SANDIA REPORT

SAND2011-3186
Unlimited Release
Printed May 2011

Techniques to Evaluate the Importance of Common Cause Degradation on Reliability and Safety of Nuclear Weapons

John L. Darby

Prepared by
Sandia National
Laboratories
Albuquerque, New Mexico 87185 and Livermore, California
94550

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd.
Springfield, VA 22161

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.fedworld.gov
Online order:

SAND2011-3186
Unlimited Release
Printed May 2011

Techniques to Evaluate the Importance of Common Cause Degradation on Reliability and Safety of Nuclear Weapons

John L. Darby
Systems Analysis, Org. 00241
Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-MS0415

Abstract

As the nuclear weapon stockpile ages, there is increased concern about common degradation ultimately leading to common cause failure of multiple weapons that could significantly impact reliability or safety. Current acceptable limits for the reliability and safety of a weapon are based on upper limits on the probability of failure of an individual item, assuming that failures among items are independent. We expanded the current acceptable limits to apply to situations with common cause failure. Then, we developed a simple screening process to quickly assess the importance of observed common degradation for both reliability and safety to determine if further action is necessary. The screening process conservatively assumes that common degradation is common cause failure. For a population with between 100 and 5000 items we applied the screening process and conclude the following. In general, for a reliability requirement specified in the Military Characteristics (MCs) for a specific weapon system, common degradation is of concern if more than 100(1 – x)% of the weapons are susceptible to common degradation, where x is the required reliability expressed as a fraction. Common degradation is of concern for the safety of a weapon subsystem if more than 0.1% of the population is susceptible to common degradation. Common degradation is of concern for the safety of a weapon component or overall weapon system if two or more components/weapons in the population are susceptible to degradation. Finally, we developed a technique for detailed evaluation of common degradation leading to common cause failure for situations that are determined to be of concern using the screening process. The detailed evaluation requires that best estimates of common cause and independent failure probabilities be produced. Using these techniques, observed common degradation can be evaluated for effects on reliability and safety.

ACKNOWLEDGMENTS

The author appreciates the review comments from Steven Hatch, Robert Waters, and Lawrence Sanchez of Sandia National Laboratories (SNL).

CONTENTS

FIGURES

TABLES

NOMENCLATURE

DOE	Department of Energy
LAC	Lightning Arrestor Connector
MC	Military Characteristics
SNL	Sandia National Laboratories
STS	Stockpile to Target Sequence

1 Introduction

As the nuclear weapon stockpile ages, there is increased concern about common degradation of weapons that can impact reliability or safety. For example, testing may indicate that the current supplied by a battery is decreasing in magnitude for all weapons with the battery due to material aging effects.

Common degradation is significant as it can ultimately lead to common cause failure that can greatly increase the probability that multiple weapons fail. For example, if the probability of failure of a weapon to perform reliably is 0.1- a reasonable upper acceptable limit assuming independent failure- the probability that a large number (large fraction of the population) of weapons fail is negligible. But, if the failure is common to all weapons, the probability that all weapons fail is 0.1. Thus, a technique is needed to quickly evaluate the significance of observed common degradation.

Current acceptable limits for the reliability and safety of a weapon are based on upper limits on the probability of failure of an individual item, assuming that failures among items are independent. For example, the number of items in a sample for estimating reliability was historically determined assuming independent failures. [Weapon Reliability Guide] [Sample with Common Cause]

If common cause degradation is observed during surveillance or other testing and evaluation activities, it is desirable to have criteria to quickly determine the significance of the degradation as a potential common cause failure.[1] We expanded the current acceptable limits to apply to situations with common cause failure, and developed a screening process to rapidly assess the importance of common cause degradation for both reliability and safety to determine if further immediate action is necessary. Also we developed a process for detailed evaluation of cases determined to be of concern based on the screening process.

The expanded criteria and screening process provide Sandia with the capability to quickly evaluate the importance of observed common cause degradation on safety and reliability. The detailed evaluation process provides Sandia with the capability to evaluate the significance of cases that are deemed to be of concern based on the screening evaluation. Both could help guide future surveillance activities.

[1] As discussed in an earlier report, in a sample of items selected for surveillance, it can be easier to detect common cause degradation or failure than to detect independent failure because common cause affects multiple items simultaneously. [Sample with Common Cause]

1.1 Reliability and Safety Acceptance Criteria

Reliability is concerned with an entire weapon system operating as designed. Weapon reliability is defined as the probability that the weapon detonates at the desired yield at the target. The weapon reliability is used in war planning and is therefore important for the success of military operations. For a weapon system, the reliability is generally on the order of 0.9 with specific reliability requirements provided in the Military Characteristics (MCs). For reliability, the maximum acceptable probability of failure (one minus the reliability) is taken to be 0.1 in this report.[2]

Safety for a nuclear weapon focuses on preventing premature detonation.[3] Safety can be evaluated at three levels: overall weapon system, weapon subsystem, or weapon component.

Safety goals for an overall weapon are based on the Walske criteria. For normal environments, the probability of premature detonation of a weapon is required to not exceed 10^{-9} during the lifetime of the weapon. Given an abnormal environment, the probability of premature detonation of a weapon is required to not exceed 10^{-6}. Normal and abnormal environments are specified in the Stockpile to Target Sequence (STS) for a specific weapon system.

A weapon consists of three safety subsystems: the arming subsystem, the intent subsystem, and the trajectory subsystem. Each subsystem consists of various components; for example, the intent strong link is a component in the intent subsystem and the trajectory strong link is a component in the trajectory subsystem. Each subsystem is designed to have a failure probability of no more than 10^{-3}. All three subsystems are qualified for normal environments, but only the intent and trajectory subsystems are qualified for abnormal environments. Assuming independence among the three subsystems, the 10^{-9} goal for normal environments is met by the three safety subsystems, and the 10^{-6} goal for abnormal environments is met by the intent and trajectory subsystems.

A component of concern for safety in any of the three safety subsystems is designed to have a failure probability no more than 10^{-4}.

In general, failures of concern for reliability are different than failures of concern for safety. For example, failure of a strong link in the open position is a concern for reliability not safety; conversely, failure of a strong link in the closed position is a concern for safety not reliability.

---

[2] The actual reliability is weapon system specific and is specified in the MCs. In this study we take the reliability as 0.9 to illustrate the process; in application, the actual reliability required by the MCs should be used. The safety goals based on the Walske criteria are not weapon system specific. In this study we use values for the safety goals based on the Walske criteria.

[3] Other safety concerns, such as preventing Pu dispersal, are also important but are not explicitly addressed in this report. The techniques provided in this report can be applied to such safety concerns given appropriate safety goals.

In this study, we consider a population in the range [100, 5000] which could be a portion of a specific weapon system or the entire stockpile.

For reliability we are concerned with the overall weapon. For safety, depending on the issue, we may be concerned with a weapon component, subsystem, or overall weapon system. We will use the term "item" to refer to the entity of concern: an overall weapon for reliability, or a weapon component, subsystem, or overall weapon for safety.

2 The Screening Process

Here we summarize a screening process to quickly assess the importance of common cause degradation for both reliability and safety and determine if further action is necessary.

For the screening process, it is assumed that the observed common degradation is a guaranteed common cause failure (the worst case). If the degradation treated as a common cause failure is acceptable, immediate further action is not required; otherwise, a timely follow-on detailed evaluation should be performed as discussed in Section 3, where the actual probability of common cause failure is considered.

We use the current acceptable limits for the probability of independent failure to screen for situations of common cause failure.

As discussed in Section 1, acceptable limits for the probability of failure of an item implicitly assume each item fails independently. Table 2-1 summarizes the acceptable limits used in this study. $P_{indep\ max}$ is the maximum independent failure probability of an item that is acceptable. As previously discussed, we assume the required reliability is 0.9; $P_{indep\ max}$ is one minus the reliability or 0.1.

Table 2-1 Acceptable Independent Failure Limits

Situation	Maximum Independent Probability of Failure of an Item ($P_{indep\ max}$)
Reliability of a weapon system taken as 0.9 [4]	0.1 [4]
Safety of a weapon system Normal environment Abnormal environment	 10^{-9} 10^{-6}
Safety of a weapon subsystem	10^{-3}
Safety of a weapon component	10^{-4}

[4] In an actual application, the weapon system reliability required by the MCs should be used.

To illustrate the problem with using the limits from Table 2-1 in the presence of common cause failure, consider the following situation.

A population of 1000 weapons has a reliability of 0.9; that is, the independent failure probability for a weapon is 0.1, the limit in Table 2-1. The expected number of failures (mean) is therefore 100; that is, if all 1000 weapons were executed, the best estimate is that 100 would fail.

