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.

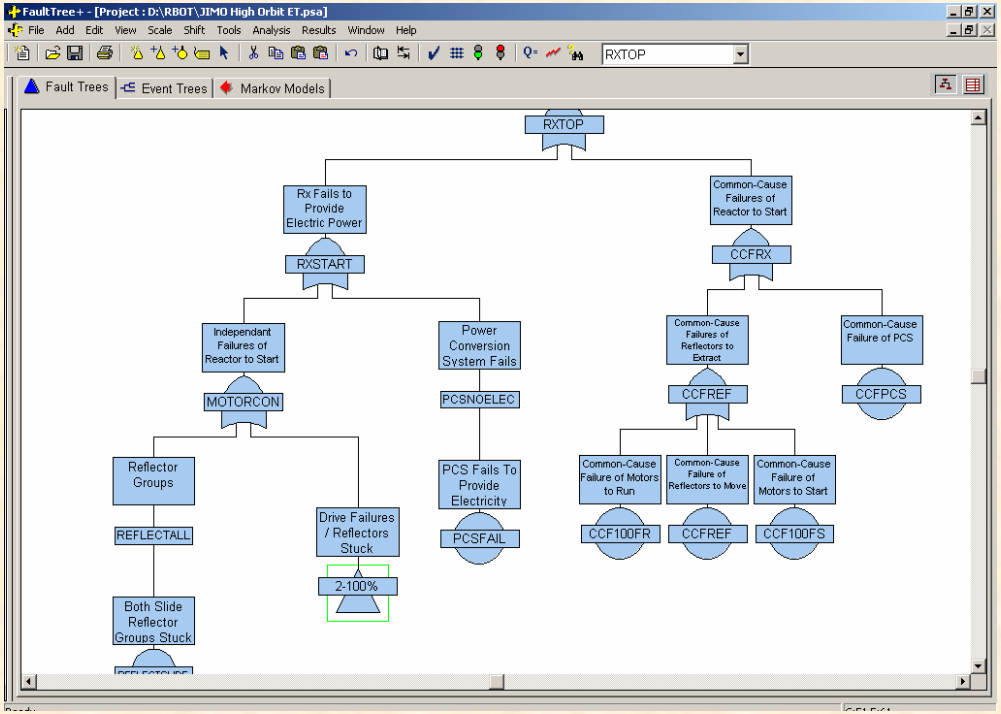
ORNL's Reactor and Facility Safety Group within the Nuclear Science and Technology Division developed a risk-based design optimization tool (RBOT) that uses a one-button architecture to allow users to evaluate

- 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.

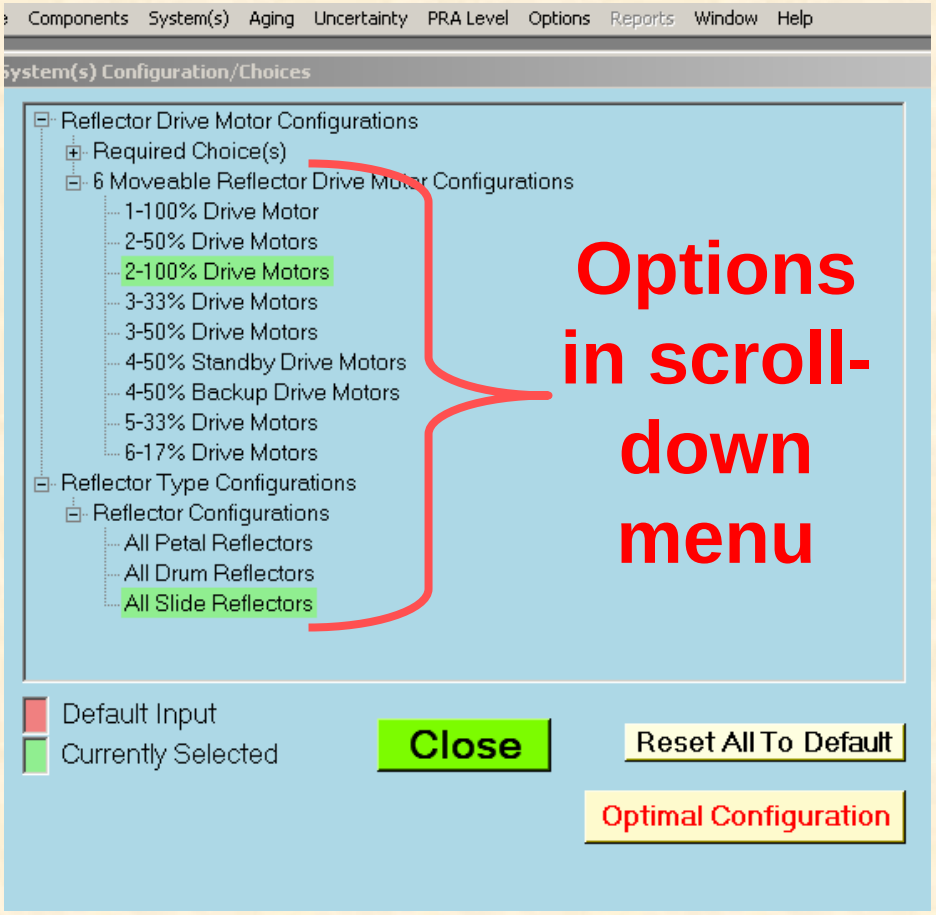
RBOT is a program that links to *FaultTree*+ and allows users to evaluate various design options as the design progresses.

FaultTree+ 11.0.lnk

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.



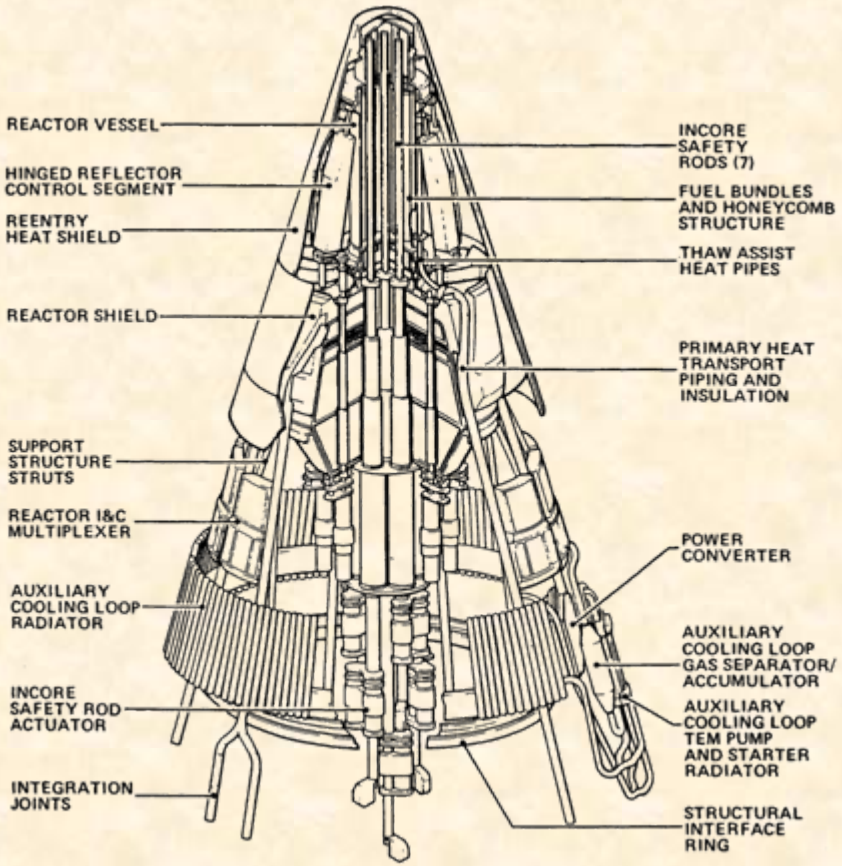
If additional design alternatives are desired and are not available in the scroll-down list of options, they can be created by a PRA analyst and added to the scroll-down list.

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.

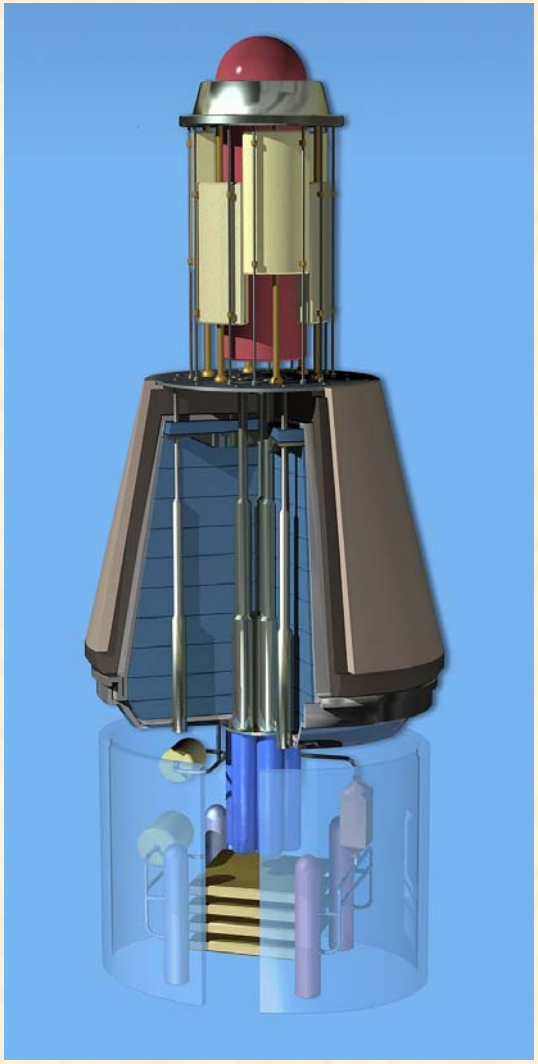
Any or all of the design options can be chosen in any order.

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.



