Modeling Common Cause Failures of Thrusters on ISS Visiting Vehicles

Megan Haught*and Gary Duncan
ARES Technical Services, Houston, TX, USA

Abstract: This paper discusses the methodology used to model common cause failures of thrusters on the International Space Station (ISS) Visiting Vehicles. The ISS Visiting Vehicles each have as many as 32 thrusters, whose redundancy and similar design make them susceptible to common cause failures. The Global Alpha Model (as described in NUREG/CR-5485) can be used to represent the system common cause contribution, but NUREG/CR-5496 supplies global alpha parameters for groups only up to size six. Because of the large number of redundant thrusters on each vehicle, regression is used to determine parameter values for groups of size larger than six. An additional challenge is that Visiting Vehicle thruster failures must occur in specific combinations in order to fail the propulsion system; not all failure groups of a certain size are critical.

Keywords: PRA, ISS, Common Cause, CCF, Global Alpha Model

1. INTRODUCTION

Common Cause Failure (CCF) events are dependent failures of (usually) redundant items not otherwise accounted for in a probabilistic risk model. Common cause failures can be due to many factors, including:

- Environmental factors (vibration, thermal stress, humidity, etc.)
- Manufacturing defects
- Human error (installation error, improper maintenance, etc.)
- Design error

A hypothetical ISS Visiting Vehicle propulsion system has 18 thrusters. The similar redundancy of the system makes it susceptible to common cause failures.

A typical common cause model considers a small number of redundant components, say two or three. It is reasonable to explicitly model individual common cause events when there are few components in a group. For example, suppose there are three redundant components, A, B, and C, and that failure of at least two of the components fails the system. There are four critical failure combinations of size two or more: AB, BC, AC, and ABC. It is straightforward to model these common cause events explicitly. Now suppose there are 18 redundant components, and that failure of at least four of the components fails the system. In this case there are a total of 261,156 critical combinations of size four or more. It is not reasonable to model this many common cause events explicitly, so a different method is needed in order to simplify the model.

The model can be made significantly more concise by lumping all common cause events into a single, global value that represents the common cause contribution for the entire system. One method for doing this is the Global Alpha Model, described in NUREG/CR-5485 [1]. An Excel-based tool that uses the Global Alpha Model to calculate the common cause contribution of a system with a large number of redundant components is the Global Alpha Model Uncertainty Tool (GAMUT), created by National Aeronautics and Space Administration (NASA) Safety and Mission Assurance (S&MA). The values calculated by GAMUT can be used in a Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) [2] fault tree.

An additional challenge with the ISS Visiting Vehicles is that not all thruster failure groups of a certain size are critical. In this example, failure of a certain number of thrusters out of 18 will fail the

*megan.b.haught@nasa.gov

system only if they occur in specific combinations. For typical common cause models, where all groups of a certain size are critical, GAMUT can calculate the number of groups of a given size that would fail the system. In this case, however, the critical combinations of failures must be calculated by hand. GAMUT then retrieves the common cause parameters for each possible number of failures and uses the equations from NUREG/CR-5485 to calculate the global common cause contribution.

GAMUT uses the 2009 update to NUREG/CR-5496 [3] as its source for the mean and uncertainty of the global alpha parameters. NUREG/CR-5496 provides alpha factors for specific component types (pumps, valves, etc.) as well as generic values. Features of the generic values include:

- Different values for demand versus rate
- Group sizes ranging from two to six
- Uncertainty parameters

GAMUT contains generic alpha values for groups of size two to 32. For values less than or equal to six, the GAMUT parameters are identical to the generic values from NUREG/CR-5496. Regression was used to determine parameter values for groups of size larger than six.

The example scenarios being considered to illustrate this approach are Abort and Collision. Each scenario has its own defined success criteria and therefore its own global common cause value.

2. ISS VISITING VEHICLE PROPULSION SYSTEM

2.1. Failure Rules

In the following configuration, 18 thrusters are arranged in four quadrants. Note that the configuration and failure rules given in Tables 1 and 2 do not reflect the actual configuration and failure rules of any of the ISS Visiting Vehicles, but are intended to serve only as an example.

