INL/CON-08-14535
PREPRINT

Common-Cause Failure Analysis in Event Assessment

ANS PSA 2008 Topical Meeting

Dana L. Kelly
Dale M. Rasmuson

September 2008

The INL is a
U.S. Department of Energy
National Laboratory
operated by
Battelle Energy Alliance

ANS PSA 2008 Topical Meeting - Challenges to PSA during the nuclear renaissance
Knoxville, Tennessee, September 7–11, 2008, on CD-ROM, American Nuclear Society, LaGrange Park, IL (2008)

COMMON-CAUSE FAILURE ANALYSIS IN EVENT ASSESSMENT[1]

Dana L. Kelly
Idaho National Laboratory
P. O. Box 1625, Idaho Falls, ID 83415
Dana.Kelly@inl.gov

Dale M. Rasmuson
U. S. Nuclear Regulatory Commission
Office of Nuclear Regulatory Research
Washington, DC 20555-0001
Dale.Rasmuson@nrc.gov

ABSTRACT

This paper describes the approach taken by the U. S. Nuclear Regulatory Commission to the treatment of common-cause failure in probabilistic risk assessment of operational events. The approach is based upon the Basic Parameter Model for common-cause failure, and examples are illustrated using the alpha-factor parameterization, the approach adopted by the NRC in their Standardized Plant Analysis Risk (SPAR) models. The cases of a failed component (with and without shared common-cause failure potential) and a component being unavailable due to preventive maintenance or testing are addressed. The treatment of two related failure modes (e.g., failure to start and failure to run) is a new feature of this paper. These methods are being applied by the NRC in assessing the risk significance of operational events for the Significance Determination Process (SDP) and the Accident Sequence Precursor (ASP) program.

Key Words: Common-cause failure, event assessment

1 INTRODUCTION

Event assessment is an application of probabilistic risk assessment (PRA) in which observed equipment failures and outages are mapped into the risk model to obtain a numerical estimate of the event's risk significance. Such an assessment can be either prospective, as when utilities use PRA as an aid in planning and scheduling equipment maintenance, or retrospective, such as in the Nuclear Regulatory Commission's Significance Determination Process. In this paper, we focus on retrospective assessments. The retrospective event assessment is still future-oriented, in the sense that one is trying to estimate the conditional probability of core damage, should the event occur again under nominally identical conditions. Because the actual event did not lead to core damage, one does not model the event exactly as it transpired, as this would lead to a conditional core damage probability (CCDP) of zero. Instead, one accounts for the possibility that equipment that functioned successfully in the actual event might, with some probability, fail to function in a future recurrence of the event. Thus, failure probabilities are left at their nominal

[1] This paper was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, of any information, apparatus, product, or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights. The views expressed in this paper are not necessarily those of the U.S. Nuclear Regulatory Commission.

values, or adjusted as necessary to reflect the conditions of the event. The adjustment to common-cause failure (CCF) probability is particularly important, as it is insufficient to simply leave CCF probabilities at their nominal values, and doing so may result in a significant underestimate of CCDP for the event.

The purpose of this paper is to extend earlier work on the treatment of CCF in event assessment [1] to the following three cases: (1) component failure with potential for CCF of redundant components, (2) failed component due to an independent cause (no CCF potential), and (3) component unavailable due to preventive maintenance or testing. Current NRC guidance is presented for identifying failures with no CCF potential, so-called independent failures. We also address CCF treatment for two failure modes (e.g., failure to start and failure to run).

2 REVIEW OF BASIC PARAMETER MODEL ASSUMPTIONS AND ALPHA-FACTOR PARAMETERIZATION

The Basic Parameter Model [2] expands the failure probability (or failure rate) of a component in a common-cause component group (CCCG) into terms involving independent failure of the component and combinations of CCFs with the other components in the CCCG. For example, in a CCCG with three redundant components, designated A, B, and C, we would have the following expansions:

$$\begin{aligned} A_t &= A_I \cup C_{AB} \cup C_{AC} \cup C_{ABC} \\ B_t &= B_I \cup C_{AB} \cup C_{BC} \cup C_{ABC} \\ C_t &= C_I \cup C_{AC} \cup C_{BC} \cup C_{ABC} \end{aligned} \tag{1}$$

The terms in Eq. 1 are defined as follows.