Risk-Based Design Optimization Tool by ORNL

File Components System(s) Aging Uncertainty PRA Level Options Reports Window Help

System(s) Configuration/Choices

- Reflector Drive Motor Configurations
  - Required Choice(s)
  - 6 Moveable Reflector Drive Motor Configurations
    - 1-100% Drive Motor
    - 2-50% Drive Motors
    - 2-100% Drive Motors
    - 3-33% Drive Motors
    - 3-50% Drive Motors
    - 4-50% Standby Drive Motors
    - 4-50% Backup Drive Motors
    - 5-33% Drive Motors
    - 6-17% Drive Motors
- Reflector Type Configurations
  - Reflector Configurations
    - All Petal Reflectors
    - All Drum Reflectors
    - All Slide Reflectors

For this example, the option being analyzed has 2-100% drive motors (i.e., each motor drives all 6 reflectors)

Default Input

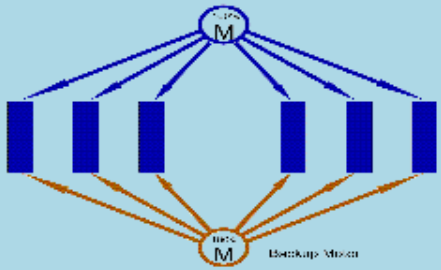
Currently Selected

Close

Reset All To Default

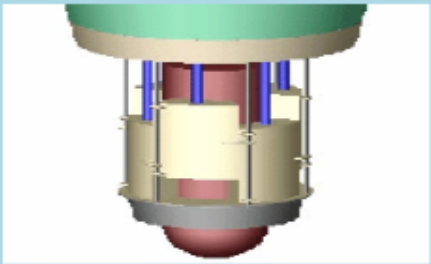
Optimal Configuration

2-100% Drive Motors



2-100% Drive Motors

All Slide Reflectors

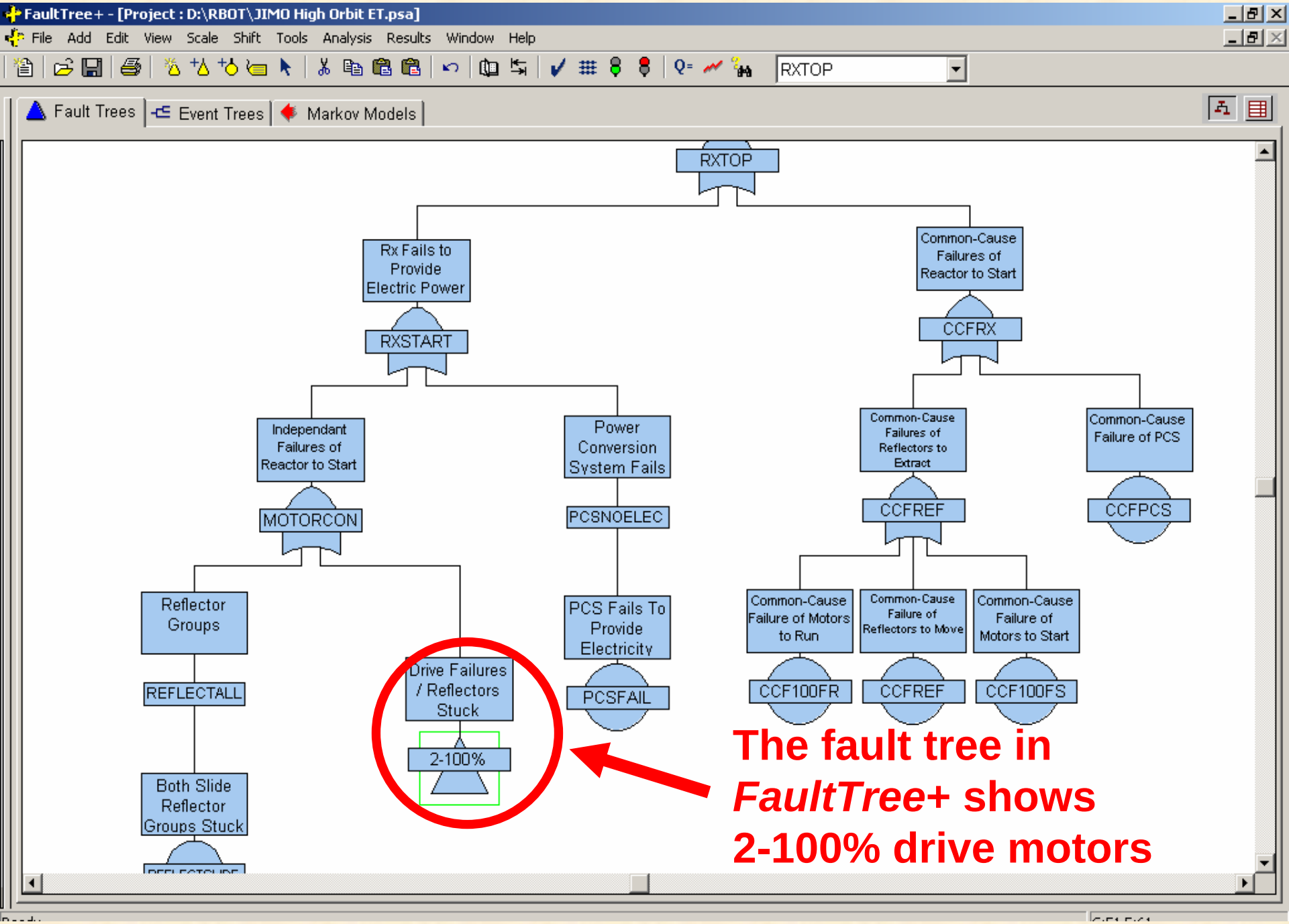


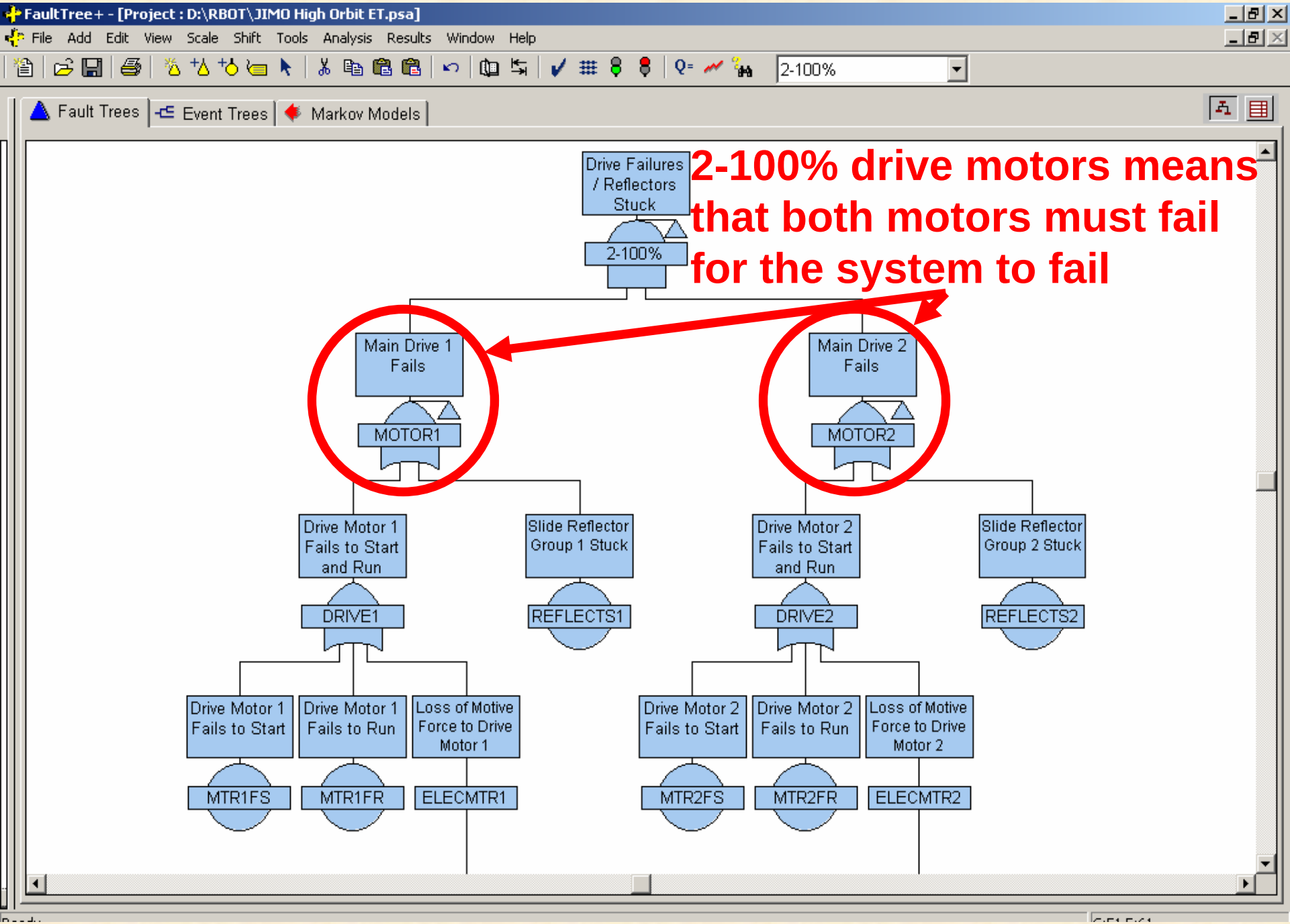
All Slide Reflectors

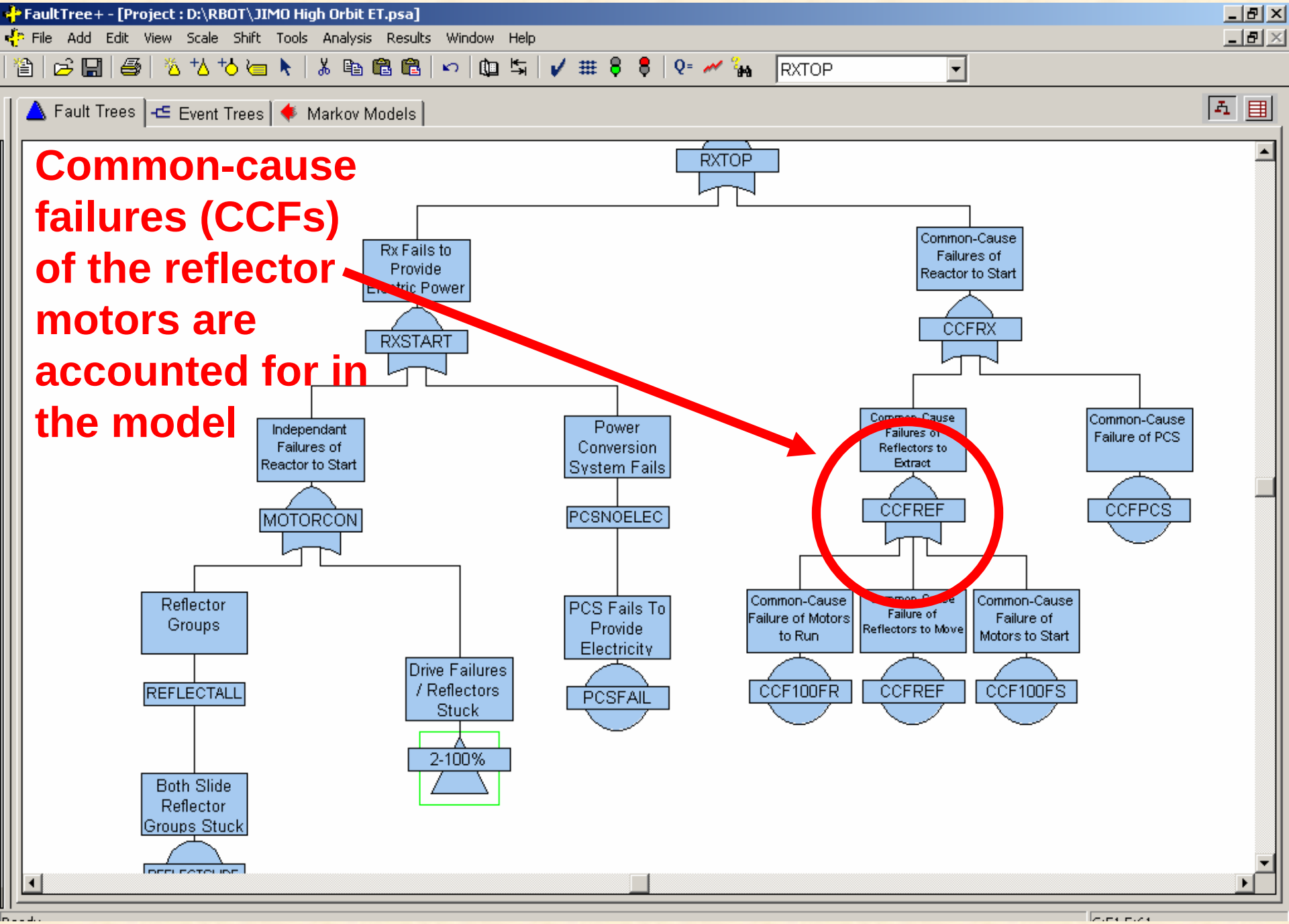
Summary Results

Calculated Results

6.63E-7


FaultTree+ - [Project : D:\RBOT\JIMO High Orbit ET.psa]
File Add Edit View Scale Shift Tools Analysis Results Window Help
RXTOP
Fault Trees
Event Trees
Markov Models
RXTOP
Rx Fails to Provide Electric Power
RXSTART
Common-Cause Failures of Reactor to Start
CCFRX
Independant Failures of Reactor to Start
MOTORCON
Power Conversion System Fails
PCSNOELEC
Common-Cause Failures of Reflectors to Extract
CCFREF
Common-Cause Failure of PCS
CCFPCS
Reflector Groups
REFLECTALL
Drive Failures / Reflectors Stuck
2-100%
PCS Fails To Provide Electricity
PCSFAIL
Common-Cause Failure of Motors to Run
CCF100FR
Common-Cause Failure of Reflectors to Move
CCFREF
Common-Cause Failure of Motors to Start
CCF100FS
Both Slide Reflector Groups Stuck
The fault tree in FaultTree+ shows 2-100% drive motors


FaultTree+ - [Project : D:\RBOT\JIMO High Orbit ET.psa]
File Add Edit View Scale Shift Tools Analysis Results Window Help
2-100%
Fault Trees
Event Trees
Markov Models
2-100% drive motors means that both motors must fail for the system to fail
Drive Failures / Reflectors Stuck
2-100%
Main Drive 1 Fails
MOTOR1
Main Drive 2 Fails
MOTOR2
Drive Motor 1 Fails to Start and Run
DRIVE1
Slide Reflector Group 1 Stuck
REFLECTS1
Drive Motor 2 Fails to Start and Run
DRIVE2
Slide Reflector Group 2 Stuck
REFLECTS2
Drive Motor 1 Fails to Start
MTR1FS
Drive Motor 1 Fails to Run
MTR1FR
Loss of Motive Force to Drive Motor 1
ELECMTR1
Drive Motor 2 Fails to Start
MTR2FS
Drive Motor 2 Fails to Run
MTR2FR
Loss of Motive Force to Drive Motor 2
ELECMTR2