Table 1: Thruster Configuration

Group Name	Q1	Q2	Q3	Q4
+Roll	D1T1	D2T1	D3T1	D4T1
-Roll	D1T2	D2T2	D3T2	D4T2
Aft (-X)	D1T3	D2T3	D3T3	D4T3
Forward (+X)	D1T4	D2T4	D3T4	D4T4
Forward (+X)	D1T5		D3T5	

The possible failure scenarios and results are given in the table below.

Table 2: Thruster Failure Rules

Failure Scenario	Result
≥1 thruster failure in a quadrant	Quadrant Failure
2 or 3 quadrant failures	Abort
4 quadrant failures	Collision

For example, the set of failures {D1T1, D1T3, D1T4} results in the failure of quadrant 1, but not in Abort or Collision. The set of failures {D2T3, D3T5} results in Abort, and the set of failures {D1T2, D2T4, D3T3, D4T1} results in Collision.

2.2. Combinatorial Failure Logic

Let k equal the number of thruster failures that have occurred. Clearly, when $k=1$, the result would be a quadrant failure, but not Abort or Collision. When $k=2$, the result is Abort only if the failures occur in different quadrants. For example, failure of {D1T1, D1T2} does not result in Abort, but failure of {D1T1, D2T1} does. The calculation of the total number of Abort failure groups when $k=2$, c_2^{Abort}, can be stated in words as follows. [Note that in the equations below, the terms $\begin{bmatrix} n \\ k \end{bmatrix}$ and $\begin{pmatrix} n \\ k \end{pmatrix}$ are both equal to $\frac{n!}{k!(n-k)!}$, and that the bracket notation is a convention to distinguish choosing groups from choosing members in a group.]

Choose both groups of five and choose one member from each group:

$$\begin{bmatrix} 2 \\ 2 \end{bmatrix}\begin{pmatrix} 5 \\ 1 \end{pmatrix}\begin{pmatrix} 5 \\ 1 \end{pmatrix}=25$$

Or, choose both groups of four and choose one member from each group:

$$\begin{bmatrix} 2 \\ 2 \end{bmatrix}\begin{pmatrix} 4 \\ 1 \end{pmatrix}\begin{pmatrix} 4 \\ 1 \end{pmatrix}=16$$

Or, choose one group of five, one group of four, and one member from each group:

$$\begin{bmatrix} 2 \\ 1 \end{bmatrix}\begin{bmatrix} 2 \\ 1 \end{bmatrix}\begin{pmatrix} 5 \\ 1 \end{pmatrix}\begin{pmatrix} 4 \\ 1 \end{pmatrix}=80$$

So, the total number of Abort failure groups when $k=2$ is:

$$c_2^{Abort}=\begin{bmatrix} 2 \\ 2 \end{bmatrix}\begin{pmatrix} 5 \\ 1 \end{pmatrix}\begin{pmatrix} 5 \\ 1 \end{pmatrix}+\begin{bmatrix} 2 \\ 2 \end{bmatrix}\begin{pmatrix} 4 \\ 1 \end{pmatrix}\begin{pmatrix} 4 \\ 1 \end{pmatrix}+\begin{bmatrix} 2 \\ 1 \end{bmatrix}\begin{bmatrix} 2 \\ 1 \end{bmatrix}\begin{pmatrix} 5 \\ 1 \end{pmatrix}\begin{pmatrix} 4 \\ 1 \end{pmatrix}=121$$

The minimum number of failures required for Collision is four. The only way that four failures will result in Collision is if there is one failure in each quadrant. When $k=4$, the total number of Collision failure groups is:

$$c_4^{Collision}=\begin{bmatrix} 2 \\ 2 \end{bmatrix}\begin{pmatrix} 5 \\ 1 \end{pmatrix}\begin{pmatrix} 5 \\ 1 \end{pmatrix}\begin{bmatrix} 2 \\ 2 \end{bmatrix}\begin{pmatrix} 4 \\ 1 \end{pmatrix}\begin{pmatrix} 4 \\ 1 \end{pmatrix}=400$$

However, when $k=4$ there are additional critical combinations that result in Abort, so when calculating c_4^{Abort} we subtract off the failure groups that result in Collision.

Thruster failure combinations not shown here require a similar but increasingly complicated combinatorial argument. The following table shows all the critical combinations for Abort and Collision for this configuration of thrusters.