Since common cause failure affects multiple weapons, we need to think about the probability that multiple weapons in the population fail. That is, we need to expand our discussion of reliability beyond the probability that an individual weapon fails to the probability that multiple weapons fail.

Let $P_{j,m}$ denote the probability that "j" or more of "m" total items fail, where m is the population of weapons of interest. As subsequently discussed in Section 3, the probability that j or more items fail independently can be calculated using the Cumulative Distribution Function (CDF) of the binomial distribution as:

$$P_{j,m\ no\ common\ cause} = 1 - CDF_{m,P_{indep}}(j-1) \qquad \text{(Eqn. 1)}$$

P_{indep} is the actual independent failure probability of an item.[5] The CDF is discussed in Section 3. Let μ denote the mean (expected value) of this binomial distribution.

Figure 2-1 shows $P_{j,m\ no\ common\ cause}$ as a function of j for a population of 1000 items each with an independent failure probability of 0.1, $P_{indep\ max}$ for reliability.[6] Note that the number of items that fail is discrete (not continuous), hence the plot in Figure 2-1 is for discrete (integer) values of j. It can be seen that the probability of multiple weapon failures starts to drop for j greater than about 90, and the probability that significantly more than the expected value (100) fail is very small. For example, the probability that 130 or more fail is only 1.3×10^{-3}.

[5] P_{indep} is the actual probability of failure; $P_{indep\ max}$ is the maximum acceptable probability of failure. That is, we require $P_{indep} \leq P_{indep\ max}$.

[6] For clarity of illustration, the ordinate in the graph of $P_{j,m}$ uses a log scale and is truncated.

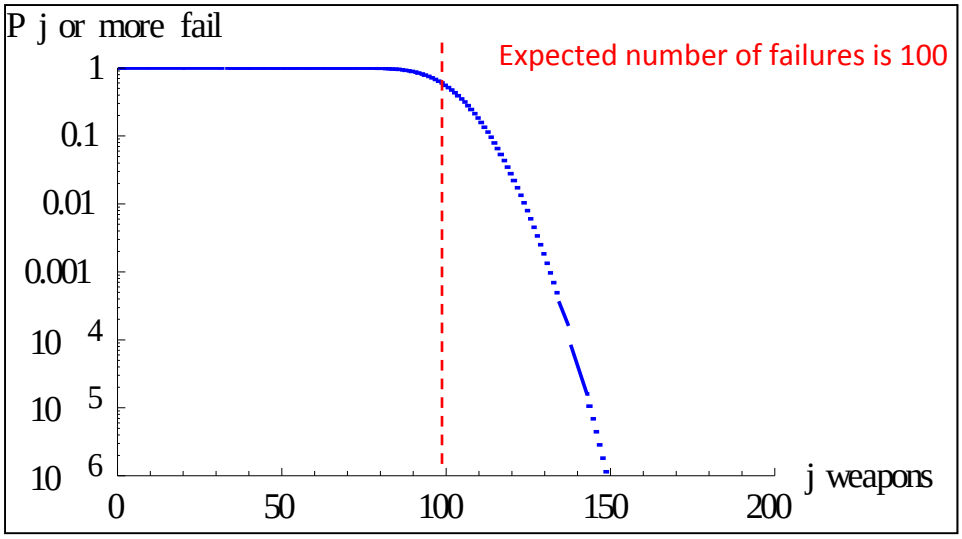

Figure 2-1 Probability j or More of 1000 Weapons Fail, P_{indep} of 0.1

If the 0.1 probability of failure is common to all weapons, then the probability that j or more weapons fail is 0.1 for any j greater than zero as indicated in Figure 2-2.[7]

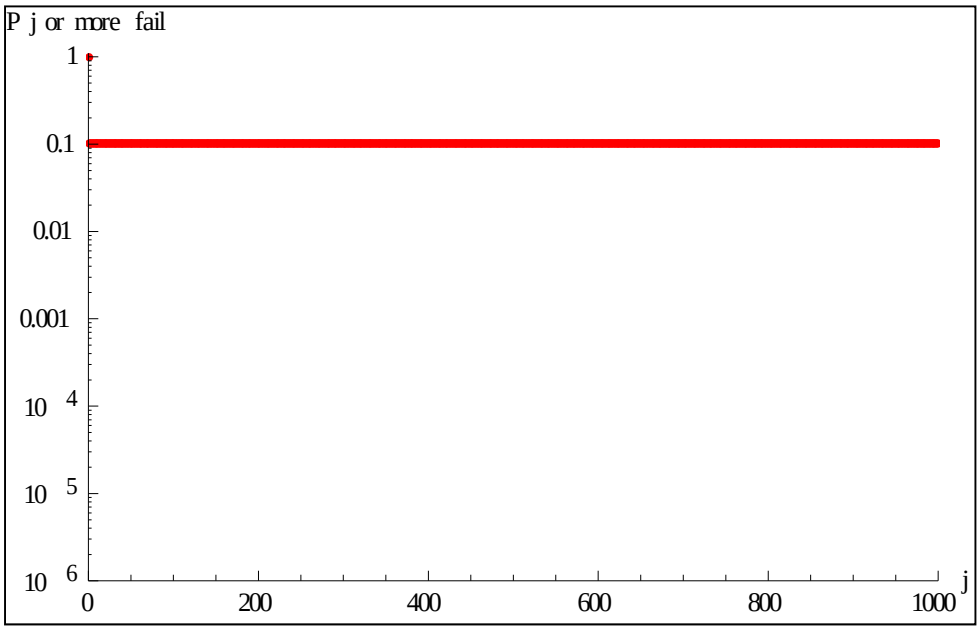

Figure 2-2 Probability j or More of 1000 Weapons Fail
with 0.1 Probability Common Cause Failure for All Weapons

With common cause failure- in contrast to the situation with only independent failure- the probability that substantially more than the number of weapons expected to fail (the mean,

[7] As previously discussed, $P_{j,m}$ is discrete. Note that at j of 0, $P_{j,m}$ is one, and that for any $j > 0$, $P_{j,m}$ is 0.1.

100) can be significant. For example, the probability that 130 or more weapons fail is 0.1, and even worse the probability that all 1000 weapons fails is also 0.1.

Therefore, we should expand our criteria for the acceptable probability of failure to consider common cause. **Instead of basing acceptance on the probability of failure of *an* item, the criteria should address the *total number* of items that can fail.**

Let "k" denote a specific "lot" of k items within the population of size m, all subject to common cause failure. This could be a sub-population of weapons for a specific weapon system, a sub-population of weapon subsystems -e.g., trajectory- for a specific weapon system, or a sub-population of components- e.g., a Lightning Arrestor Connector (LAC)- of a weapon subsystem. For example, we may be concerned with the sub-population for a particular warhead that contains a specific LAC; only some of the warheads contain this LAC, others contain a LAC of a different type and design. Note that we do not require all items in the population be subject to common cause failure, only a certain specific subset or lot.[8]

For the expanded acceptance criteria for screening, we require k to be sufficiently small, such that even if all k items fail by common cause with certainty, there is zero probability that more than μ_{max} items fail by common cause, where μ_{max} is the expected (mean) number of failures given the maximum acceptable independent probability of failure.[9] Since $\mu_{max} = P_{indep\ max} \times m$, we require that k/m not exceed $P_{indep\ max}$, where $P_{indep\ max}$ is the maximum acceptable independent failure probability for the case of interest as given in Table 2-1.

Therefore, we have the following simple expanded acceptance criteria for screening:

The fraction of items (k) within a population (m) subject to common cause degradation of concern, shall not exceed the maximum allowed expected number of failures (μ_{max}) assuming only independent failure. Therefore k shall not exceed μ_{max}, or equivalently, k/m shall not exceed $P_{indep\ max}$.

Two examples follow to show how the criteria can be used in the screening process.

As previously discussed for the reliability of 1000 items (i.e., weapons) with a maximum independent failure probability of failure of 0.1, the expected number of failures is 100. For common cause degradation- assumed to be common cause failure for screening as previously discussed- we require that k not exceed 100, or that k/m not exceed 0.1. Figure 2-3 shows $P_{j.m}$ using this requirement.

[8] For k of zero there is no common cause failure. For k of one, there is not really a common cause failure as the probability of failure of only one item is increased. k of two or greater represents a true common cause failure.

[9] μ_{max} is μ for Equation 1 with P_{indep} equal to $P_{indep\ max}$.