FaultTree+ - [Project : D:\RBOT\JIMO High Orbit ET.psa]
File Add Edit View Scale Shift Tools Analysis Results Window Help
RXTOP
Fault Trees
Event Trees
Markov Models
Common-cause failures (CCFs) of the reflector motors are accounted for in the model
RXTOP
Rx Fails to Provide Electric Power
RXSTART
Independant Failures of Reactor to Start
MOTORCON
Reflector Groups
REFLECTALL
Both Slide Reflector Groups Stuck
Drive Failures / Reflectors Stuck
2-100%
Power Conversion System Fails
PCSNOELEC
PCS Fails To Provide Electricity
PCSFAIL
Common-Cause Failures of Reactor to Start
CCFRX
Common-Cause Failures of Reflectors to Extract
CCFREF
Common-Cause Failure of PCS
CCFPCS
Common-Cause Failure of Motors to Run
CCF100FR
Common-Cause Failure of Reflectors to Move
CCFREF
Common-Cause Failure of Motors to Start
CCF100FS

Risk-Based Design Optimization Tool by ORNL

File Components System(s) Aging Uncertainty PRA Level Options Reports Window Help

System(s) Configuration/Choices

- Reflector Drive Motor Configurations
  - Required Choice(s)
  - 6 Moveable Reflector Drive Motor Configurations
    - 1-100% Drive Motor
    - 2-50% Drive Motors
    - 2-100% Drive Motors
    - 3-33% Drive Motors
    - 3-50% Drive Motors
    - 4-50% Standby Drive Motors
    - 4-50% Backup Drive Motors
    - 5-33% Drive Motors
    - 6-17% Drive Motors
- Reflector Type Configurations
  - Reflector Configurations
    - All Petal Reflectors
    - All Drum Reflectors
    - All Slide Reflectors

The reflector option chosen is for slide reflectors

Default Input

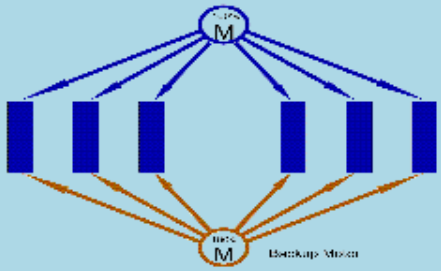
Currently Selected

Close

Reset All To Default

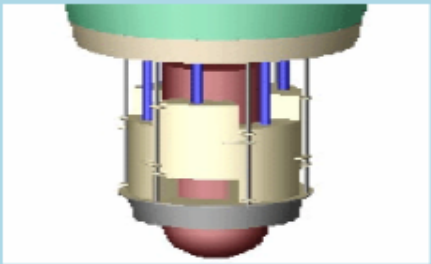
Optimal Configuration

2-100% Drive Motors



2-100% Drive Motors

All Slide Reflectors

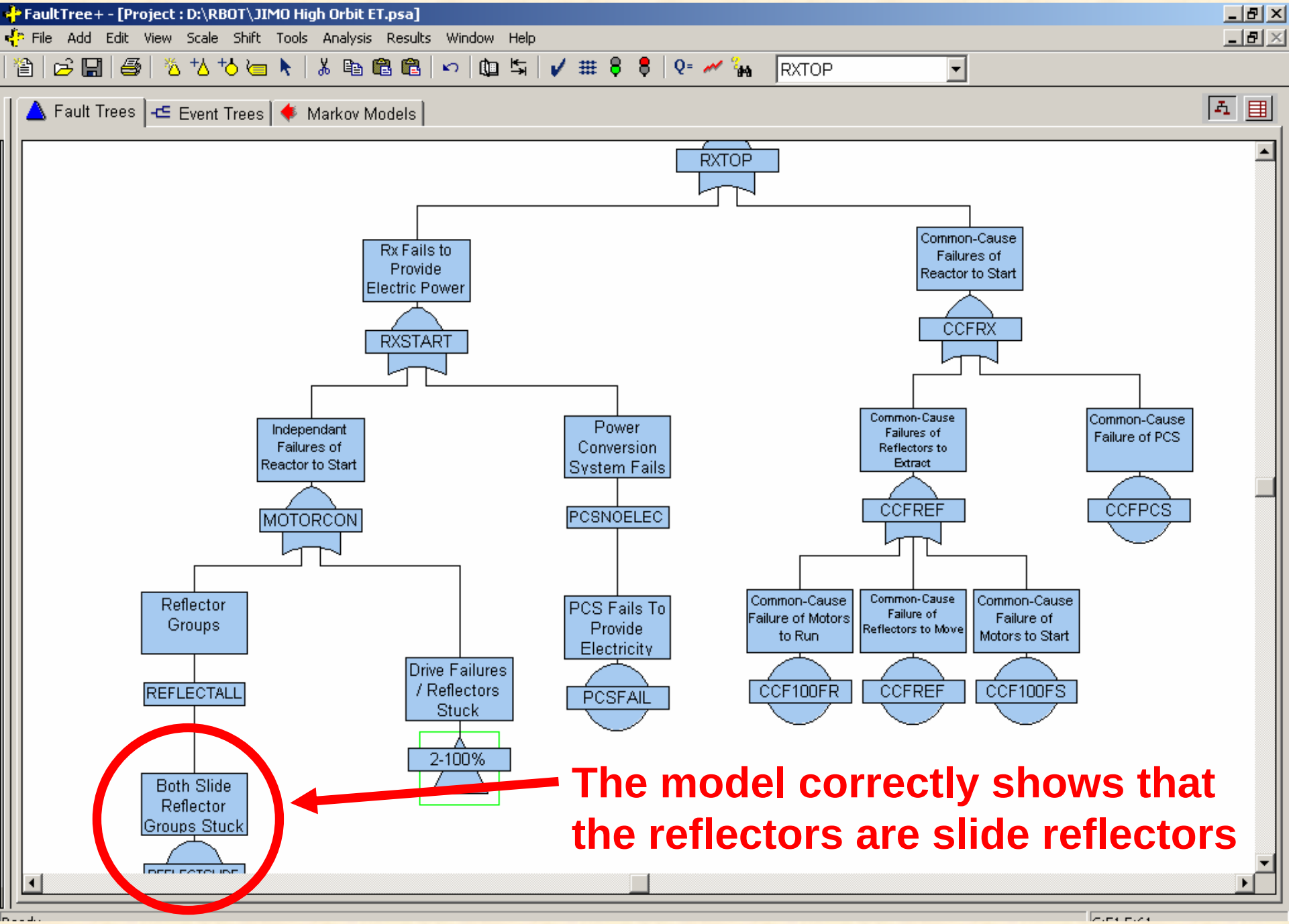


All Slide Reflectors

Summary Results

Calculated Results

6.63E-7


FaultTree+ - [Project : D:\RBOT\JIMO High Orbit ET.psa]
File Add Edit View Scale Shift Tools Analysis Results Window Help
RXTOP
Fault Trees
Event Trees
Markov Models
RXTOP
Rx Fails to Provide Electric Power
RXSTART
Common-Cause Failures of Reactor to Start
CCFRX
Independant Failures of Reactor to Start
MOTORCON
Power Conversion System Fails
PCSNOELEC
Common-Cause Failures of Reflectors to Extract
CCFREF
Common-Cause Failure of PCS
CCFPCS
Reflector Groups
REFLECTALL
Drive Failures / Reflectors Stuck
2-100%
PCS Fails To Provide Electricity
PCSFAIL
Common-Cause Failure of Motors to Run
CCF100FR
Common-Cause Failure of Reflectors to Move
CCFREF
Common-Cause Failure of Motors to Start
CCF100FS
Both Slide Reflector Groups Stuck
The model correctly shows that the reflectors are slide reflectors

What if a different drive motor configuration was evaluated?