A_t = Total failure of A from all causes,
B_t = Total failure of B from all causes,
C_t = Total failure of C from all causes,
A_I = failure of A from independent causes,
B_I = failure of B from independent causes,
C_I = failure of C from independent causes,
C_{AB} = failure of A and B from common causes,
C_{AC} = failure of A and C from common causes,
C_{BC} = failure of B and C from common causes,
C_{ABC} = failure of A, B, and C from common causes.

As discussed in [2], a common convention is to treat Eq. 1 as a partition, so the events in the partition are considered to be mutually exclusive. This leads to cut sets such as $\{C_{AB}, C_{AC}\}$, $\{C_{AB}, C_{BC}\}$, and $\{C_{AC}, C_{BC}\}$ for a CCCG with a two-of-three success criterion being dropped. This is a reasonable convention as it is difficult to justify the validity of such cut sets. In practice it is difficult to distinguish them from C_{ABC}, and they contribute insignificantly to the total probability of failure of the CCCG.

The BPM for CCF contains an underlying assumption of symmetry: the probabilities of similar events involving similar components (i.e., events in the same CCCG) are the same. This approach takes advantage of the physical symmetries associated with identical redundant components in reducing the number of parameters that need to be quantified. For example, in Eq. 1 it is typically assumed that

$$\begin{aligned} \Pr[A_I] = \Pr[B_I] = \Pr[C_I] &= Q_1 \\ \Pr[C_{AB}] = \Pr[C_{AC}] = \Pr[C_{BC}] &= Q_2 \\ \Pr[C_{ABC}] &= Q_3 \end{aligned} \tag{2}$$

In other words, the probability of occurrence of any basic event within a given CCCG is assumed to depend only on the number and not on the specific components in that basic event. This is called the **symmetry assumption**. The situation in which this assumption is not satisfied as a result of a degraded component is analyzed in [3].

Thus, for a CCCG of size m, the BPM defines

$$Q_t = \sum_{k=1}^{m} \binom{m-1}{k-1} Q_k^{(m)} \tag{3}$$

In Eq. 3 $Q^{(m)}_k$ = probability of a CCBE involving k specific components in a CCCG of size m, ($1 \le k \le m$) .

2.1 Alpha-Factor Parameterization of BPM

For several practical reasons, it is often more convenient to rewrite the $Q^{(m)}_k$'s of the BPM in terms of other more easily quantifiable parameters. For this purpose the U. S. NRC has adopted a parametric model known as the alpha factor model [2]. The alpha-factor model develops CCF probabilities from a set of failure ratios and the total component failure probability (Q_t). The parameters of the model are

Q_t = total failure probability of each component due to all independent and CCF events.
α_k = fraction of the total number of failure events that occur in the CCCG that involve the failure of k components due to a common cause.

Using these parameters, depending on the assumption regarding the way components in the CCCG are tested, the probability of a CCBE involving failure of k components in a CCCG of m components is given by the following (see [2]):

- For a staggered testing scheme:

$$Q_k^{(m)} = \frac{1}{\binom{m-1}{k-1}} \alpha_k Q_t \tag{4}$$

- For a non-staggered testing scheme or if there is no testing scheme:

$$Q_k^{(m)} = \frac{k}{\binom{m-1}{k-1}} \frac{\alpha_k}{\alpha_t} Q_t \tag{5}$$

where

$$\alpha_t = \sum_{k=1}^{m} k\alpha_k \ . \tag{6}$$

3 CONDITIONAL PROBABILITY AND EVENT ASSESSMENT

Conditional probability is defined by the following:

$$\begin{aligned} \Pr[A \mid B] &= \frac{\Pr[A \cap B]}{\Pr[B]} \text{ provided } \Pr[B] > 0 \text{ or} \\ \Pr[B \mid A] &= \frac{\Pr[A \cap B]}{\Pr[A]} \text{ provided } \Pr[A] > 0. \end{aligned} \tag{7}$$

Note that if $A \cap B = \varnothing$, then Pr[A|B] = 0. A set of events cannot be both mutually exclusive and statistically independent. Two events, A and B, are said to be statistically independent if and only if $\Pr[A \cap B] = \Pr[A]\Pr[B]$. If A and B are statistically independent, then Pr[A|B] = Pr[A] and Pr[B|A] = Pr[B].