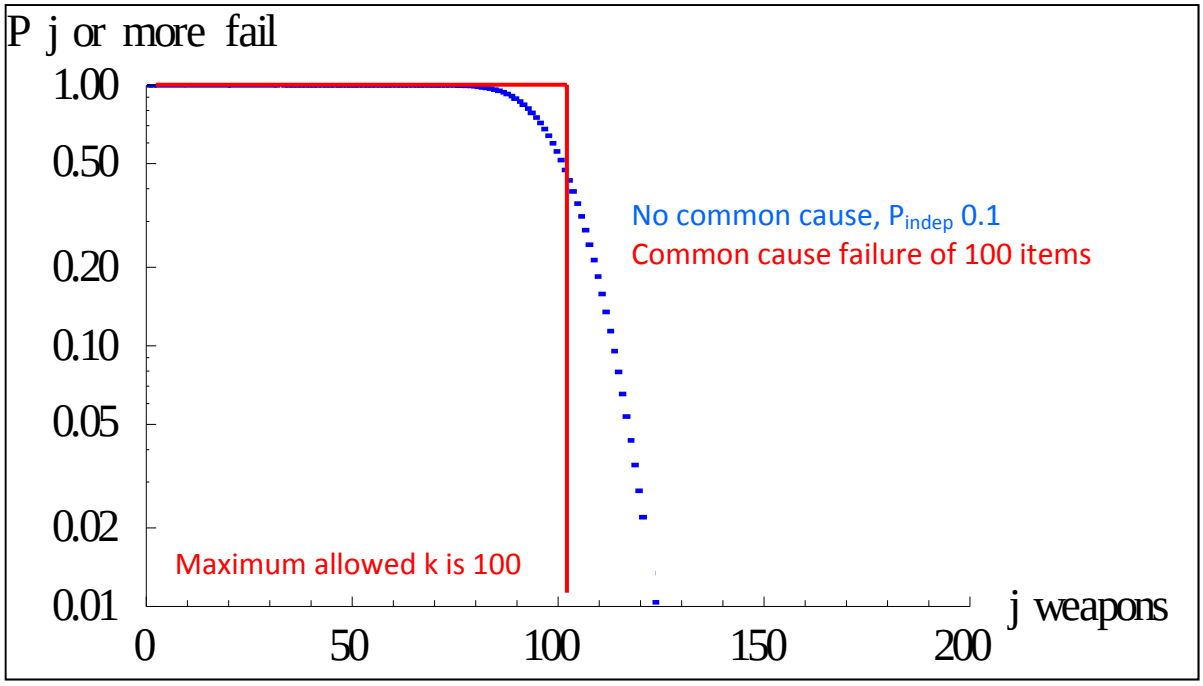

Figure 2-3 Example of Expanded Acceptance Criteria for Reliability of 1000 Weapons

As another example, consider the safety of 5000 items (e.g., subsystems) with a maximum acceptable independent failure probability of 10^{-3}. The expected number of failures is 5. For common cause degradation- assumed to be common cause failure for screening as previously discussed- we require that k not exceed 5, or that k/m not exceed 10^{-3}. Figure 2-4 illustrates this example.

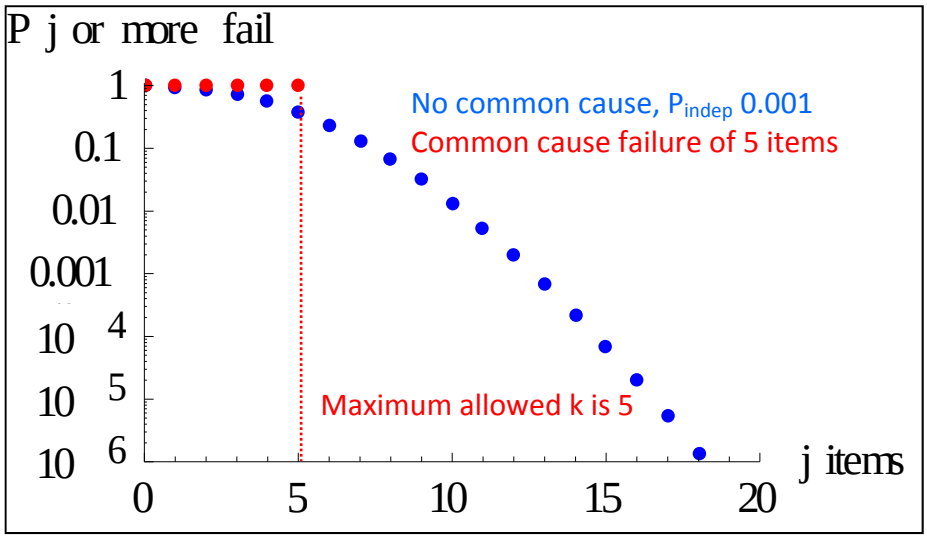

Figure 2-4 Example of Expanded Acceptance Criteria for Safety of 5000 Subsystems

In Table 2-2 we summarize the expanded acceptance criteria for the cases of interest from Table 2-1. The expanded acceptance criteria are very simple: k/m cannot exceed $P_{indep\ max}$.

Table 2-2 Screening Limits for Common Cause

Situation	Maximum Fraction of Population Allowed to Fail with Certainty by Common Cause (k/m)
Reliability of a weapon system taken as 0.9 [10]	0.1 [10]
Safety of a weapon system Normal environment Abnormal environment	 10^{-9} 10^{-6}
Safety of a weapon subsystem	10^{-3}
Safety of a weapon component	10^{-4}

If k/m is less than $P_{indep\ max}$ for the situation of concern, further immediate evaluation is not necessary. Otherwise, further detailed evaluation as discussed on Section 3 is warranted.

In general, for a reliability requirement specified in the Military Characteristics (MCs) for a specific weapon system, common degradation is of concern if more than 100(1 – x)% of the weapons are susceptible to common degradation, where x is the required reliability expressed as a fraction. For example, as indicated in Table 2-2 if the reliability requirement is 0.9, then common degradation is of concern for the reliability of a weapon system if 10% or more of the weapons are susceptible to common degradation.

For safety, the maximum fraction allowed to fail by common cause is 10^{-3} at the subsystem level: 0.1% of the population. For example, for a population of up to 2000 subsystems, failure of two or more by common cause is of concern, and for a population of 5000 items no more than 5 can fail by common cause.[11]

For safety at either the component or weapon system level, the maximum fraction of items allowed to fail by common cause is so small for the population sizes of interest that no more than two components or weapon systems are allowed to fail by common cause.[12]

3 Detailed Evaluation

The screening evaluation of Section 2 assumes that observed common degradation results in guaranteed common cause failure. Using this assumption, acceptable upper limits on the fraction of items that can fail by common cause were derived and summarized in Table 2-2.

[10] As previously discussed, in actual application the weapon system specific reliability required by the MCs should be used.

[11] For a population with 1000 subsystems, the maximum allowed k is 1. However, this is failure of only one item, which is technically not a common cause failure.

[12] For example, for 5000 items with P_{indep} of 10^{-4} for a component, k/m is 10^{-4} and k is 0.5.

If the fraction of items susceptible to common degradation exceeds the allowable limit, then a more detailed evaluation is warranted to assess the significance of the degradation.

The screening evaluation conservatively assumed that the probability of common cause failure is 1.0. For the detailed evaluation we must:

- Estimate the probability of common cause failure based on the level of common degradation that is observed, and
- Consider the fact that items can fail either independently or by common cause.

The probability that "j" (or more) of m items fail- independently or by common cause- is denoted as $P_{j,m}$. $P_{j,m}$, is: [13, 14]

$$P_{j,m} = P_{cc}(1 - CDF_{m-k,P_{indep}}(j-k-1)) + (1-P_{cc})(1 - CDF_{m,P_{indep}}(j-1))$$

(Eqn. 2)

The first term is the probability that k items all fail due to common cause and (j - k), or more, from the remaining (m – k) items fail independently. The second term is the probability that none of the k items fail by common cause, and j, or more, of m total items fail independently. Equation 2 is our analytic model and we implemented this model in Mathematica.[15] [Mathematica] Note that for the case of j ≤ k, the first term in Equation 2 reduces to P_{cc}, and for j of 0 the second term in Equation 2 reduces to $(1 – P_{cc})$.[16] For example, for j of zero $P_{j,m} = P_{cc} + (1 – P_{cc})$ which is one as expected, regardless of the values of k, P_{CC}, or P_{indep}.

In Section 3.1 we notionally consider two bounding cases to provide the framework for subsequently developing the acceptance criteria for the detailed evaluation. Specifically, we consider: (1) only independent failure and (2) only common cause failure. Then, in Section 3.2 we provide the acceptance criteria for the detailed evaluation, and apply it to example

[13] For a discrete random variable X (here, the number of items failed), the Probability Density Function PDF(x) is the probability that X equals x. The Cumulative Distribution Function CDF(x) is the probability that X ≤ x. CCDF(x) = 1 – CDF(x) is the probability that X > x. For discrete X, the probability that X ≥ x (x or more fail) is 1 – CDF(x – 1). [Probability and Statistics] The binomial distribution has two parameters for the random variable X: the total number of items, and the probability that an item fails. In equation 2, 1 – CDF(j) is the probability that X is greater than j. We want the probability that X is *equal to or* greater than j, hence the (j-1) in equation 2.

