Welcome to an Overview of ORNL’s Risk-Based Design Optimization Tool (RBOT)

Mike Muhlheim

(865) 574-0386
muhlheimmd@ornl.gov
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.
ORNL’s Reactor and Facility Safety Group within the Nuclear Science and Technology Division developed a risk-based design optimization tool (RBOT) that uses a one-button architecture to allow 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.
RBOT is a program that links to *FaultTree+* and allows users to evaluate various design options as the design progresses.

*FaultTree+ 11.0.Ink*
A company’s own PRA analysts develop the base case model(s) and the design alternatives.
RBOT takes the models and allows users to change a design by picking one of the design alternatives that they modeled from a scroll-down menu.
If additional design alternatives are desired and are not available in the scroll-down list of options, they can be created by a PRA analyst and added to the scroll-down list.
When a design alternative is chosen, the resulting fault tree is the same as that which would result if those choices were the original base case design.
Any or all of the design options can be chosen in any order.
Because all choices remain available, no information is lost, and the design can be returned to any previous state.
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.
For this example, the option being analyzed has 2-100% drive motors (i.e., each motor drives all 6 reflectors).
The fault tree in FaultTree+ shows 2-100% drive motors.
2-100% drive motors means that both motors must fail for the system to fail.
Common-cause failures (CCFs) of the reflector motors are accounted for in the model.
The reflector option chosen is for slide reflectors.
The model correctly shows that the reflectors are slide reflectors.
What if a different drive motor configuration was evaluated?
Choosing the option for 4-50% drive motors, 2 in standby, is made by clicking on that option.
As before, the figure changes to show the current design option under evaluation.
The 2-100% drive motor option is changed automatically in FaultTree+ by RBOT to 2-50% main drive motors and 2-50% standby motors.
Because 4 of the 6 reflectors must operate for success, the failure of either 50% main drive motors will cause the system to fail.
Because the standby drive motors can drive either bank of reflectors, both must fail for the system to fail.
The common-cause failure probability is changed to show that 3 of the 4 drive motors must fail for the system to fail.
The probability of failure is transmitted back to RBOT.

Calculated Results

6.63E-7
All of the parameters of interest that are available in FaultTree+ are still available via RBOT.
Interestingly, a risk-based system analysis shows that the 5-motor arrangement is the optimal number for a system that requires 4 of 6 reflectors to move for success.
It turns out that a 5-motor system requires the largest number of motors to fail (4) for the system to fail (4 of the 6 reflectors must move for success).
A similar review of the other reflector motor options clearly shows why any of the other options require fewer reflector motors to fail for the system to fail.
For example, a system with 6 reflector drive motors—1 for each reflector—requires 3 motors to fail for the system to fail.
Consider the following example of optimizing the safety systems in the International Reactor Innovative and Secure (IRIS).
• IRIS is an advanced light-water reactor (LWR) with an integral primary circuit

• The design team is an international consortium led by Westinghouse/BNFL (~20 organizations from 9 countries, including industry, laboratories, utilities, academia)
The Automatic Depressurization System (ADS) uses pressure relief valves to depressurize the reactor. Block valves are used to prevent an inadvertent blowdown.
There are 4 loops in the Emergency Heat Removal System (EHRS) that use natural circulation to remove heat from the reactor core.
Either of these valves must open to initiate natural circulation cooling using the EHRS.
The **11** Component Choices Yielded **160** Design Alternatives

- Block valve position and type
- Number and capacity of relief valves in the ADS (1-100%, 2-50%, 2-100% RVs)
- Type of valves in the EHRS main and bypass lines
The AOVs were originally chosen because they are the most reliable valves available.
Changing the valves in the EHRS to valves with a higher failure rate actually improved the reliability of the system!
Mixing the valve types provided an even more reliable system because it removed the common-cause failure contribution of the valves.
Opening the block valves in the ADS removed their “fails-to-open” failure mode and provided the most reliable design of the options provided.
Insights and lessons learned from RBOT helped the IRIS design / PRA team for Westinghouse achieve a 2 order-of-magnitude reduction in the base-case core damage frequency.
In fact, Westinghouse modified the design of its AP1000 during its design certification review by the Nuclear Regulatory Commission to include combinations of AOVs and MOVs in safety systems.
RBOT can be expanded to simultaneously evaluate external events, such as seismic or fire, during the design phase by choosing a database whereby all seismically qualified components or components affected by a fire fail at their nominal failure rate while those not qualified or affected are assumed to be failed.
Military planes, ships, and armored vehicles can be evaluated for maneuverability or fire power by failing equipment and support systems in the vicinity of an impact or explosion.
Any new design or design upgrade would benefit greatly from using a tool such as RBOT.
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