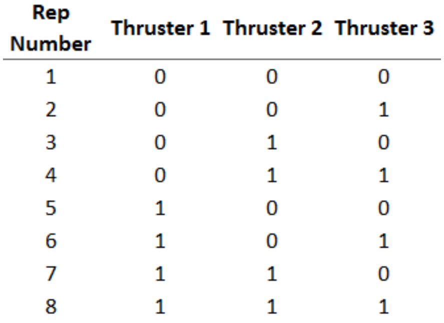
Table 3: Thruster Critical Combinations

Failures	Total Combinations	Abort Critical Combinations	Collision Critical Combinations
1	18	0	0
2	153	121	0
3	816	788	0
4	3,060	2,648	400
5	8,568	5,766	2,800
6	18,564	8,864	9,700
7	31,824	10,024	21,800
8	43,758	8,498	35,260
9	48,620	5,420	43,200
10	43,758	2,573	41,185
11	31,824	884	30,940
12	18,564	208	18,356
13	8,568	30	8,538
14	3,060	2	3,058
15	816	0	816
16	153	0	153
17	18	0	18
18	1	0	1

2.3. Brute Force Failure Logic

The combinatorial argument described above can be verified by Brute Force. In the Brute Force method, every possible combination of failures is listed (2^{18} = 262,144 combinations in this case) and for each, logic is applied to determine whether the combination is critical. For example, if there were three thrusters there would be 2^3 = 8 possible combinations of failure. Below, a one (1) represents failure and a zero (0) represents success.

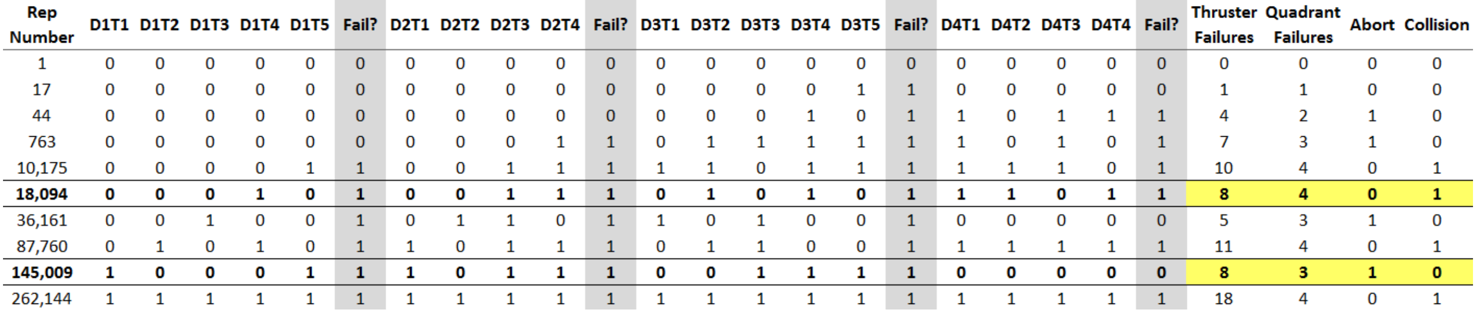
Figure 1: 2^3 Brute Force Failure Combinations



Rep Number	Thruster 1	Thruster 2	Thruster 3
1	0	0	0
2	0	0	1
3	0	1	0
4	0	1	1
5	1	0	0
6	1	0	1
7	1	1	0
8	1	1	1

The figure below is a sample of 10 of the 2^{18} possible failure combinations.