Basically, when we want to estimate the probability of an event, conditional upon the occurrence of another event, we are conditioning on the event that has occurred. Thus, the proper figure of merit is a conditional probability. That is,

$$\Pr[S \mid E] = \frac{\Pr[S \cap E]}{\Pr[E]}. \tag{8}$$

4 EXAMPLE PROBLEM TO ILLUSTRATE CCF ADJUSTMENTS

Consider a CCCG of size three. We denote the components by A, B, and C. We will consider two CCF-susceptible failure modes – failure to start, denoted by S, and failure to run, denoted by R. The S and R can be a superscript, subscript, or a regular letter, depending upon the context. We will present the details of the calculation for this case to illustrate how the result depends upon the underlying BPM and associated simplifying assumptions and the definition of conditional probability.

Using the BPM, we define the total failure to start of component A by the following equation:

$$A_t^S = A_S \cup S_{AB} \cup S_{AC} \cup S_{ABC} \tag{9}$$

where

A_t^S = Total Failure to start of component A from all causes
A_S = Failure to start of component A from independent causes
S_{AB} = Failure of components A and B to start due to common causes
S_{AC} = Failure of components A and C to start due to common causes
S_{ABC} = Failure of components A, B, and C to start due to common causes

As mentioned earlier, we will follow the suggested convention of [2] and assume that this representation of A_t^S constitutes a partition.

Similarly, we define total failure to start of components B and C by the following equations:

$$B_t^S = B_S \cup S_{AB} \cup S_{BC} \cup S_{ABC}$$
$$C_t^S = C_S \cup S_{AC} \cup S_{BC} \cup S_{ABC} \quad (10)$$

The terms in these equations are defined analogously to the ones for component A.

We define total failure to run of component A by a similar equation:

$$A_t^R = A_R \cup R_{AB} \cup R_{AC} \cup R_{ABC} \quad (11)$$

where

A_t^R = Total failure to run of component A from all causes

A_t^R = Total Failure to run of component A from all causes
A_R = Failure to run of component A from independent causes
R_{AB} = Failure of components A and B to run due to common causes
R_{AC} = Failure of components A and C to run due to common causes
R_{ABC} = Failure of components A, B, and C to run due to common causes

Similarly, we define total failure to run of components B and C by the following equations:

$$B_t^R = B_R \cup R_{AB} \cup R_{BC} \cup R_{ABC}$$
$$C_t^R = C_R \cup R_{AC} \cup R_{BC} \cup R_{ABC} \quad (12)$$

The terms of these equations are defined analogously to the ones for component A.

The success criterion we will consider is that one of the three components must function. Thus, to have failure of the system, all three components must fail. They can fail to start or fail to run. The fault tree is shown in Figure 1. Note that this is not typical of most PRA fault trees, as it has been expanded to include all elements of the BPM, which are needed for the exact solution. Table I lists the failure probabilities for the failure-to-start and failure-to-run modes, including CCF parameters. Table II lists the basic event probabilities produced by the alpha-factor parameterization of the BPM, assuming staggered testing.

Table III shows the quantified cut sets. Note that cut sets such as $S_{AB}S_{AC}$ have not been included, as discussed above. However, other similarly structured cut sets, such as $R_{AC}S_{BC}$ are included, because each term is a contributor to the total failure probability of a component to run or start, respectively. Hence, in order to conserve the total probability of failure for each component, these terms must be included. The total failure probability for the 3-train CCCG is 1.24×10^{-4}.