Risk-Based Design Optimization Tool by ORNL

File Components System(s) Aging Uncertainty PRA Level Options Reports Window Help

System(s) Configuration/Choices

- Reflector Drive Motor Configurations
  - Required Choice(s)
  - 6 Moveable Reflector Drive Motor Configurations
    - 1-100% Drive Motor
    - 2-50% Drive Motors
    - 2-100% Drive Motors
    - 3-33% Drive Motors
    - 3-50% Drive Motors
    - 4-50% Standby Drive Motors
    - 4-50% Backup Drive Motors
    - 5-33% Drive Motors
    - 6-17% Drive Motors
- Reflector Type Configurations
  - Reflector Configurations
    - All Petal Reflectors
    - All Drum Reflectors
    - All Slide Reflectors

Choosing the option for 4-50% drive motors, 2 in standby, is made by clicking on that option

Default Input

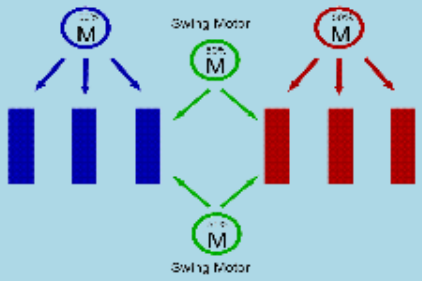
Currently Selected

Close

Reset All To Default

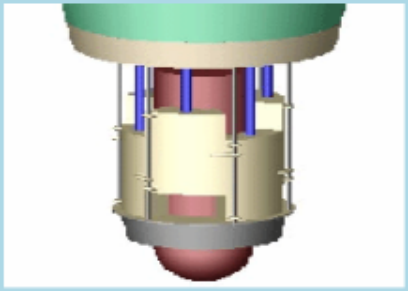
Optimal Configuration

4-50% Standby Drive Motors



4-50% Standby Drive Motors

All Slide Reflectors



All Slide Reflectors

Summary Results

Calculated Results

5.28E-7

Risk-Based Design Optimization Tool by ORNL

File Components System(s) Aging Uncertainty PRA Level Options Reports Window Help

System(s) Configuration/Choices

- Reflector Drive Motor Configurations
  - Required Choice(s)
  - 6 Moveable Reflector Drive Motor Configurations
    - 1-100% Drive Motor
    - 2-50% Drive Motors
    - 2-100% Drive Motors
    - 3-33% Drive Motors
    - 3-50% Drive Motors
    - 4-50% Standby Drive Motors
    - 4-50% Backup Drive Motors
    - 5-33% Drive Motors
    - 6-17% Drive Motors
- Reflector Type Configurations
  - Reflector Configurations
    - All Petal Reflectors
    - All Drum Reflectors
    - All Slide Reflectors

As before, the figure changes to show the current design option under evaluation

Default Input

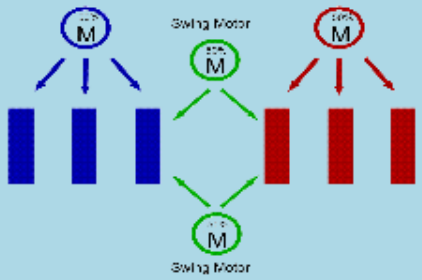
Currently Selected

Close

Reset All To Default

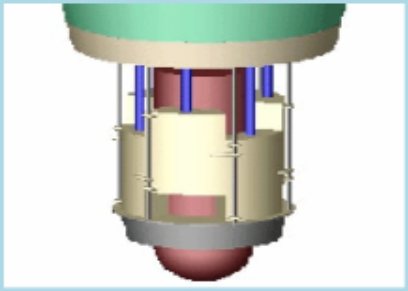
Optimal Configuration

4-50% Standby Drive Motors



4-50% Standby Drive Motors

All Slide Reflectors



All Slide Reflectors

Summary Results

Calculated Results

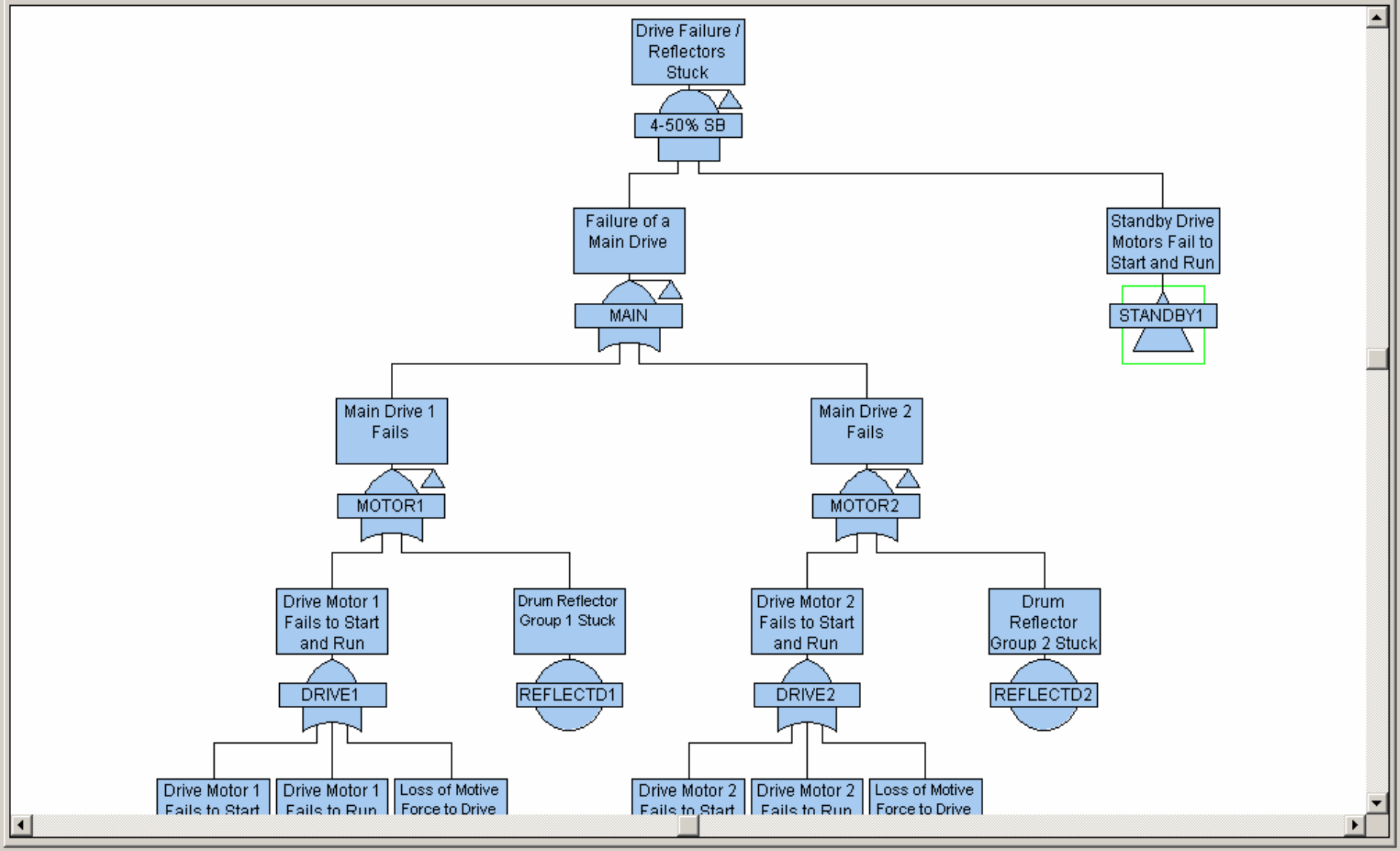
5.28E-7

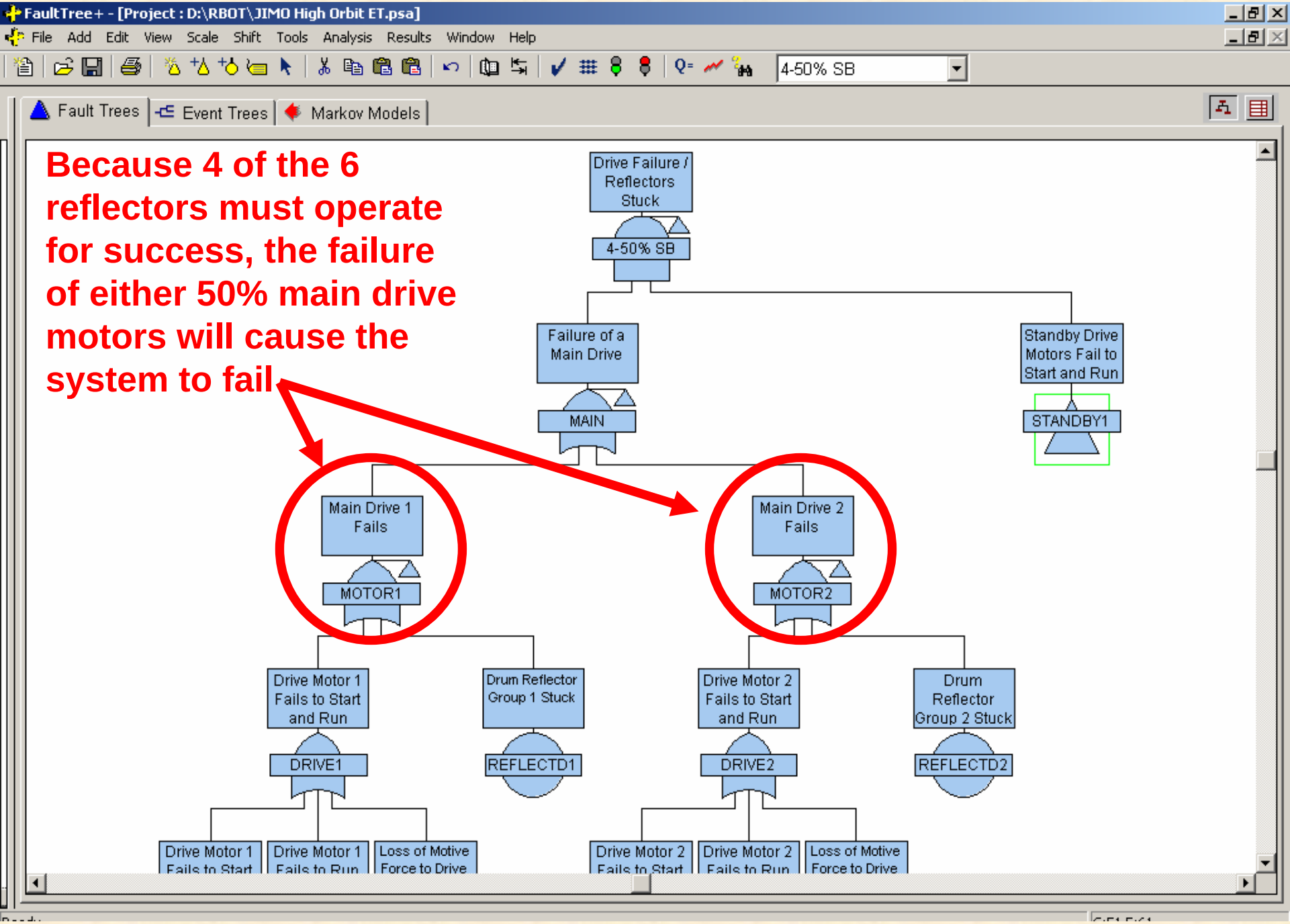
FaultTree+ - [Project : D:\RBOT\JIMO High Orbit ET.psa]