[14] Common cause failure has been extensively evaluated in Probabilistic Risk Analysis (PRA) of commercial nuclear power plants. [Safety Goals] Our model benefited from this work. See Appendix C.

[15] We also developed a Monte Carlo sampling model in Java to evaluate $P_{j,m}$ as a check on the analytic model. [Sample with Common Cause] Results from the two models agree.

[16] That is, CDF(x) is zero for any x < 0, as verified with Mathematica.

situations where the earlier screening evaluation indicates that the follow-on detailed evaluation is warranted.

3.1 Bounding Cases

Consider two bounding cases defining the two extremes for this analysis.

1. With no common cause failure, Equation 2 simplifies to Equation 1 as given in Section 2.
2. With no independent failure, P_{indep} is zero, and Equation 2 becomes: [17]

$$P_{j,m\ no\ independent\ failure} = P_{cc}\ \ for\ 0 < j \le k$$
$$P_{j,m\ no\ independent\ failure} = 0\ \ for\ j > k$$

(Eqn. 3)

$P_{j,m\ no\ common\ cause}$ and $P_{j,m\ no\ independent\ failure}$ as functions of j are shown notionally in Figure 3-1.[18]

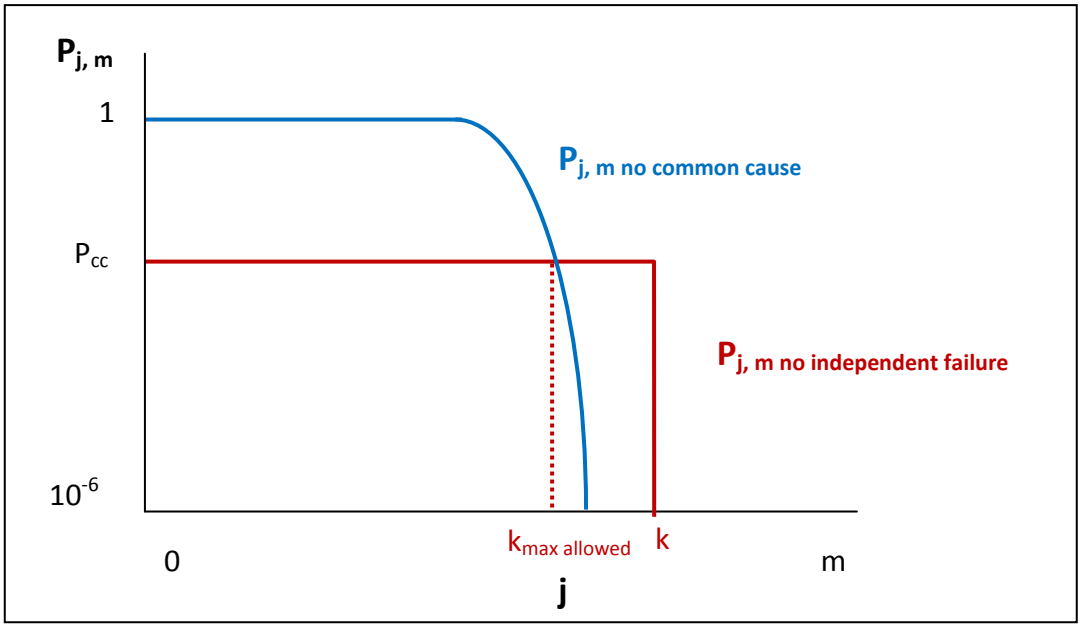

Figure 3-1 Bounding Cases

$P_{j,m}$ is a non-increasing function of j, the number of items failed. At j of zero $P_{j,m}$ is the probability that zero or more items fail which is always 1.0. For any j between 1 and m, $P_{j,m}$ depends on P_{indep}.

[17] At j of zero $P_{j,m}$ is always one.

[18] For simplicity of illustration, the notional graphs for $P_{j,m}$ do not consider that the function is discrete, and- for cases with only common cause failure- do not explicitly show that $P_{j,m}$ is always one at j of zero. Accurate graphs of $P_{j,m}$ for example situations are provided later.

Note the significant difference between the two situations. With only independent failure, $P_{j,m}$ decreases with increasing j for sufficiently large j. With only common cause failure $P_{j,m}$ is a constant for all k items subject to common cause failure, and $P_{j,m}$ is zero for j greater than k. For the latter situation the probability that all k items fail is the same as the probability that one item fails. This is a mathematical depiction of the behavior previously discussed: common cause failure can substantially increase the probability that multiple items fail, whereas with only independent failure the probability that j or more items fail is small if j exceeds the expected number of failures.

For a specific value of P_{cc}, there is a maximum k allowed- denoted as $k_{max\ allowed}$- such that $P_{j,m\ no\ independent\ failure}$ is less than $P_{j,m\ no\ common\ cause}$ for all j in [0, m]. Figure 3-1 shows a situation with k sufficiently large such that that $P_{j,m\ no\ independent\ failure}$ for some j in [0,m] exceeds $P_{j,m\ no\ common\ cause}$. As indicated in the figure, for $P_{j,m\ no\ independent\ failure}$ for any j in [0, m] to not exceed $P_{j,m\ no\ common\ cause}$, k cannot exceed some maximum $k_{max\ allowed}$. That is, for common cause to not be of concern, the number of items subject to common cause failure, k, cannot exceed a specific value $k_{max\ allowed}$ as indicated in Figure 3-1.

Figure 3-2 notionally indicates how $k_{max\ allowed}$ increases with decreasing P_{cc}.

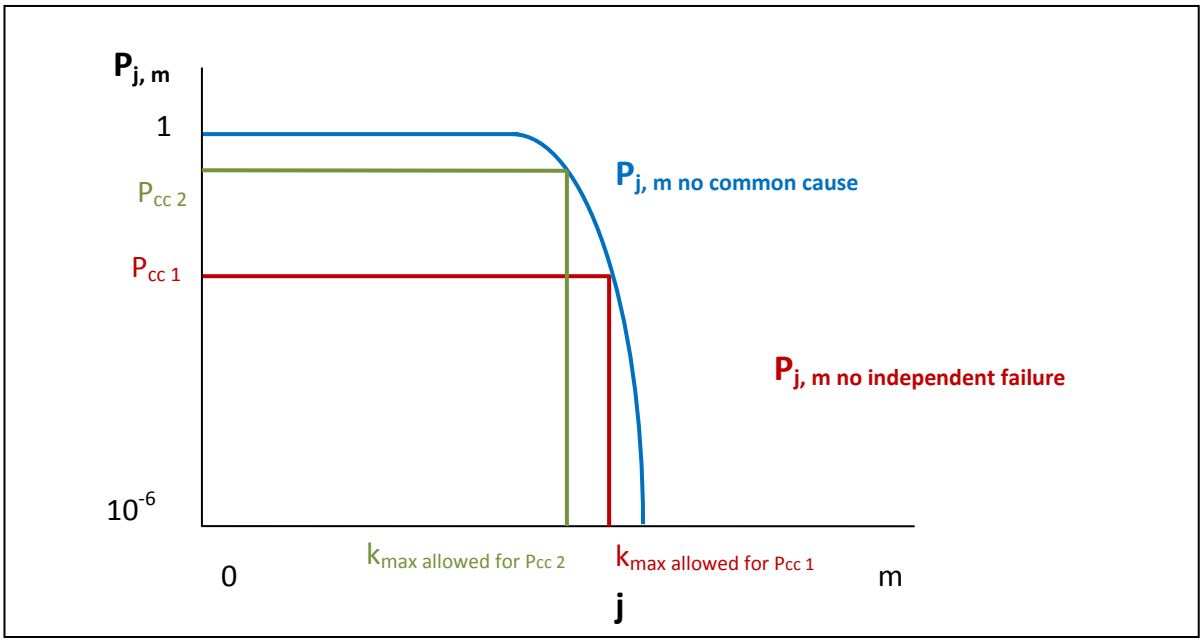

Figure 3-2 Notional Example for $k_{max\ allowed}$ as function of P_{cc}

Note that a lower value of P_{cc} results in a higher number of items allowed to have common cause failure, $k_{max\ allowed}$.

So far we considered the bounding cases to illustrate that for a sufficiently small value of P_{cc}, the probability that j or more items fail due to common cause can be less than the probability that j or more items fail independently. We now apply this insight to develop the detailed acceptance criteria.

3.2 Acceptance Criteria for Detailed Evaluation

The screening process previously discussed in Section 2 assumes that common cause degradation always results in a common cause failure; that is, it assumes P_{cc} of one.

The prior discussion in Section 3.1 notionally shows that for sufficiently small P_{cc} common cause failure is not of concern relative to independent failure.