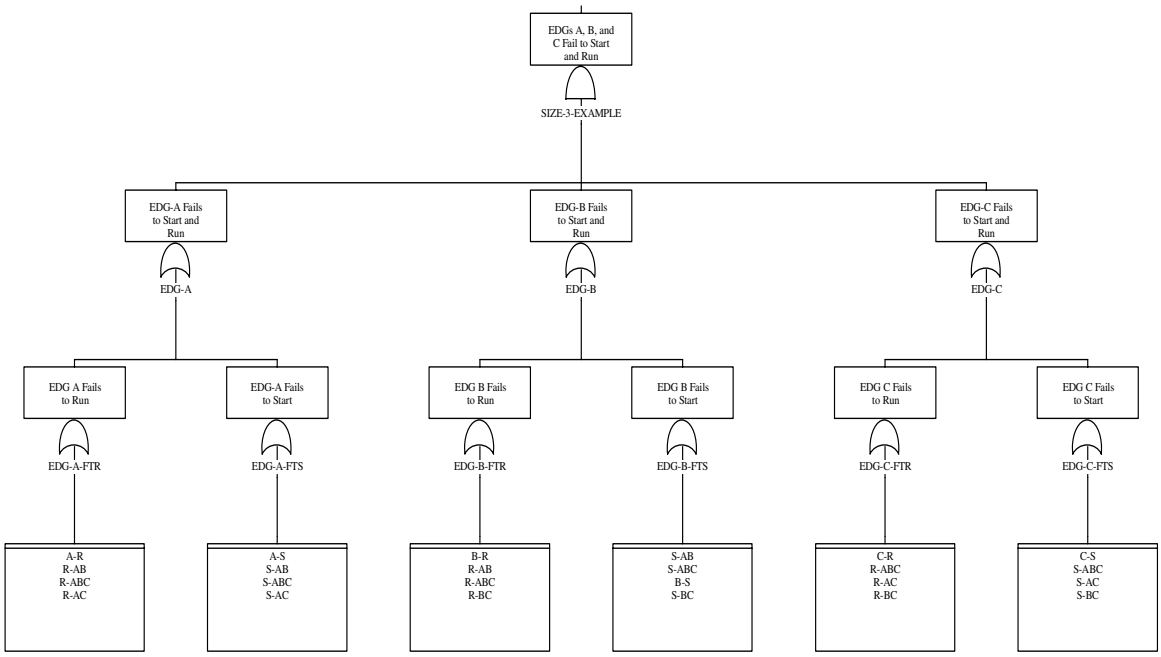

Figure 1 Example fault tree for two failure modes and three components

Table I Component failure mode probabilities for Figure 1

Failure to Start				Failure to Run			
		Q_T	5.000E-03			Q_T	1.193E-02
α_1	0.98195	Q_1	4.910E-03	α_1	0.97029	Q_1	1.158E-02
α_2	0.0134	Q_2	3.350E-05	α_2	0.0223	Q_2	1.330E-04
α_3	0.00465	Q_3	2.325E-05	α_3	0.00741	Q_3	8.840E-05

Table II Basic event probabilities for Figure 1

Basic Event	Failure Probability	Basic Event	Failure Probability
A-S	4.91E-03	A-R	1.16E-02
B-S	4.91E-03	B-R	1.16E-02
C-S	4.91E-03	C-R	1.16E-02
S-AB	3.35E-05	R-AB	1.33E-04
S-AC	3.35E-05	R-AC	1.33E-04
S-BC	3.35E-05	R-BC	1.33E-04
S-ABC	2.33E-05	R-ABC	8.84E-05

Table III Cut set probabilities for fault tree in Figure 1

Cut set	Cut set Probability	Cut set	Cut set	Cut set Probability	Cut set
1	8.840E-05	R-ABC	15	3.886E-07	A-R, S-BC
2	2.325E-05	S-ABC	16	2.797E-07	A-R, B-S, C-S
3	1.561E-06	A-R, B-R, C-R	17	2.797E-07	A-S, B-S, C-R
4	1.543E-06	B-R, R-AC	18	2.797E-07	A-S, B-R, C-S
5	1.543E-06	C-R, R-AB	19	1.645E-07	C-S, S-AB
6	1.543E-06	A-R, R-BC	20	1.645E-07	B-S, S-AC
7	6.607E-07	A-R, B-S, C-R	21	1.645E-07	A-S, S-BC
8	6.607E-07	A-R, B-R, C-S	22	1.184E-07	A-S, B-S, C-S
9	6.607E-07	A-S, B-R, C-R	23	4.455E-09	R-AC, S-AB
10	6.530E-07	B-S, R-AC	24	4.455E-09	R-BC, S-AB
11	6.530E-07	C-S, R-AB	25	4.455E-09	R-AB, S-AC
12	6.530E-07	A-S, R-BC	26	4.455E-09	R-BC, S-AC
13	3.886E-07	C-R, S-AB	27	4.455E-09	R-AB, S-BC
14	3.886E-07	B-R, S-AC	28	4.455E-09	R-AC, S-BC
Total 1.244E-04			**Total CCF 1.20E-04**		

