one-button architecture allows all of these alternatives to be evaluated probabilistically with ease and provides designers insights into system behavior. In addition, the architecture allows analysts to evaluate all of the design alternatives by providing a list of the top (best) and bottom (worst) “n” alternatives.

Another important lesson learned is that what appears to be a logical decision for “optimizing” a system (without actually evaluating it) may in fact be the wrong decision. For example, removing MOVs from consideration because their failure probability is two to three times that of AOVs¹⁵⁻¹⁸ would be wrong. A more detailed evaluation shows that the CCF probability for two AOVs is typically greater than that for two MOVs by a factor of 1.2 to 2.0 (Refs. 15-17, 19) (Fig. 6). Because CCFs typically dominate the failure modes of reliable systems (i.e., the CCF probability is larger than the failure probability for the independent valves multiplied together), using the more “unreliable” valves results in a more “reliable” system (Fig. 7).

True optimization must consider not only different alternatives for valves (motor-, air-, or solenoid-operated valves) but alternatives for all equipment including pumps (motor-, diesel, or turbine-driven) and instrumentation and controls (analog and digital). As the evaluation of IRIS safety systems shows, true optimization must consider CCFs, recovery factors, unavailability of components and systems from test and maintenance, and the initial conditions of the equipment (open and closed).

V. Conclusions

Optimization requires looking at different cases for different systems in various combinations. Similarly, understanding how a plant operates and how different modeling assumptions affect the results requires this same type of procedure to see how everything behaves under different circumstances. By use of PRA modules that can be changed with the touch of a button, IRIS designers can easily perform trade-off studies of different system arrangements. Feedback early in the design process provides designers with the opportunity to examine and better understand the impacts of design alternatives as they are integrated at a systems level. Evaluating failure modes provides clues on how the system can be improved. Further, with information available early in the design process on external events (e.g., seismic and flooding) and shutdown events, designers will be able to significantly improve the safety; reliability; and cost of building, maintaining, and operating the plant.

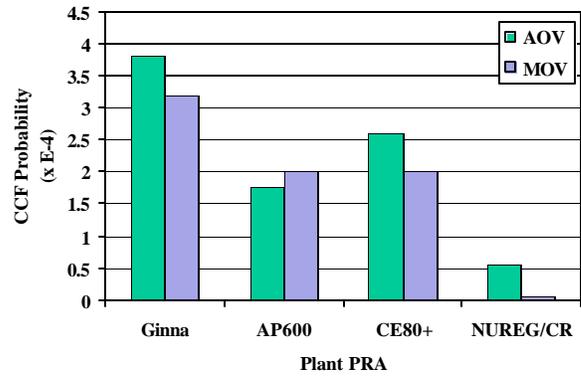


Fig. 6 Common-cause failure probabilities for AOVs and MOVs from different PRAs.

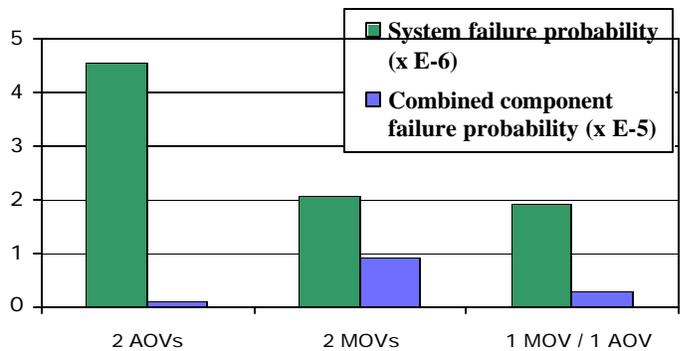


Fig. 7 The use of more reliable components may result in a more unreliable system because of common-cause failure contributions.

The risk-based tool for IRIS has shown that a few component choices yield many design alternatives and that “logical” decisions for optimization may be wrong. 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, feedback on design alternatives is immediate, and true optimization and understanding can be achieved.

Acknowledgment

This work was performed under funding provided by ORNL’s Laboratory Directors’ 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. M. D. Carelli and B. Petrovic, “Next Generation Advanced Reactor,” *Nucl. Plant J.*, May–June 2001.

2. 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.
 3. 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.
 4. 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.
 5. AP600 PRA, Revision 6, Section 59.2, "Use of PRA in the Design Process," Westinghouse, November 15, 1995.
 6. 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.
 7. 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.
 8. Isograph Reliability Software, *FaultTree+ V10*, 1986-2003.
 9. D. C. Bley and D. H. Johnson, "On Encountering Small Numbers: How Good Models Go Bad," *Proc. Probabilistic Safety Assessment and Management II*, San Diego, California, March 20–25, 1994.
 10. J. P. Poloski et al., *Reliability Study: Auxiliary/Emergency Feedwater System, 1987–1995*, NUREG/CR-5500, Vol. 1, U.S. Nuclear Regulatory Commission, August 1998.
 11. D. Hittner et al., "Industrial Needs in R&D for the Safety and Competitiveness of the Next Generation of Reactors (MICA)," *FISA 99: EU Research in Safety*, Office for Official Publications of the European Communities, Luxembourg, November 29–December 1, 1999, 2000.
 12. *Perspectives Gained from the Individual Plant Examination of External Events (IPEEE) Program*, NUREG-1742, U.S. Nuclear Regulatory Commission, April 2002.
 13. T. Sato, A. Tanabe, and S. Kondo, "PSA in Design of Passive/Active Safety Reactors," *Reliability Eng. Syst. Safety*, Vol. 52, Elsevier, 1996.
 14. 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.
 15. *Simplified Passive Advanced Light Water Reactor Plant Program, AP600 Probabilistic Risk Assessment*, Rev. 7, Westinghouse Electric Corporation, June 28, 1996.
 16. *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.
 17. 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.
 18. 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.
 19. F. M. Marshall et al., *Common-Cause Failure Parameter Estimations*, NUREG/CR-5497, U.S. Nuclear Regulatory Commission, October 1998.
-