For the detailed evaluation we estimate the actual $P_{j,m}$ using Equation 2, which requires an estimate of the actual P_{cc} and the actual P_{indep}, and compare the result to the maximum allowed $P_{j,m\ no\ common\ cause}$ calculated using Equation 1 using the maximum acceptable independent failure probability $P_{indep\ max}$.

For the detailed evaluation, using the best estimates of both P_{cc} and P_{indep}, we require that k be sufficiently small such that the best estimate curve for $P_{j,m}$ calculated using Equation 2 not exceed $P_{j,m\ no\ common\ cause\ max}$ for all j from 0 to m. $P_{j,m\ no\ common\ cause\ max}$ is $P_{j,m\ no\ common\ cause}$ calculated using Equation 1 using the maximum allowed value $P_{indep\ max}$ for P_{indep}.

Stated simply, we require that for all j, our best estimate of $P_{j,m}$ not exceed the situation where only independent failures occur with the maximum acceptable probability for independent failure. That is, the maximum acceptable case for only independent failure always bounds our best estimate considering the actual independent and common cause failure probabilities.

Note that the detailed evaluation requires knowledge of P_{cc} whereas the screening approach assumed P_{cc} of 1.0.

For a real life situation, the actual value P_{indep} is not zero. We estimate P_{indep} as well as P_{cc} and generate our best estimate for $P_{j,m}$ using Equation 2. We compare this best estimate $P_{j,m,}$ to $P_{j,\ m\ no\ common\ cause\ max}$. The following examples clarify the process.

Assume testing indicates that 20% of a population of 1000 weapons has a degradation that affects reliability. Also assume that the required reliability is 0.9. First, we apply the screening criteria to determine if this degradation warrants detailed evaluation. As previously discussed, no detailed knowledge of the actual probabilities of failure are used in the screening process; we simply compare the number of items susceptible to common cause degradation, to the expected number of failures assuming only independent failure with the maximum acceptable probability of failure. Only if the screening criteria are not met do we need to spend the effort to estimate the actual failure probabilities P_{cc} and P_{indep}.

Applying the screening criteria developed in Section 2, the number of items with common cause is large enough to require further detailed evaluation because more than 10% of the population is affected; specifically, 200 weapons are subject to degradation (k) but the

expected number of failures (μ_{max}) considering only independent failure, with the maximum acceptable probability, is 100 . Since k > μ_{max}, a follow on detailed evaluation is warranted.

For the detailed evaluation, we must estimate the actual values for P_{CC} and P_{indep}. Significant effort may be required to produce these estimates. For this example, assume that the observed degradation is best considered as a common cause failure with P_{cc} of 0.1, and that P_{indep} is 0.05. Using equation 2, $P_{j,m}$ as a function of j is shown in Figure 3-3. For j less than about 50, independent failure dominates (for 1000 items each failing independently with probability 0.05, the probability that 40 or more fail is 0.92.) For j greater than about 70 up to 200, common cause dominates (the probability that j or more items fail by common cause is 0.1 for any j up to 200).

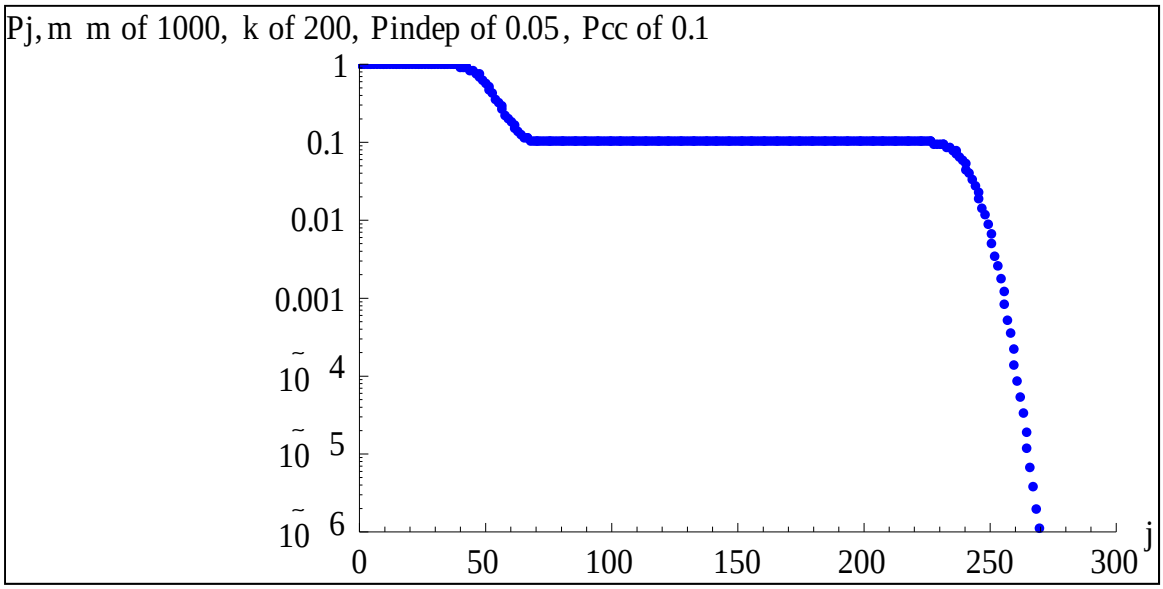

Figure 3-3 $P_{j,m}$ for m of 1000, k of 200, P_{indep} of 0.05, P_{cc} of 0.1

To apply the detailed screening criteria, we compare the results of Figure 3-3 to the case of $P_{j,m\ \text{no common cause max}}$ where $P_{indep\ max}$ is 0.1. Figure 3-4 provides this comparison. The shaded area in the figure indicates the region where the actual $P_{j,m}$ is not bounded by the acceptance curve.

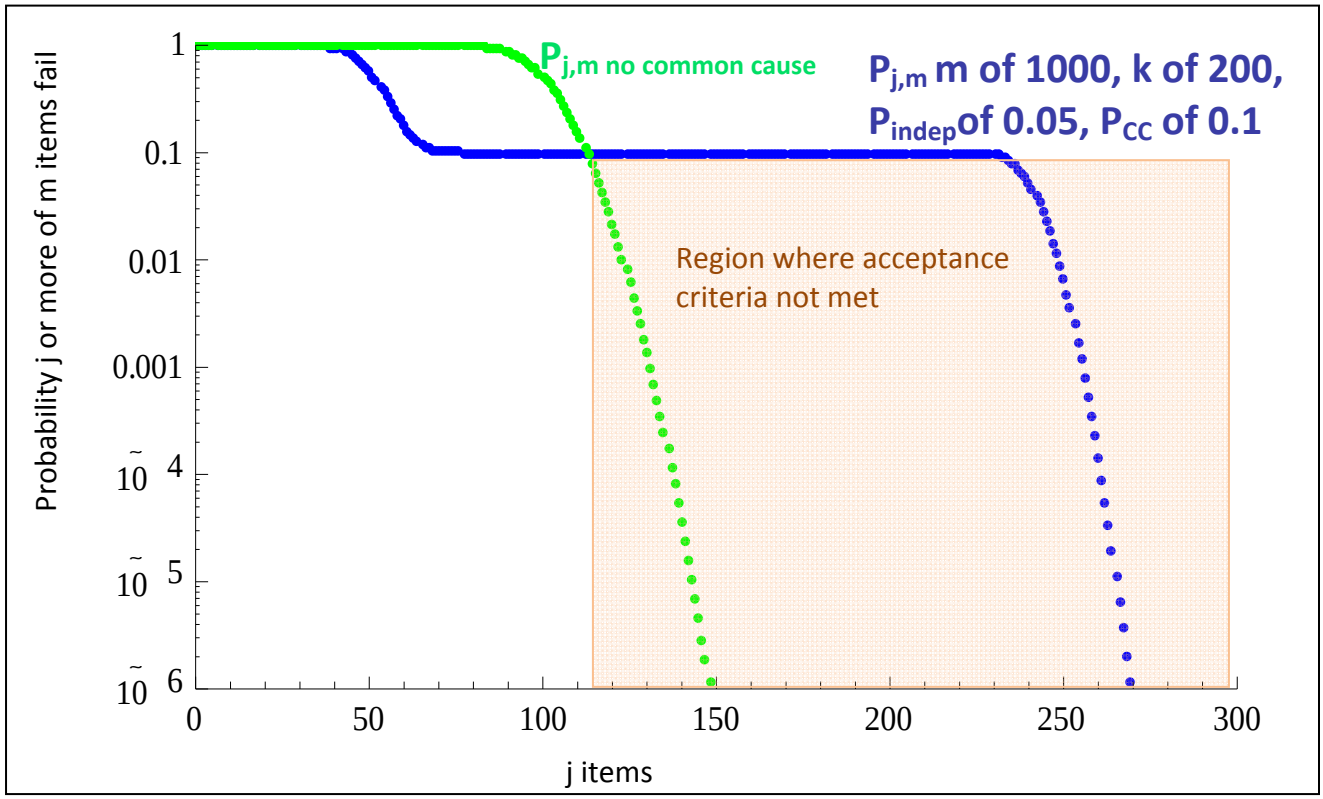

Figure 3-4 Example 1: Comparison of Actual $P_{j,m}$ to $P_{j,m\ no\ common\ cause\ max}$

Using the acceptance criteria for the detailed evaluation, based on Figure 3-4 we conclude that the common degradation is of concern, since for j greater than about 113, our estimate of the actual $P_{j,m}$ is greater than $P_{j,m\ no\ common\ cause\ max}$. That is, using data from the detailed evaluation, the actual $P_{j,m}$ is not less than $P_{j,m\ no\ common\ cause\ max}$ for all j in [0, m]. This indicates that efforts should be undertaken to reduce the risk due to common cause failure.