4.1 Failure to Start with CCF Potential

We now estimate the conditional failure probability of the CCCG given that component A fails to start, and this failure has the potential to be shared with the other two components in the CCCG. To obtain the cut sets for the numerator of the calculation, we construct a fault tree with the top event in Figure 1 ANDed with A_T^S. Table IV lists the 22 cut sets for this case along with the numerical results. Note that, among these results, are cut sets such as {A-S, R-ABC}. This cut set may appear odd, as it seems to imply that component A both fails to start and fails to run. However, R-ABC is a contributor to the total *failure-to-run* probability of components B and C. This probability has not been changed by the failure of A to start, so such terms remain in the results.

The conditional failure probability is obtained by dividing each cut set's probability by the total failure-to-start probability of component A (i.e., 0.005). The results are contained in the last column of Table IV. The total conditional probability is equal to 5.400×10^{-3}.

4.2 Independent Failure to Start

Conditioning upon an independent component failure (i.e., a failure with no potential for shared common-cause mechanisms with other components in the CCCG) is the exception, rather than the rule. The NRC guidance specifies that this can be done if there is clear and convincing evidence of either no shared cause or no coupling factor between the failed component and other components in the CCCG, the latter being a very unlikely outcome for a group of redundant (as opposed to diverse) components.

Assume that the success criterion for the CCCG is 1-of-3. The numerator cut sets for the conditional probability that the CCCG fails, given that component "A" has failed independently, are derived in Eq. 13. In deriving this result we have applied the assumption that the BPM constitutes a partition of each failure mode. This leads to the elimination of cut sets such as $A_I^S C_I^R C_{AB}^S$.

$$\begin{aligned} S \bigcap A_I^S = {} & A_I^S B_I^R C_I^R \bigcup A_I^S B_I^R C_I^S \bigcup A_I^S B_I^S C_I^R \bigcup A_I^S B_I^S C_I^S \\ & \bigcup A_I^S B_I^R C_{AC}^R \bigcup A_I^S C_I^R C_{AB}^R \bigcup A_I^S C_{BC}^S \bigcup A_I^S C_{BC}^R \\ & \bigcup A_I^S B_I^S C_{AC}^R \bigcup A_I^S C_I^S C_{AB}^R \bigcup A_I^S C_{ABC}^R \end{aligned} \tag{13}$$

The results of applying this calculation to our size-three example above are shown in Table V.

Table IV Cut sets and probabilities given component A fails to start with CCF potential

No.	Cut Set	Cut Set Probability	Conditional Probability
1	S-ABC	2.325E-5	4.65E-03
2	A-S, B-R, C-R	6.607E-7	1.32E-04
3	A-S, R-BC	6.530E-7	1.31E-04
4	A-S, R-ABC	4.340E-07	8.68E-05
5	B-R, S-AC	3.886E-7	7.77E-05
6	C-R, S-AB	3.886E-7	7.77E-05
7	A-S, B-S, C-R	2.790E-7	5.58E-05
8	A-S, B-R, C-S	2.790E-7	5.58E-05
9	A-S, S-BC	1.645E-07	3.29E-05
10	B-S, S-AC	1.645E-07	3.29E-05
11	C-S, S-AB	1.645E-07	3.29E-05
12	A-S, B-S, C-S	1.184E-07	2.37E-05
13	A-S, C-R, R-AB	7.575E-09	1.52E-06
14	A-S, B-R, R-AC	7.575E-09	1.52E-06
15	R-AB, S-AC	4.455E-09	8.91E-07
16	R-BC, S-AC	4.455E-09	8.91E-07
17	R-AC, S-AB	4.455E-09	8.91E-07
18	R-BC, S-AB	4.455E-09	8.91E-07
19	A-S, C-S, R-AB	3.206E-09	6.41E-07
20	A-S, B-S, R-AC	3.206E-09	6.41E-07
21	R-ABC, S-AC	2.961E-09	5.92E-07
22	R-ABC, S-AB	2.961E-09	5.92E-07
Total		**2.699E-05**	**5.400E-03**
CCF		**2.565E-05**	**5.13E-03**