Figure 2: 2^{18} Brute Force Failure Combinations



Rep Number	D1T1	D1T2	D1T3	D1T4	D1T5	Fail?	D2T1	D2T2	D2T3	D2T4	Fail?	D3T1	D3T2	D3T3	D3T4	D3T5	Fail?	D4T1	D4T2	D4T3	D4T4	Fail?	Thruster Failures	Quadrant Failures	Abort	Collision
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	1	1	0	0
44	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	1	1	1	4	2	1	0
763	0	0	0	0	0	0	0	0	0	1	1	0	1	1	1	1	1	1	0	1	0	1	7	3	1	0
10,175	0	0	0	0	1	1	0	0	1	1	1	1	1	0	1	1	1	1	1	1	0	1	10	4	0	1
18,094	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**1**	**1**	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**1**	**1**	**0**	**1**	**1**	**8**	**4**	**0**	**1**
36,161	0	0	1	0	0	1	0	1	1	0	1	1	0	1	0	0	1	0	0	0	0	0	5	3	1	0
87,760	0	1	0	1	0	1	1	0	1	1	1	0	1	1	0	0	1	1	1	1	1	1	11	4	0	1
145,009	**1**	**0**	**0**	**0**	**1**	**1**	**1**	**0**	**1**	**1**	**1**	**0**	**0**	**1**	**1**	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**8**	**3**	**1**	**0**
262,144	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	18	4	0	1

The thrusters listed in the first row correspond to the configuration shown in Table 1. For example, {D1T1, D1T2, D1T3, D1T4, D1T5} are the thrusters in quadrant 1. If at least one thruster in a quadrant fails, the quadrant is considered failed. For example, suppose there are eight thruster failures. In the sample above, this occurs twice (rep 18,094 and rep 145,009). The first time, all four quadrants fail and the result is Collision. The second time, only three quadrants fail and the result is Abort. The Abort and Collision results are counted for every instance of eight failures, and the result is 8,498 instances of Abort and 35,260 instances of Collision. This matches the combinatorial output shown in Table 3.

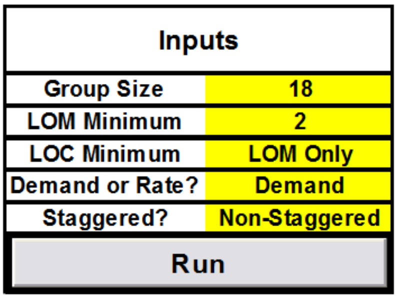
3. USING GAMUT

Once the critical combinations have been calculated, GAMUT is used to determine the common cause contribution of the thruster system to the end states Abort and Collision. For more details on the Global Alpha Model equations and their implementation in the GAMUT model logic, see the GAMUT documentation [4].

Common cause models require the assumption of either a staggered or a non-staggered system. In a staggered system, individual units can be tested and replaced as needed. In a non-staggered system, the items are installed and operated as a group; individual units cannot be isolated from the system and tested. ISS Visiting Vehicle thrusters are assumed to be non-staggered systems because there is no testing or replacement of individual units. ISS Visiting Vehicle thrusters are also assumed to operate on demand.

GAMUT requires the inputs shown below. For the ISS Visiting Vehicles, LOM = Abort and LOC = Collision. The group size is 18 and the results will be used for Abort. The minimum number of failures that can result in Abort is two. The Visiting Vehicle thrusters are a non-staggered system and operate on demand.

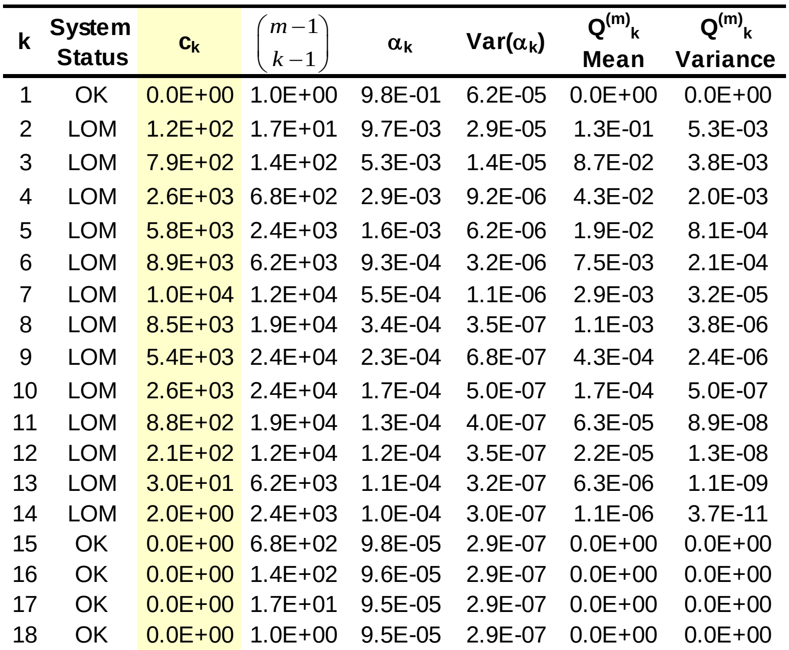
Figure 3: GAMUT inputs



Inputs	
Group Size	18
LOM Minimum	2
LOC Minimum	LOM Only
Demand or Rate?	Demand
Staggered?	Non-Staggered