As another example, assume testing indicates that 15 weapons in a population of 100 have a degradation that affects reliability. Also assume that the required reliability is 0.9. Since k of 15 exceeds μ_{max} of 10, detailed evaluation is warranted. Assume the observed degradation is best considered as a common cause failure with P_{cc} of 0.01, and that P_{indep} is 0.03. Figure 3-5 compares the actual $P_{j,m}$ to the acceptable bounding curve.

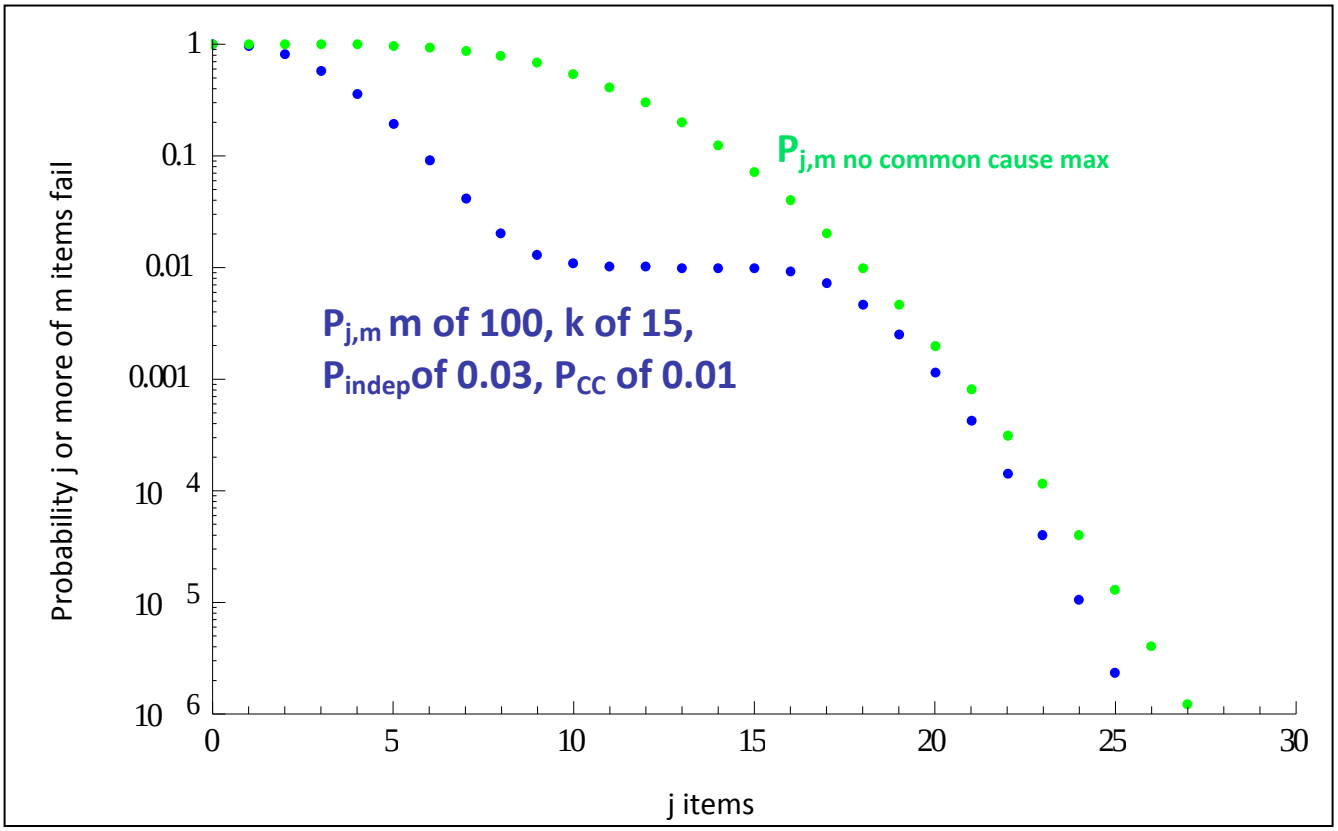

Figure 3-5 Example 2: Comparison of Actual $P_{j,m}$ to $P_{j,m \text{ no common cause max}}$

Based on Figure 3-5, we conclude that the common degradation is not of significant concern for reliability, since for all j in [0, m] the best estimate for $P_{j,m}$ is below the acceptable bounding curve.

4 Conclusions

We expanded the current acceptable limits for failure for reliability and safety to apply to situations with common cause failure.

We developed a screening process for evaluating the conditions under which common degradation may be of immediate concern for the reliability or safety of a nuclear weapon system, subsystem, or component.

For a population in the range [100, 5000] we evaluated the screening process and conclude the following.

Assuming a reliability requirement of 0.9, common degradation is of potential concern for the reliability of a weapon system if 10% or more of the weapons are susceptible to common degradation. In general, for a specific reliability requirement specified in the MCs, call it x

where x is in [0, 1], common degradation is of potential concern if more than 100(1 – x)% of the weapons are susceptible to common degradation.

Common degradation is of potential concern for the safety of a weapon component or overall weapon system if two or more components/weapons are susceptible to degradation.

Common degradation is of potential concern for the safety of a weapon subsystem if more than 0.1% of the population is susceptible to common degradation. The acceptable number of subsystems that can be degraded ranges from no more than two (for a population of up to about 2000), up to five (for a population of 5000 items).

In contrast to the case for reliability where 10% of the weapons can fail by common cause without cause for major concern, for safety common degradation requires detailed evaluation if a small number (two to five) weapon subsystems, components, or overall weapons are affected. This is due to the higher independent failure probability limit of 0.1 for reliability as compared to the much lower failure limit for safety of 10^{-3} or less.

If a common degradation is of potential concern based on the screening process, immediate detailed evaluation of the effect of the common degradation is recommended. We provided a technique that can be used for the detailed evaluation.

These techniques are available for use by analysts at SNL to quickly evaluate the importance of common cause degradations for both reliability and safety.

It is recommended that these techniques be applied at SNL to a test case to prove their usefulness. Specifically, the data should be interrogated to select common cause degradation of concern for each weapon system, and the techniques should be applied to these cases of concern.

References

1. [Mathematica] Mathematica software version 7.0.1, Wolfram Research.
2. [Probability and Statistics] E.R. Dougherty, Probability and Statistics for the Engineering, Computing, and Physical Sciences, Prentice Hall, 1990.
3. [Safety Goals] Kumamoto, Hiromitsu, Satisfying Safety Goals by Probabilistic Risk Assessment, Springer, 2007, Chapter 8 "Common Cause Failure".
4. [Sample with Common Cause] Darby, J., and Drewien, C. "Evaluation of the Effect of Common Cause Degradation on Sample Size for System-Level Surveillance Testing of Nuclear Weapons ", (OUO) SAND2010-7672, November, 2010.
5. [Uncertainty Approaches] Helton, J.C., Johnson, J.D., and Oberkampf, W. L., "An Exploration of alternative approaches to the representation of uncertainty in model predictions", Reliability Engineering and System Safety 85 (2004) 39-71.
6. [Weapon Reliability Guide] "Nuclear Weapon Reliability Evaluation Guide", First Edition, SAND2002-8133, April, 2002.

Appendix A. Average Failure Model

This appendix demonstrates that a simple model that treats common cause as increasing the independent failure probability of an item is not a good model.

The average probability of failure of an item considering common cause is:

$$P_{avg} = \frac{k}{m}\left(P_{indep} + P_{cc}\right) + \frac{m-k}{m} P_{indep} \qquad \text{(Eqn. A-1)}$$

If we assume that every item fails independently with probability P_{avg} this is a poor approach; although it considers common cause in the failure probability P_{avg} for each item, it treats each item as failing independently with probability P_{avg}.