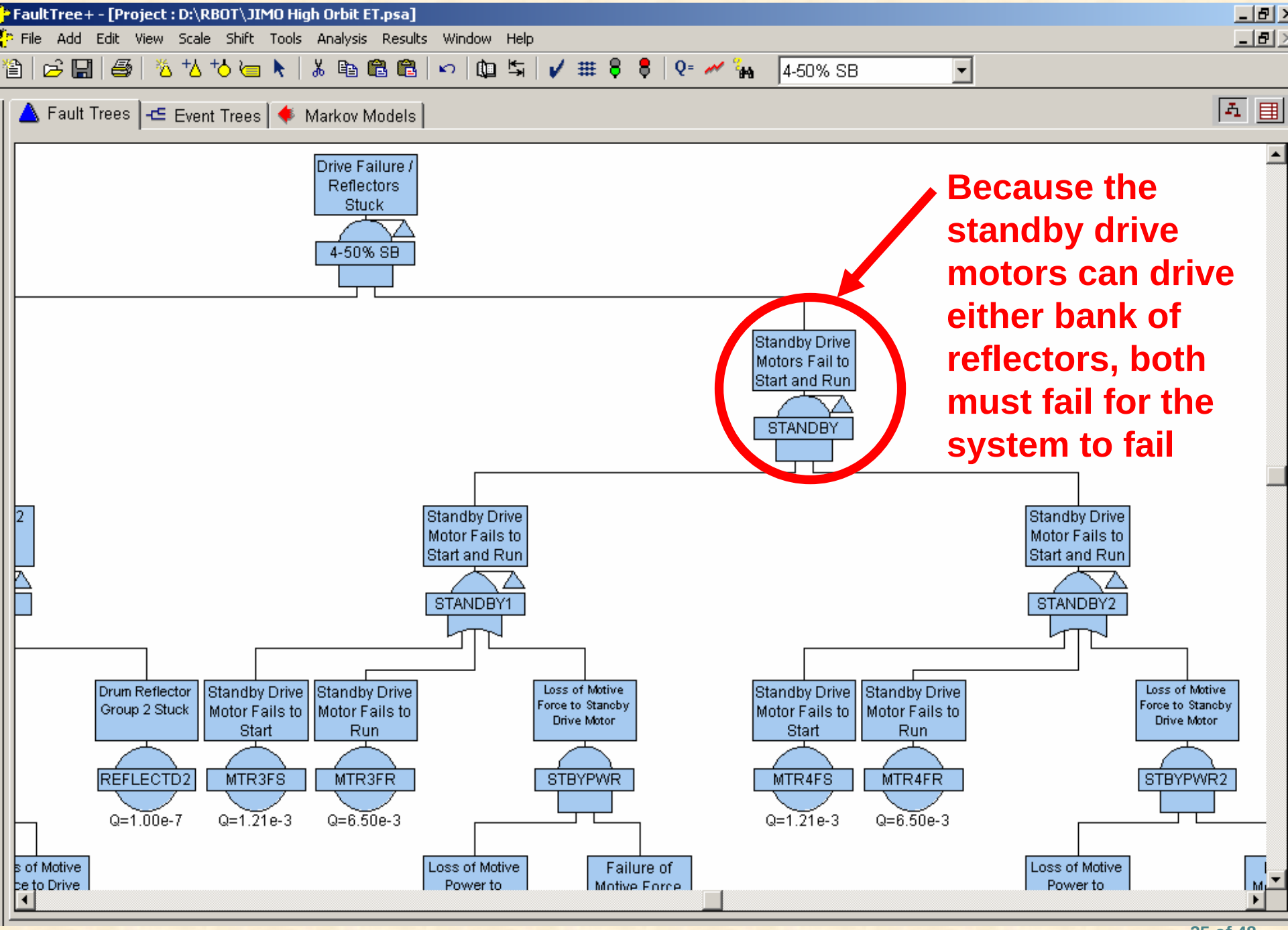
File Add Edit View Scale Shift Tools Analysis Results Window Help

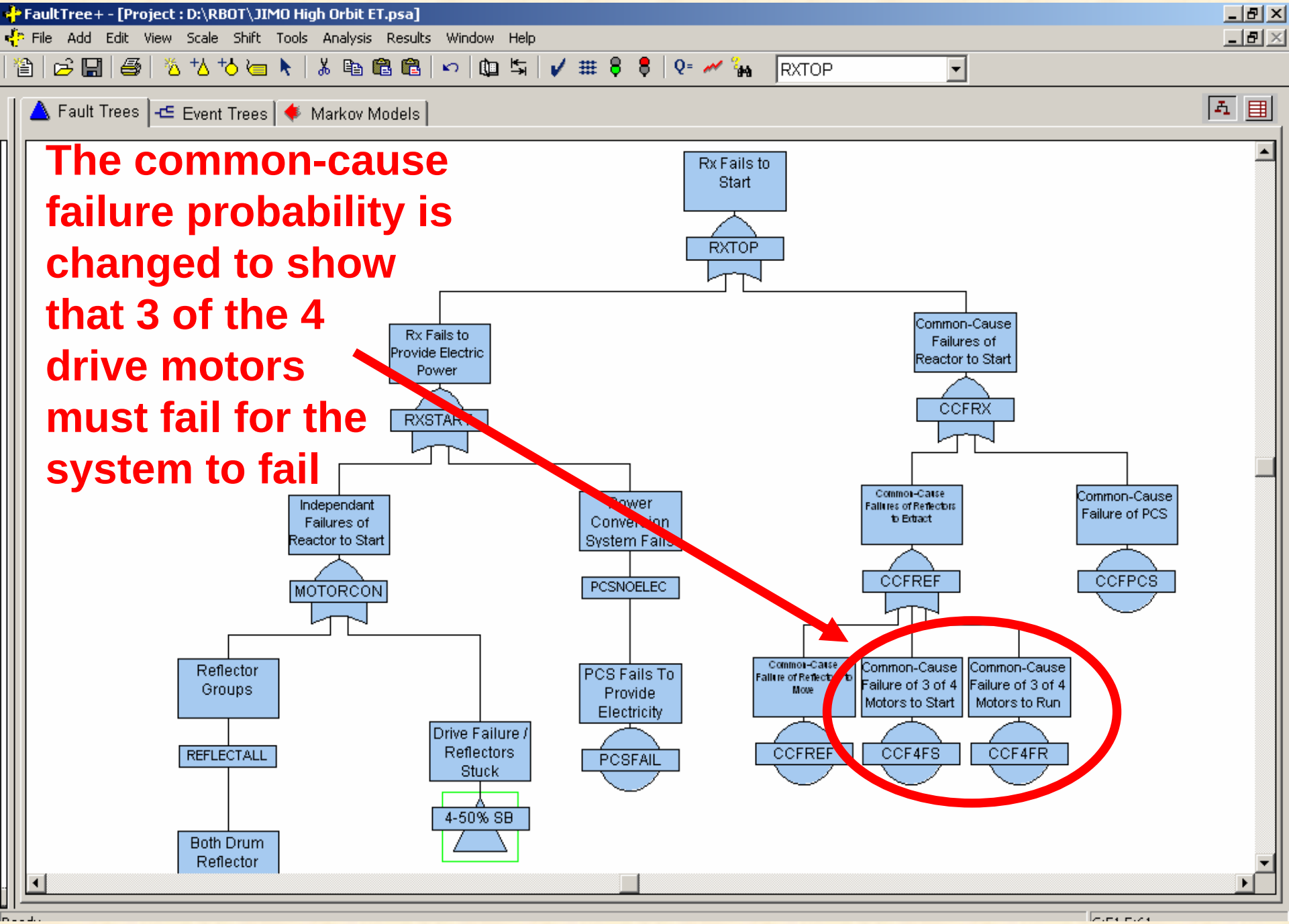
4-50% SB

Fault Trees | Event Trees | Markov Models




FaultTree+ - [Project : D:\RBOT\JIMO High Orbit ET.psa]
File Add Edit View Scale Shift Tools Analysis Results Window Help
4-50% SB
Fault Trees
Event Trees
Markov Models
Because 4 of the 6 reflectors must operate for success, the failure of either 50% main drive motors will cause the system to fail
Drive Failure / Reflectors Stuck
4-50% SB
Failure of a Main Drive
MAIN
Standby Drive Motors Fail to Start and Run
STANDBY1
Main Drive 1 Fails
MOTOR1
Main Drive 2 Fails
MOTOR2
Drive Motor 1 Fails to Start and Run
DRIVE1
Drum Reflector Group 1 Stuck
REFLECTD1
Drive Motor 2 Fails to Start and Run
DRIVE2
Drum Reflector Group 2 Stuck
REFLECTD2
Drive Motor 1 Fails to Start
Drive Motor 1 Fails to Run
Loss of Motive Force to Drive
Drive Motor 2 Fails to Start
Drive Motor 2 Fails to Run
Loss of Motive Force to Drive


FaultTree+ - [Project : D:\RBOT\JIMO High Orbit ET.psa]
File Add Edit View Scale Shift Tools Analysis Results Window Help
4-50% SB
Fault Trees
Event Trees
Markov Models
Drive Failure / Reflectors Stuck
4-50% SB
Standby Drive Motors Fail to Start and Run
STANDBY
Because the standby drive motors can drive either bank of reflectors, both must fail for the system to fail
Standby Drive Motor Fails to Start and Run
STANDBY1
Standby Drive Motor Fails to Start and Run
STANDBY2
Drum Reflector Group 2 Stuck
REFLECTD2
Q=1.00e-7
Standby Drive Motor Fails to Start
MTR3FS
Q=1.21e-3
Standby Drive Motor Fails to Run
MTR3FR
Q=6.50e-3
Loss of Motive Force to Standby Drive Motor
STBYPWR
Loss of Motive Power to
Failure of Motive Force
Standby Drive Motor Fails to Start
MTR4FS
Q=1.21e-3
Standby Drive Motor Fails to Run
MTR4FR
Q=6.50e-3
Loss of Motive Force to Standby Drive Motor
STBYPWR2
Loss of Motive Power to