After GAMUT is run, column c_k contains the number of critical combinations for each group of size k. GAMUT assumes that every group of a certain size is critical. For example, when $k = 2$, GAMUT calculates $c_2^{Abort} = \binom{18}{2} = 153$. But in the Visiting Vehicle thruster case, not all failure groups of a certain size are critical. A group of two failures is only critical if the failures occur in different quadrants, and so in the thruster case $c_2^{Abort} = 121$ as calculated in Section 2.2. So after running GAMUT, replace the column containing values for c_k with the numbers of "Abort Critical Combinations" given in Table 3. It is important that GAMUT is not run again after replacing these values, because this would overwrite the manually entered values for c_k.

Figure 4: Entering the Critical Combinations

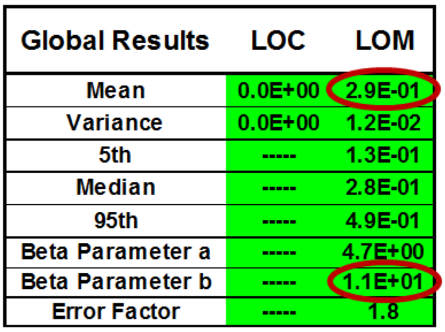


k	System Status	c_k	$\binom{m-1}{k-1}$	α_k	Var(α_k)	$Q^{(m)}_k$ Mean	$Q^{(m)}_k$ Variance
1	OK	0.0E+00	1.0E+00	9.8E-01	6.2E-05	0.0E+00	0.0E+00
2	LOM	1.2E+02	1.7E+01	9.7E-03	2.9E-05	1.3E-01	5.3E-03
3	LOM	7.9E+02	1.4E+02	5.3E-03	1.4E-05	8.7E-02	3.8E-03
4	LOM	2.6E+03	6.8E+02	2.9E-03	9.2E-06	4.3E-02	2.0E-03
5	LOM	5.8E+03	2.4E+03	1.6E-03	6.2E-06	1.9E-02	8.1E-04
6	LOM	8.9E+03	6.2E+03	9.3E-04	3.2E-06	7.5E-03	2.1E-04
7	LOM	1.0E+04	1.2E+04	5.5E-04	1.1E-06	2.9E-03	3.2E-05
8	LOM	8.5E+03	1.9E+04	3.4E-04	3.5E-07	1.1E-03	3.8E-06
9	LOM	5.4E+03	2.4E+04	2.3E-04	6.8E-07	4.3E-04	2.4E-06
10	LOM	2.6E+03	2.4E+04	1.7E-04	5.0E-07	1.7E-04	5.0E-07
11	LOM	8.8E+02	1.9E+04	1.3E-04	4.0E-07	6.3E-05	8.9E-08
12	LOM	2.1E+02	1.2E+04	1.2E-04	3.5E-07	2.2E-05	1.3E-08
13	LOM	3.0E+01	6.2E+03	1.1E-04	3.2E-07	6.3E-06	1.1E-09
14	LOM	2.0E+00	2.4E+03	1.0E-04	3.0E-07	1.1E-06	3.7E-11
15	OK	0.0E+00	6.8E+02	9.8E-05	2.9E-07	0.0E+00	0.0E+00
16	OK	0.0E+00	1.4E+02	9.6E-05	2.9E-07	0.0E+00	0.0E+00
17	OK	0.0E+00	1.7E+01	9.5E-05	2.9E-07	0.0E+00	0.0E+00
18	OK	0.0E+00	1.0E+00	9.5E-05	2.9E-07	0.0E+00	0.0E+00

4. GAMUT RESULTS

The results shown below represent the common cause contribution of this ISS Visiting Vehicle thruster system to the end state Abort. The common cause event in SAPHIRE should have a Beta distribution, and the values required by SAPHIRE are the Mean and Beta Parameter b. The common cause event needs to be multiplied by the independent failure probability in SAPHIRE using a compound event. The reader is directed to the document "Implementing a Global Alpha Common Cause Model in SAPHIRE" [5] for more details on how to correctly model a global alpha common cause model in SAPHIRE.