Table V Cut sets and conditional probabilities given A fails to start with no CCF potential

No.	Cut Sets	Cut Set Probability	Conditional Probability
1	A-S, B-R, C-R	6.607E-07	1.35E-04
2	A-S, R-BC	6.530E-07	1.33E-04
3	A-S, R-ABC	4.340E-007	8.84E-05
4	A-S, B-S, C-R	2.797E-07	5.70E-05
5	A-S, B-R, C-S	2.797E-07	5.70E-05
6	A-S, S-BC	1.645E-07	3.35E-05
7	A-S, B-S, C-S	1.184E-07	2.41E-05
8	A-S, C-R, R-AB	7.575E-09	1.54E-06
9	A-S, B-R, R-AC	7.575E-09	1.54E-06
10	A-S, C-S, R-AB	3.206E-09	6.53E-07
11	A-S, B-S, R-AC	3.206E-09	6.53E-07
Total		**2.61E-06**	**5.32E-04**
CCF		**1.272E-06**	**2.59E-04**

4.3 Test or Preventive Maintenance Outage

In this case the condition is that one component in a CCCG is out of service for preventive maintenance or testing. We will again consider a CCCG of size 3, with components designated A, B, and C, and a one-of-three success criterion. We will assume that component A is unavailable due to preventive maintenance and that it is not in a failed state (as it would be if the maintenance outage were for corrective maintenance). Although component A is out for preventive maintenance and thus cannot itself fail, the potential exists for causes and coupling factors still to be shared between component A and the other components in the CCCG. That is, C_{AC}, C_{AB}, and C_{ABC} have not occurred, but they could occur. These events now represent shocks that have the potential to fail components A and C, A and B, or A, B, and C, respectively. An alternative perspective is that removing component A from service has not affected the total failure probability for either of the other two components, and the total failure probability, by the BPM, includes terms such as C_{AC}, C_{AB}, and C_{ABC}. Since component A is unavailable, but not failed, the cut sets for this case reduce to

$$S = \left\{ \begin{array}{l} B_I^R C_I^R, B_I^S C_I^R, B_I^R C_I^S, B_I^S C_I^S, \\ C_{BC}^R, B_I^R C_{AC}^R, C_I^R C_{AB}^R, C_{BC}^S, B_I^S C_{AC}^S, \\ C_I^S C_{AB}^S, B_I^R C_{AC}^S, B_I^S C_{AC}^R, C_I^R C_{AB}^S, C_I^S C_{AB}^R, \\ C_{ABC}^S, C_{ABC}^R \end{array} \right\} \tag{14}$$

Applying the values in Table II to this equation, the system failure probability with component A out for preventive maintenance becomes 5.66E-04, an increase from the nominal value of 1.24E-04 shown in Table III. The CCF probability becomes 2.84E-04, about a factor of 2 higher than the nominal value.

5 SUMMARY

We have illustrated three cases for CCF adjustment, using a three-train CCCG with a one-of-three success criterion: the default case of failure with CCF potential, independent failure, and outage for preventive maintenance or testing. Table VI summarizes the results of these calculations. As this table shows, failure with CCF potential has the largest impact on the conditional failure probability of the CCCG, causing it to increase over an order of magnitude from the nominal case. Independent failure of a component or outage for preventive maintenance or testing results in a significantly smaller increase in the CCCG failure probability.

Table VI Summary of Calculations

Case	Conditional CCCG Failure Probability	Conditional CCF Probability
Nominal	1.244E-04	1.20E-04
Failure of component with CCF potential	5.400E-03	5.13E-03
Independent component failure	5.320E-04	2.59E-04
Preventive maintenance or testing outage of component	5.660E-04	2.84E-04

6 REFERENCES

1. Rasmuson, Dale M., "Treatment of Common-Cause Failures in Event Assessment," Probabilistic Safety Assessment and Management 4, New York, 1998.

2. Pickard, Lowe, and Garrick, Inc., *Procedures for Treating Common Cause Failures in Safety and Reliability Studies,* U. S. Nuclear Regulatory Commission, NUREG/CR-4780, 1988.

3. Rasmuson, Dale M. and Kelly, Dana L, "Common-Cause Failure Analysis in Event Assessment," *Journal of Risk and Reliability*. Accepted for publication.