FaultTree+ - [Project : D:\RBOT\JIMO High Orbit ET.psa]
File Add Edit View Scale Shift Tools Analysis Results Window Help
RXTOP
Fault Trees
Event Trees
Markov Models
The common-cause failure probability is changed to show that 3 of the 4 drive motors must fail for the system to fail
Rx Fails to Start
RXTOP
Rx Fails to Provide Electric Power
RXSTART
Common-Cause Failures of Reactor to Start
CCFRX
Independant Failures of Reactor to Start
MOTORCON
Power Conversion System Fails
PCSNOELEC
Common-Cause Failures of Reflectors to Extract
CCFREF
Common-Cause Failure of PCS
CCFPCS
Reflector Groups
REFLECTALL
Both Drum Reflector
Drive Failure / Reflectors Stuck
4-50% SB
PCS Fails To Provide Electricity
PCSFAIL
Common-Cause Failure of Reflectors to Move
CCFREF
Common-Cause Failure of 3 of 4 Motors to Start
CCF4FS
Common-Cause Failure of 3 of 4 Motors to Run
CCF4FR

Risk-Based Design Optimization Tool by ORNL

File Components System(s) Aging Uncertainty PRA Level Options Reports Window Help

System(s) Configuration/Choices

- Reflector Drive Motor Configurations
  - Required Choice(s)
  - 6 Moveable Reflector Drive Motor Configurations
    - 1-100% Drive Motor
    - 2-50% Drive Motors
    - 2-100% Drive Motors
    - 3-33% Drive Motors
    - 3-50% Drive Motors
    - 4-50% Standby Drive Motors
    - 4-50% Backup Drive Motors
    - 5-33% Drive Motors
    - 6-17% Drive Motors
- Reflector Type Configurations
  - Reflector Configurations
    - All Petal Reflectors
    - All Drum Reflectors
    - All Slide Reflectors

Default Input

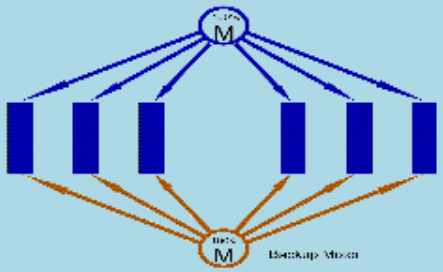
Currently Selected

Close

Reset All To Default

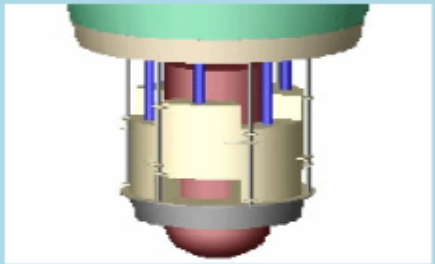
Optimal Configuration

2-100% Drive Motors



2-100% Drive Motors

All Slide Reflectors



All Slide Reflectors

Summary Results

Calculated Results

6.63E-7

The probability of failure is transmitted back to RBOT.

Results

Summary | Importance | Appearance: | Cut Sets | Show Frequency | Show Cut Set Importance

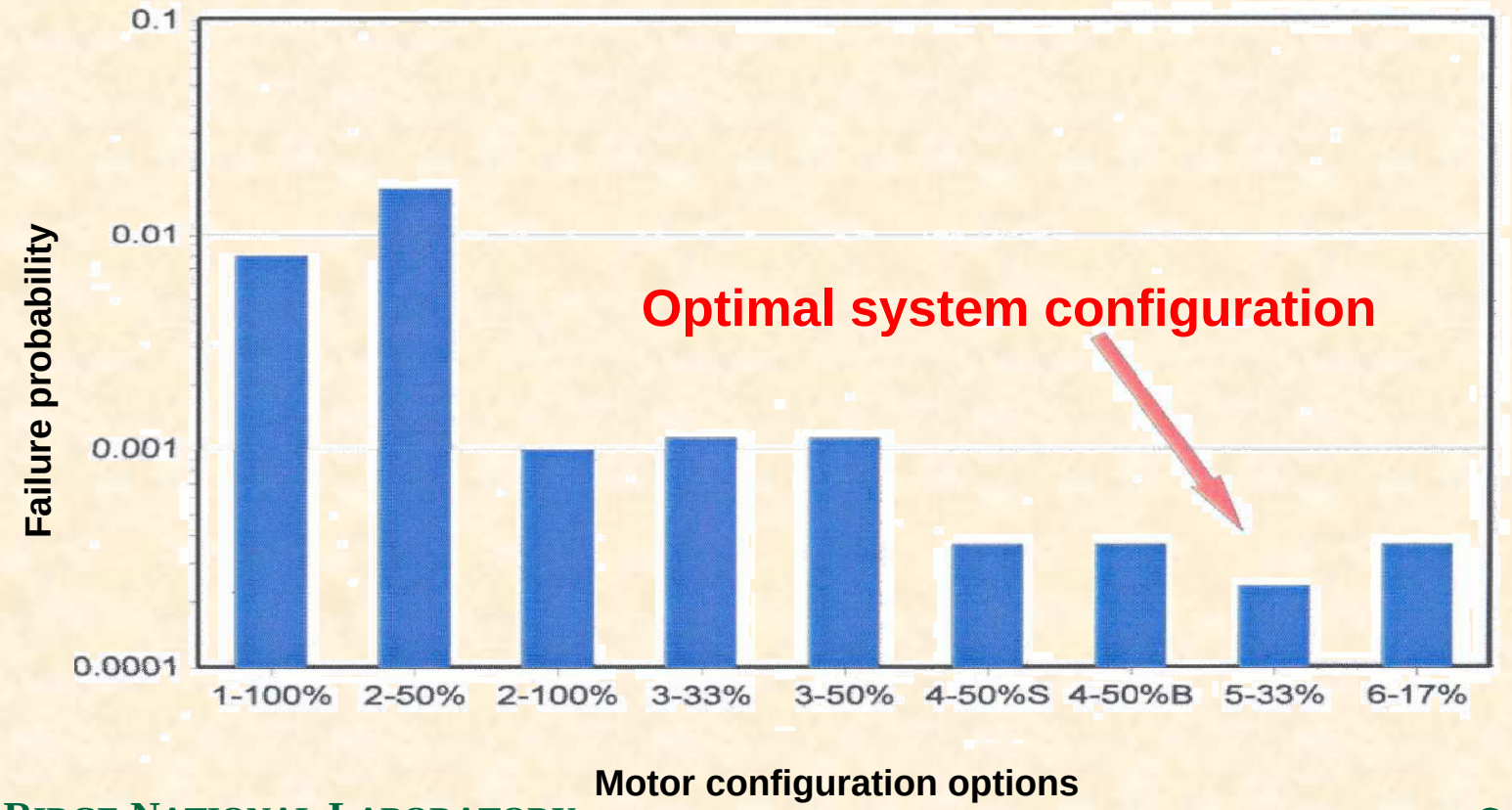
No.	Q	Minimal Cut Set
1	2.74e-7	MTR1FR. MTR3FR. MTR4FR
2	2.74e-7	MTR2FR. MTR3FR. MTR4FR
3	5.11e-8	MTR1FR. MTR3FS. MTR4FR
4	5.11e-8	MTR2FR. MTR3FS. MTR4FR
5	5.11e-8	MTR1FS. MTR3FR. MTR4FR
6	5.11e-8	MTR1FR. MTR3FR. MTR4FS
7	5.11e-8	MTR2FS. MTR3FR. MTR4FR
8	5.11e-8	MTR2FR. MTR3FR. MTR4FS
9	9.50e-9	MTR2FS. MTR3FR. MTR4FS

All of the parameters of interest that are available in *FaultTree+* are still available via RBOT

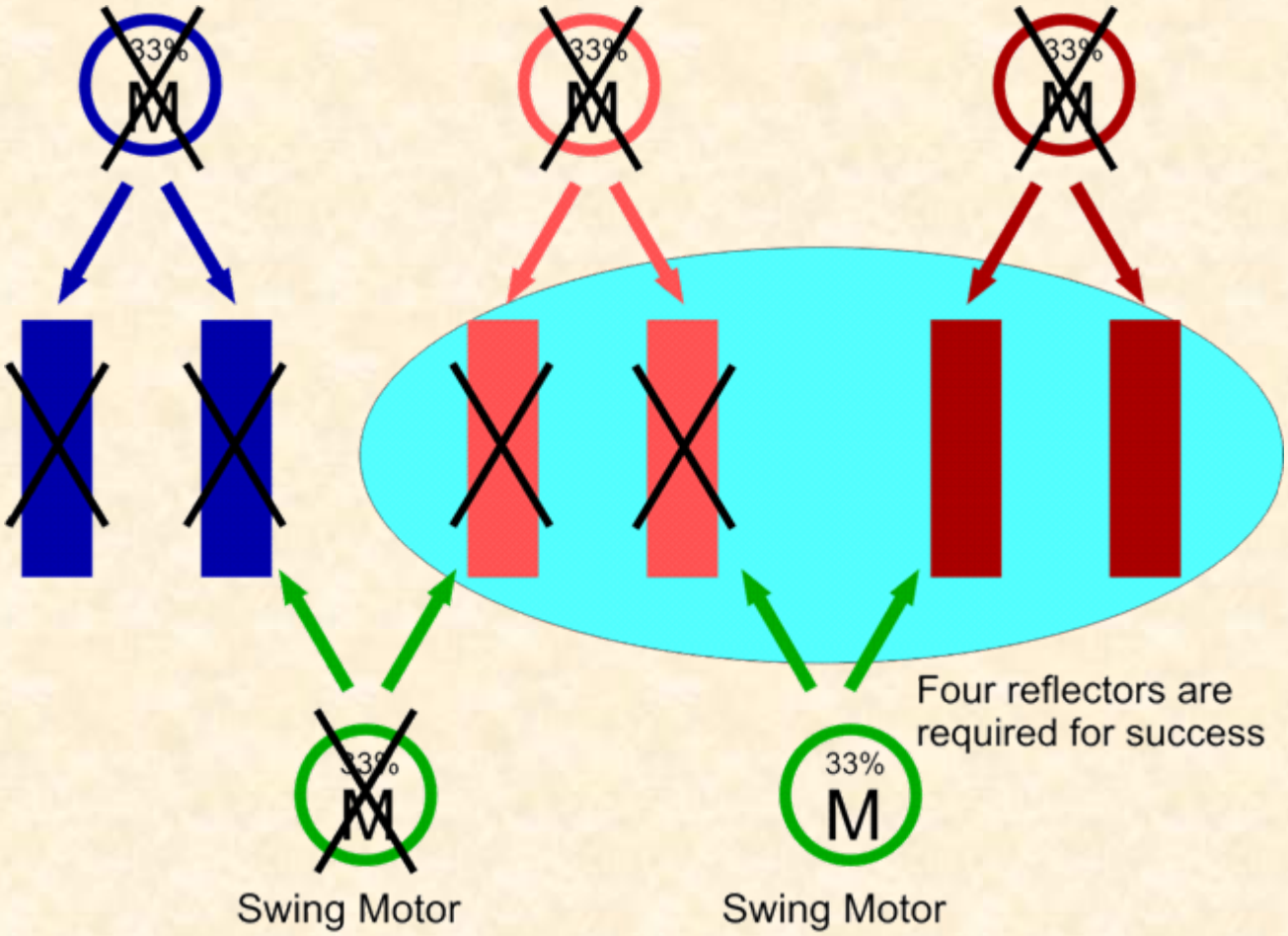
Event Filter :

Trace Cut Set | Clear Cut Set Trace | Cut Set Details... | Quit

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.