In reality common cause failure results in simultaneous failure of more than one item: k items can all fail due to common cause as well as fail independently, and (m – k) items can only fail independently.

Here we compare results using the simple P_{avg} model to the $P_{j,m}$ model of Section 3 and show that the average model can be highly inaccurate.

Consider an evaluation of the safety of a weapon component. The population is 500 components 80 of which are subject to common cause failure. P_{indep} is 8×10^{-5} and P_{cc} is 3×10^{-5}. Using equation 2, P_{avg} is 8.5×10^{-5}, below the acceptable limit of 10^{-4}, and using P_{avg} we conclude that the component meets its safety requirement.

However, to accurately consider the effect of common cause failure, we evaluate the probability that j or more items fail.

The probability that j or more items fail using the P_{avg} model can be calculated with equation 1 using P_{avg} of equation A-1 for P_{indep} in equation 1; that is, we increase the independent probability of failure for each item.

The probability that j or more items fail is more accurately evaluated with $P_{j,m}$ as given in equation 2.

Figure A-1 compares the results of the two models. For clarity the discrete points in the figure have been joined with a line.

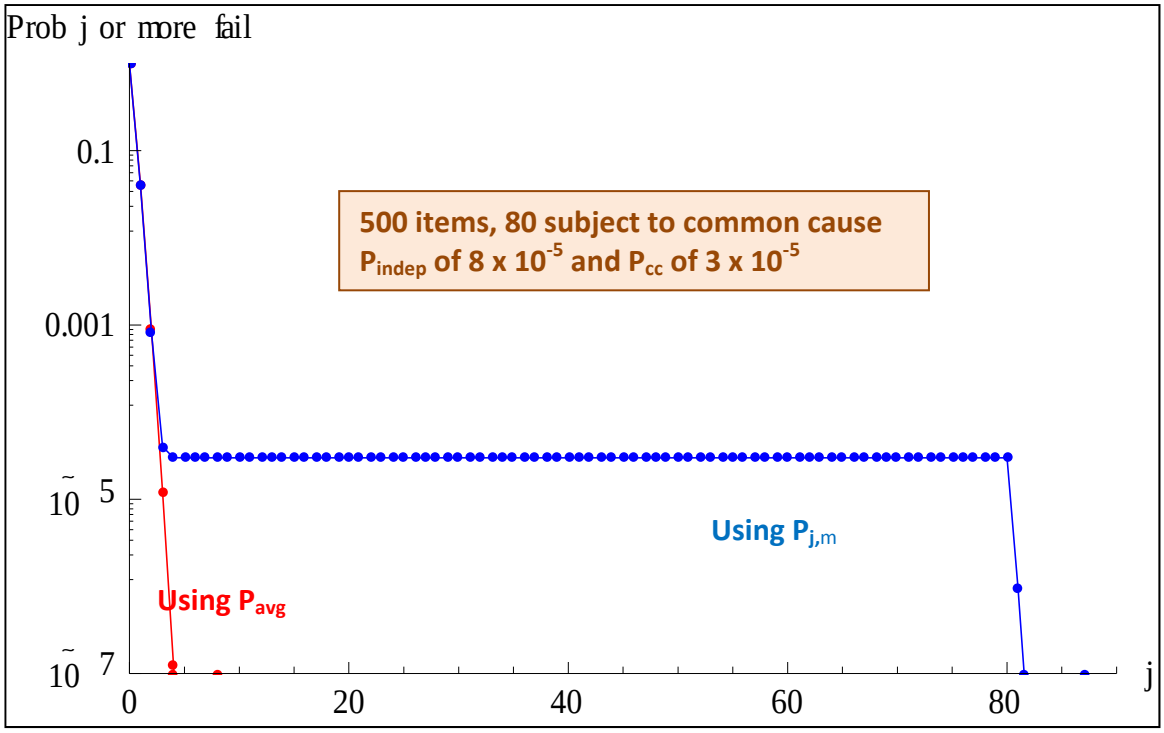

Figure A-1 Comparison of P_{avg} and $P_{j,m}$ Models

As indicated in Figure A-1, the P_{avg} model severely under-predicts the probability that 3 or more items fail. The $P_{j,m}$ model shows that there is a probability of 3×10^{-5} that 80 or more of the 500 items fail.

Appendix B. Model for Subpopulation Having Increased Independent Failure Probability

Although this work focused on common cause failure, during the effort we developed a model to evaluate the case where part of the population has a defect that increases the probability of independent failure. That model is summarized here.

k of the m items each fail independently with probability $P_{indep}|degradation$, and the remaining (m –k) items fail independently with probability P_{indep}.

In Mathematica form, the probability that j or more of the m items fail is:[19]

$$P_{j,m\ Degraded} = Sum[PDF_{k,P_{indep}|\deg radation}(j_1) * PDF_{m-k,P_{indep}}(j_2), \{j_1, 0, k\}, \{j_2, j - j_1, m - k\}] \quad \text{(Eqn. B-1)}$$

The total number of items failed is j; j_1 is the number of items that are degraded that fail and (j - j_1) is the number of items that are not degraded that fail. $PDF_{k,Pindep|degradation}(j_1)$ is the probability that (exactly) j_1 items fail; $PDF_{m\text{-}k,Pindep}(j_2)$ is the probability that (exactly) j_2 items fail. The inner sum is over all j_2 from (j – j_1) to (m-k) for a fixed j_1; the outer sum is over all j_1 from zero to k.

Assume that 10% of a population of 100 weapon systems has a safety problem with a subsystem, and that detailed evaluation concludes that the degradation increases P_{indep}. For example, for a certain lot a component has a design flaw that results in an increase in the probability of failure of each subsystem in the lot.

Detailed evaluation supports a P_{indep} of 5×10^{-4} for the subsystem in the items without the degradation, and $P_{indep}|degradation$ of 4×10^{-3} for the subsystem in the items with the degradation. Using equation B-1, $P_{j,m\ Degraded}$ as a function of j is shown in Figure B-1. We truncate the results for $P_{j,m\ Degraded}$ in Figure B-1 at j of 7 since for higher j, $P_{j,m\ Degraded}$ is insignificantly small (less than 10^{-12}).

[19] $PDF_{n,p}$ denotes the probability density function for the binomial distribution with parameters n (trials) and p (probability of failure).

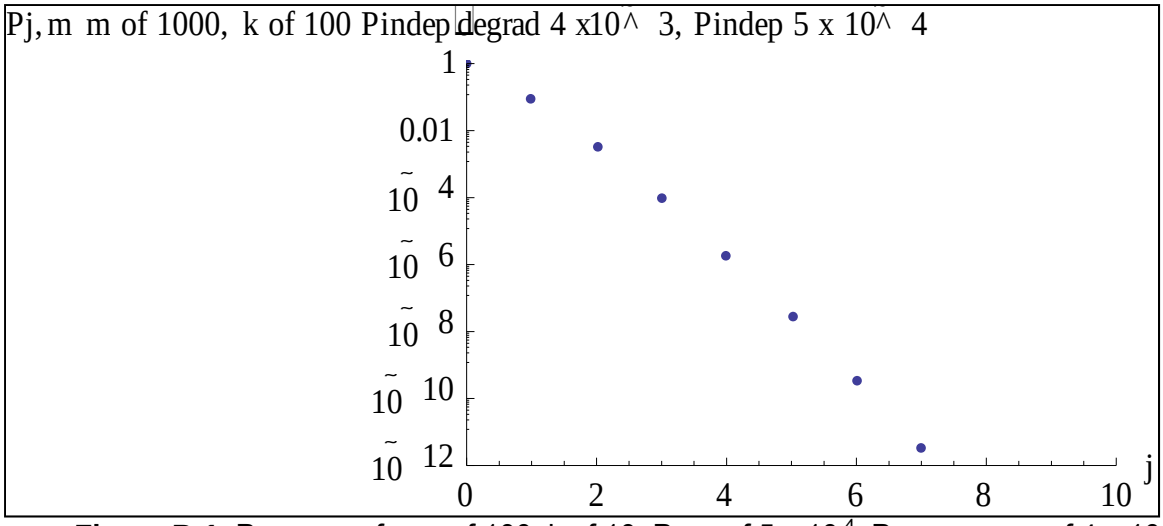

Figure B-1 $P_{j,m\ Degraded}$ for m of 100, k of 10, P_{indep} of 5 x 10^{-4}, $P_{indep|degradation}$ of 4 x 10^{-3}

Figure B-2 is the case of $P_{j,m\ no\ common\ cause\ max}$ (using the maximum allowed $P_{indep\ max}$ of 0.001 for a subsystem). Figure B-3 compares the results of Figures B-1 and B-2.