Figure 5: GAMUT Results



Global Results	LOC	LOM
Mean	0.0E+00	2.9E-01
Variance	0.0E+00	1.2E-02
5th	-----	1.3E-01
Median	-----	2.8E-01
95th	-----	4.9E-01
Beta Parameter a	-----	4.7E+00
Beta Parameter b	-----	1.1E+01
Error Factor	-----	1.8

Below are the GAMUT results for Abort and Collision for the given thruster configuration.

Table 4: Global Alpha Model Results

End State	Mean	Beta Parameter b
Abort	2.9E-01	11
Collision	5.5E-02	28

That is, 29% of all independent thruster failures are expected to be part of a common cause group that will result in system Abort.

5. MODEL CONSIDERATIONS

Common cause failures of the ISS Visiting Vehicle thrusters were previously modeled using a Beta Model, also described in NUREG/CR-5485 [1]. The Beta Model is easy to implement and is usually the default common cause model. It cannot, however, be used to assess the likelihood of Abort. The Beta Model assumes that any common cause failure results in the failure of every member of the group, and hence all outcomes of a Beta Model will necessarily result in Collision. The beta value that was used for common cause failures of Visiting Vehicle thrusters was $\beta = 1.1\text{E-}01$. That is, 11% of the time that a failure occurs, every item in the population fails. This generic beta screening value was originally believed to be conservative.

However, the ISS Visiting Vehicle thrusters have some unique properties. They comprise a very large group that can fail with as few as two failures. When $k = 2$, there are $\binom{18}{2} = 153$ possible combinations of two failures, of which 121 are critical (resulting in Abort). In the Global Alpha Model, given a failure, the fraction of failures that result in a group of size $k = 2$ is $\alpha_k = 9.7\text{E-}03$, a value extrapolated from the 2009 version of NUREG/CR-5496 [3]. The fraction of failures that are groups of size $k = 2$ in a group of size 18 is $Q_k^{(m)} = 1.3\text{E-}01$. This is already larger than the screening value of $\beta = 1.1\text{E-}01$, and is only for a group of size two; the end result includes common cause failure groups of all sizes.

When modeling common cause failures of ISS Visiting Vehicle thrusters, the Beta Model gives a lower result than the Global Alpha Model. This might seem counterintuitive. The Beta Model implicitly assumes alpha parameters for all failure group sizes, and like the Global Alpha Model it yields a single, global common cause value. Apparently, the implied alpha parameters used by the Beta Model are lower than the generic NUREG values used in this study. However, for more typical common cause models with a smaller number of components, the Beta Model might be appropriate for Collision considerations.

6. CONCLUSION

The methodology described here has been used to model common cause of thrusters and valves on all the ISS Visiting Vehicles, including Shuttle, as well as common cause failures of Russian Service Module (SM) thrusters, Beta Gimbal Assemblies (BGAs), the Low-Impact Docking System (LIDS), and power feeds to the Multipurpose Laboratory Module (MLM) and Functional Cargo Block (FGB). It is the recommended common cause methodology for any system with a large number of similar redundant components, particularly when specific failure combinations are required to fail the system, as it provides a comprehensive and representative calculation of the likelihood of specific common cause failure combinations.

References

[1] U.S. Nuclear Regulatory Commission, *Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment, NUREG/CR-5485*, November 1998.

[2] Idaho National Laboratory (INL$_{©}$), SAPHIRE$^{®}$, Version 7.27, Idaho Falls, Idaho.

[3] U.S. Nuclear Regulatory Commission, *CCF Parameter Estimations, 2009 Update to NUREG/CR-5496*, January 2011.

[4] Reistle, Bruce, *Global Alpha Model Uncertainty Tool (GAMUT)*, July 2011.

[5] Reistle, Bruce, *Implementing a Global Alpha Common Cause Model in SAPHIRE*, July 2009.