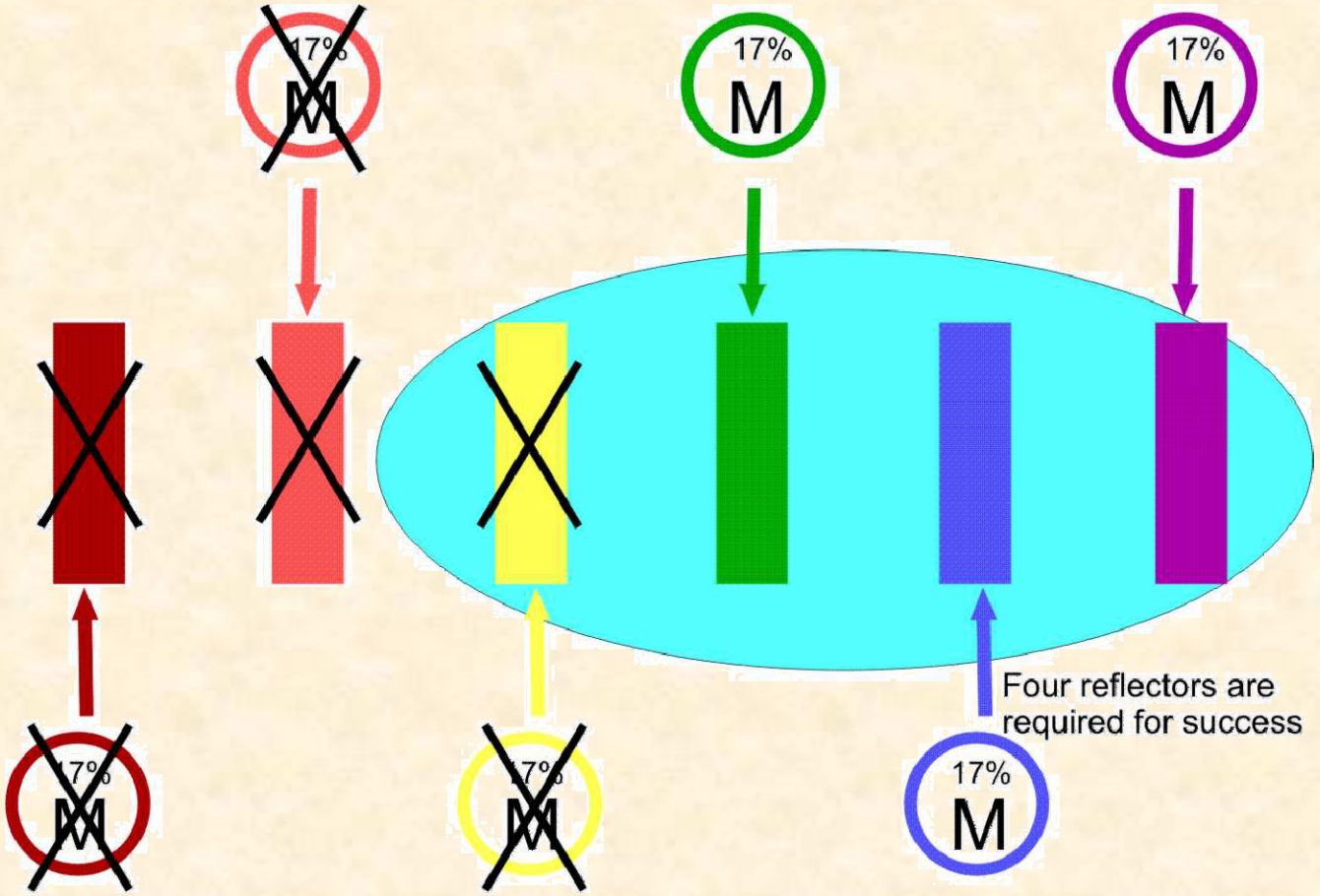


It turns out that a **5**-motor system requires the largest number of motors to fail (**4**) for the system to fail (**4** of the **6** reflectors must move for success).



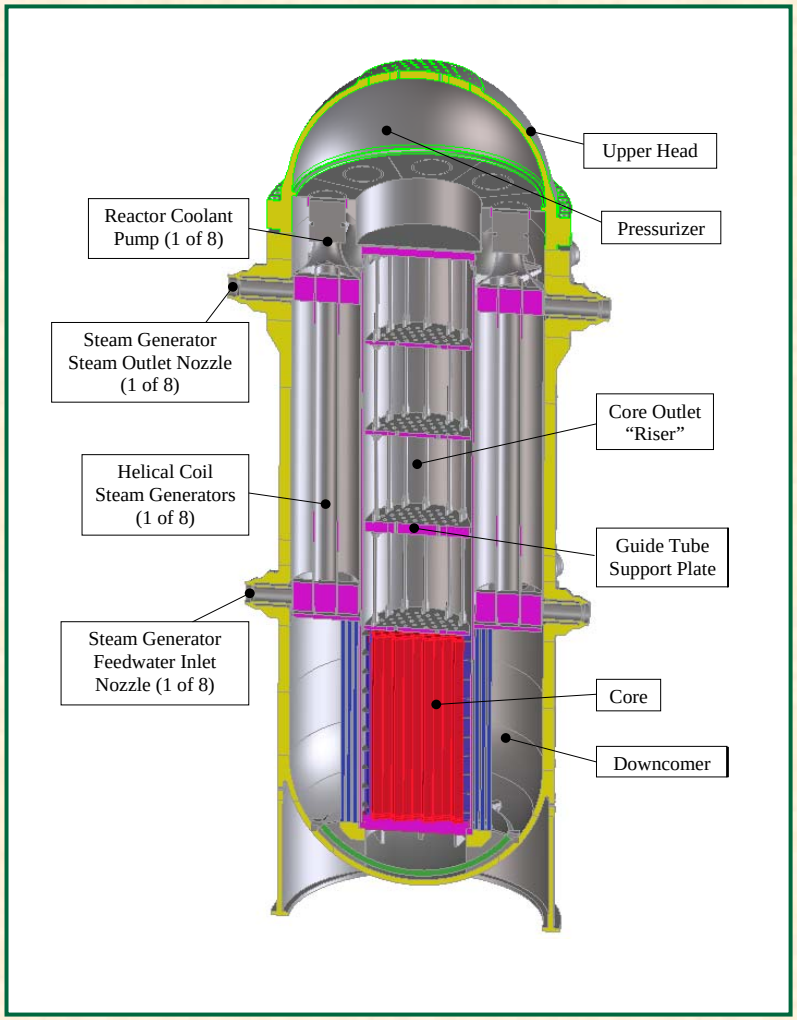
A similar review of the other reflector motor options clearly shows why any of the other options require fewer reflector motors to fail for the system to fail.

For example, a system with 6 reflector drive motors—1 for each reflector— requires 3 motors to fail for the system to fail.

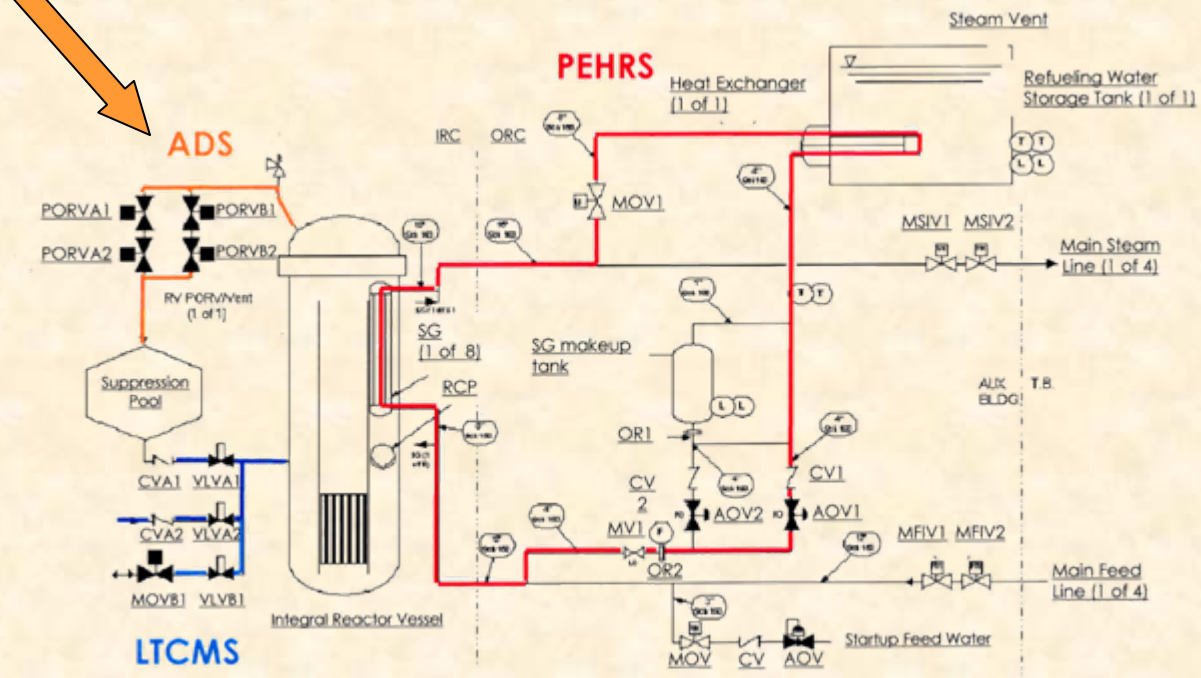


Consider the following example of optimizing the safety systems in the International Reactor Innovative and Secure (IRIS).

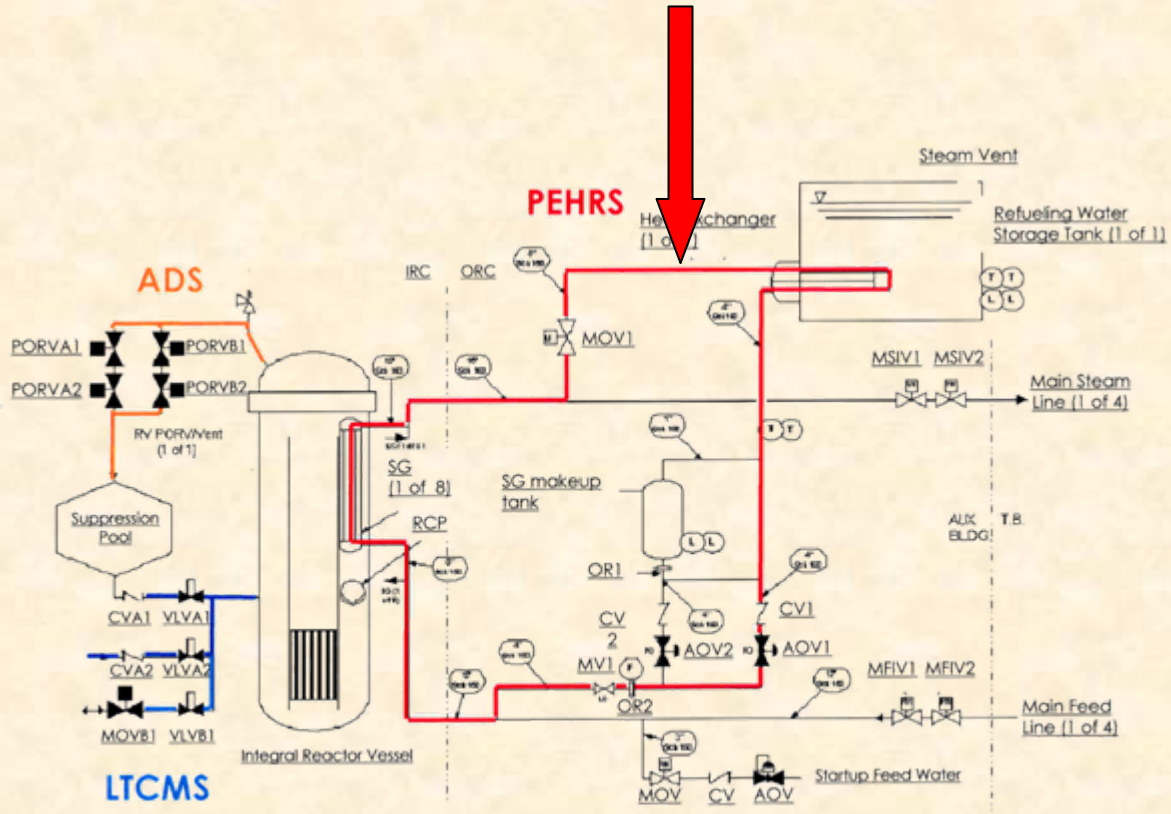
- IRIS is an advanced light-water reactor (LWR) with an integral primary circuit
- The design team is an international consortium led by Westinghouse/BNFL (~20 organizations from 9 countries, including industry, laboratories, utilities, academia)

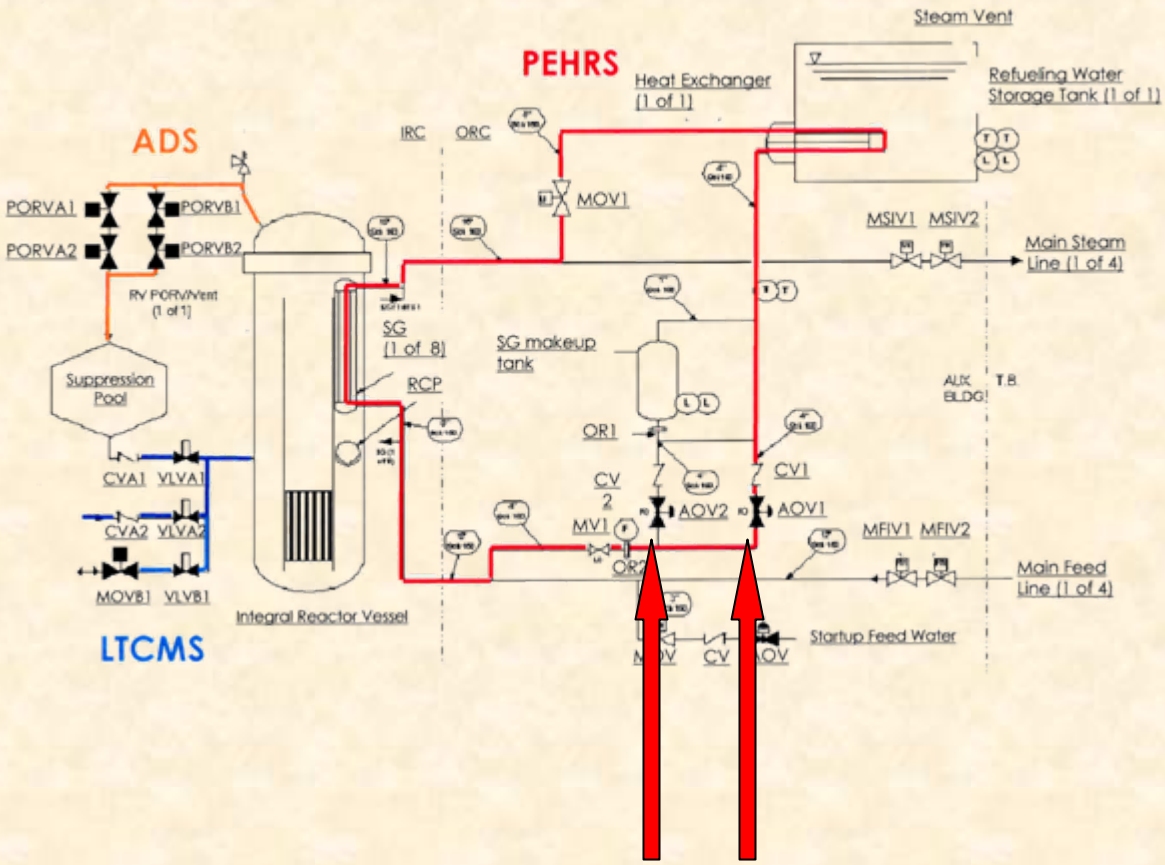


The Automatic Depressurization System (ADS) uses pressure relief valves to depressurize the reactor. Block valves are used to prevent an inadvertent blowdown.



There are 4 loops in the Emergency Heat Removal System (EHRS) that use natural circulation to remove heat from the reactor core.

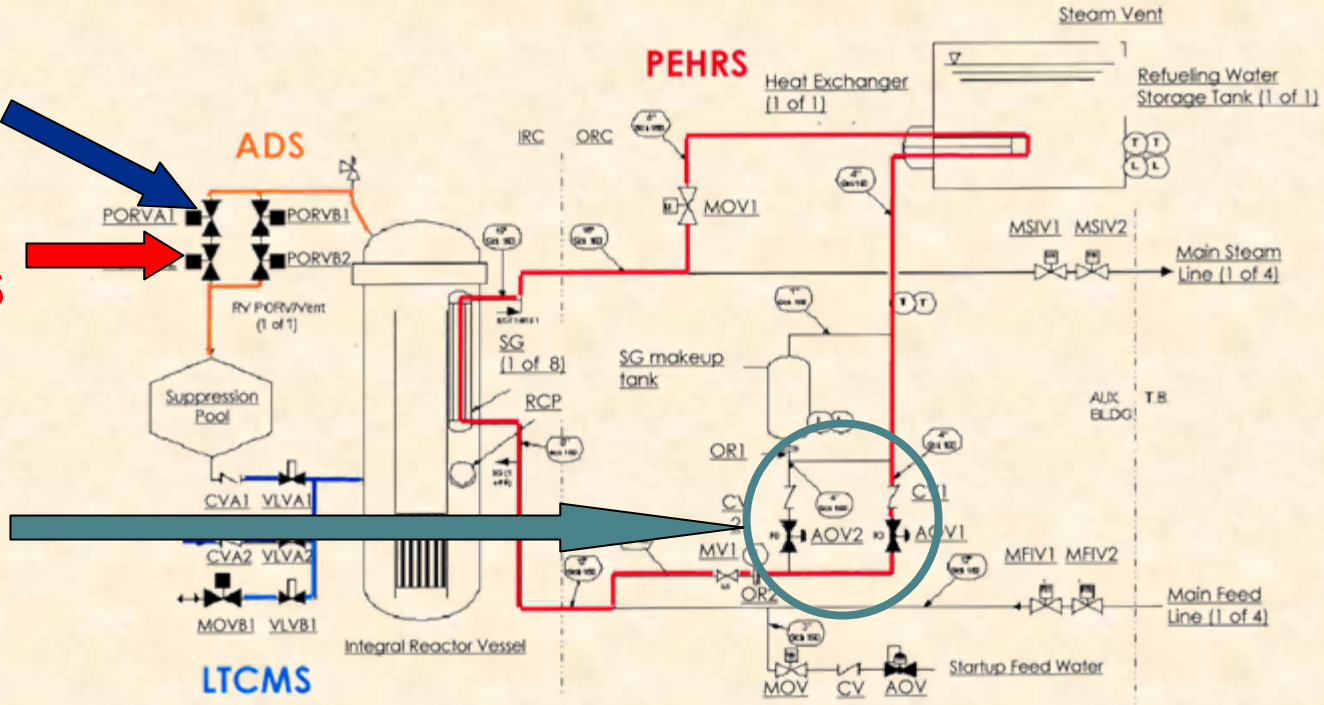




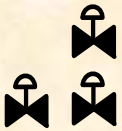
Either of these valves must open to initiate natural circulation cooling using the EHRS.

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**



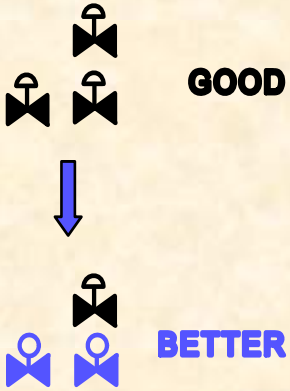
BASE CASE
ADS block valves closed
Valves in EHRS are AOVs



GOOD

The AOVs were originally chosen because they are the most reliable valves available.

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!

Changing the valves in the EHRS to valves with a higher failure rate actually improved the reliability of the system!

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!

Mixing the valve types provided an even more reliable system because it removed the common-cause failure contribution of the valves.

BASE CASE
ADS block valves closed
Valves in EHRS are AOVs

GOOD

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

BETTER

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

BETTER

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

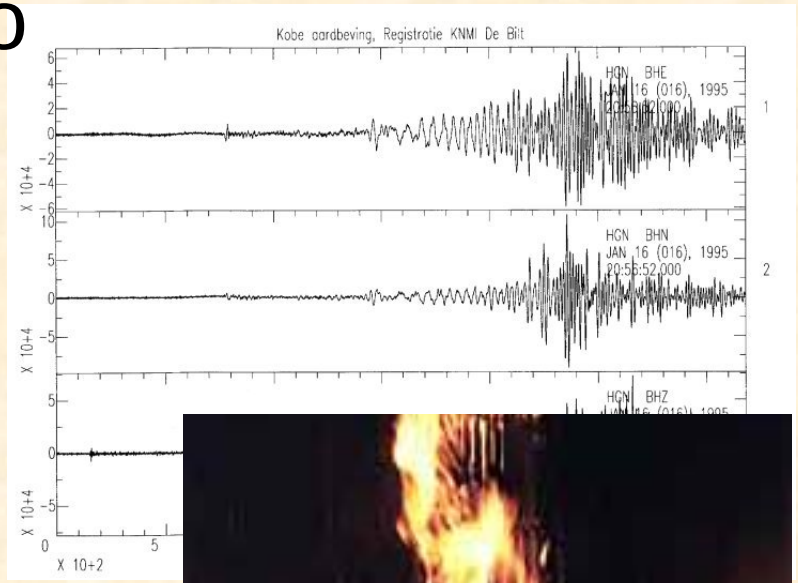
BEST

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