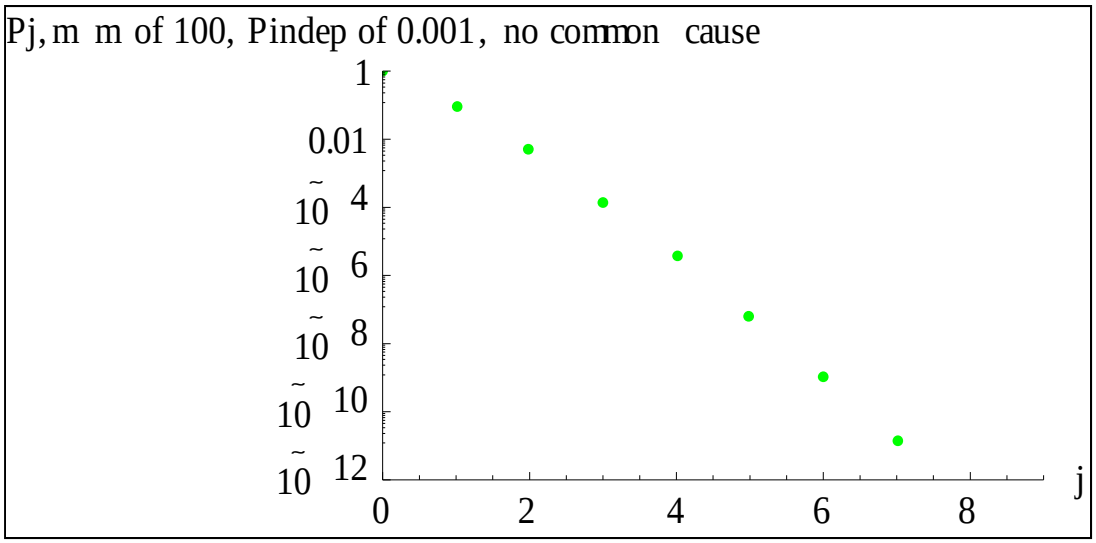

Figure B-2 $P_{j,m\ no\ common\ cause\ max}$ for m of 100, $P_{indep\ max}$ of 0.001

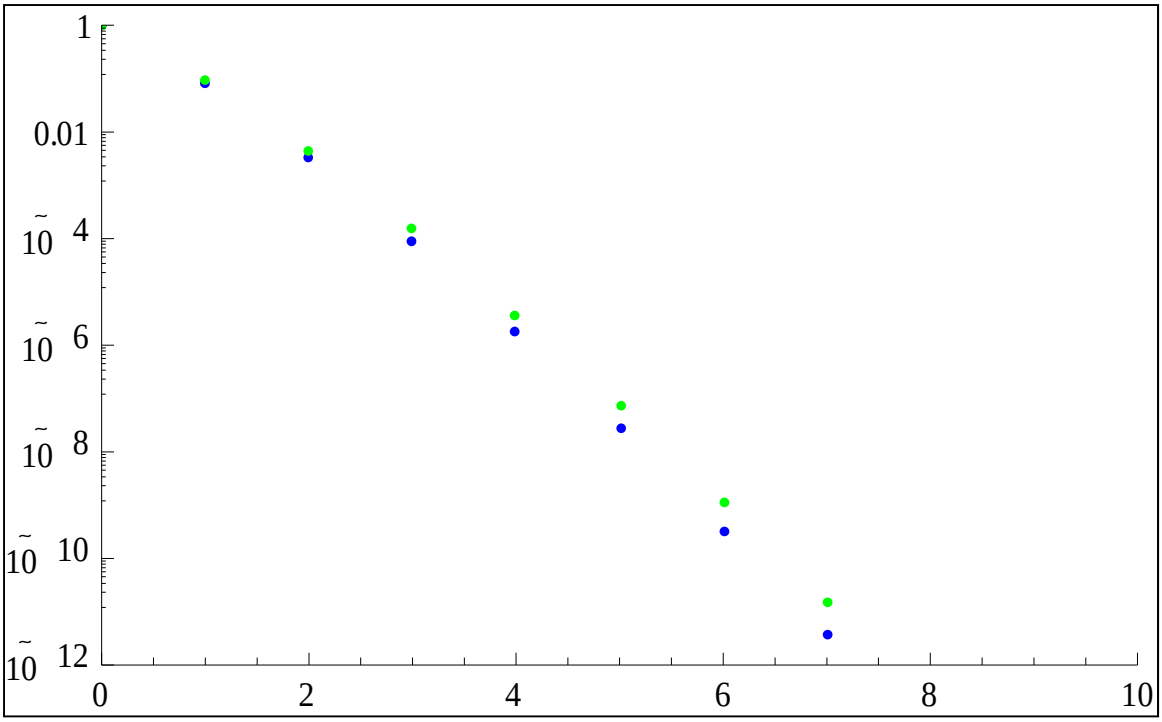

Figure B-3 Comparison of Figures B-1 and B-2 Results

Comparing the results of Figures B-1 and B-2, we conclude that the common degradation is not of concern, since using results from the detailed evaluation
$P_{j,m\ Degraded}$ is essentially the same as $P_{j,m\ no\ common\ cause\ max}$ for all j where $P_{j,m}$ is not insignificantly small.

Appendix C. Simple Example of Common Cause Failure

Insight as to how common cause failure can increase the failure probability can be gained from considering a simple two-component system. The reference provides more details. [Safety Goals]

The following simple example indicates how common cause failure can greatly increase the likelihood of failure of two items. This could represent failure of a two-train safety system in a nuclear power plant where success requires that one of two pumps (items) operate. Let C denote the common cause failure for the two items; let A denote the independent failure of the first item and B the independent failure of the second item. Failure of both items is: (C U A) ∩ (C U B) = C U (A ∩ B).[20] The probability for failure of both items is: P(C) + P(A) P(B) – P(C) P(A) P(B).[21]

For P(C) of 0.02, and both P(A) and P(B) of 0.03, the probability that both items fail is 0.021; if each item failed only independently with probability 0.05 (sum of P_{cc} and P_{indep}), the probability that both fail would be significantly lower: 0.0025. This result can also be obtained using our model of equation 2.

This simple example illustrates the point that for systems where more than one item must fail for overall failure, if the probabilities of independent failure are small, then a small common cause failure probability can dominate the overall probability of system failure. Failure to consider common cause in such cases results in a significant under-estimate of the system failure probability.[22]

[20] U denotes logical OR and ∩ denotes logical AND.

[21] The rare event approximation ignores the third term: P(C) P(A) P(B). For two events R and S, P(R U S) = P(R) + P(S) – P(R ∩ S) where ∩ denotes the logical AND operation. P(R ∩ S) = P(R) * P(S) only if R and S are independent. If R and S are mutually exclusive P(R ∩ S) = 0. The rare event approximation neglects the "cross term" and approximates P(R U S) as P(R) + P(S). The rare event approximation gives an upper bound on P(R U S), and is always conservative if R and S are failure events, but it is a poor estimate if P(R) and P(S) are not small.

[22] To reduce common cause failure systems should be diverse instead of redundant. For example, for the two-pump example if the two pumps are of different types- one motor driven and the other steam driven- the potential for common cause failure may possibly be reduced. True diversity is difficult to achieve; even with two different pumps common failures due to maintenance or common operating environments may exist between the pumps.

Distribution

1	MS0405	Kevin Maloney	0416 (electronic copy)
1	MS0405	Lawrence Sanchez	0416 (electronic copy)
1	MS0405	Robert Waters	0416 (electronic copy)
1	MS0415	Keith Almquist	0541 (electronic copy)
1	MS0415	John Darby	0541 (electronic copy)
1	MS0415	Celeste Drewien	0541 (electronic copy)
1	MS0415	Steven Hatch	0541 (electronic copy)
1	MS0415	Ronald Pedersen	0541 (electronic copy)
1	MS0417	David Fordham	0543 (electronic copy)
1	MS0421	Michael Sjulin	0540 (electronic copy)
1	MS0424	Donald Waye	0547 (electronic copy)
1	MS0492	Jeffrey D. Brewer	0411 (electronic copy)
1	MS0492	Thomas D. Brown	0411 (electronic copy)
1	MS0639	Corey A. Cruz	2950 (electronic copy)
1	MS0639	Kathleen Diegert	2950 (electronic copy)
1	MS0748	Jon Helton	1545 (electronic copy)
1	MS0829	Janet Sjulin	0413 (electronic copy)
1	MS0830	Thomas Kerschen	0413 (electronic copy)
1	MS0830	Douglas Loescher	0413 (electronic copy)
1	MS9007	Rene Bierbaum	8245 (electronic copy)
1	MS9007	James Ringland	8245 (electronic copy)
1	MS0899	Technical Library	9536 (electronic copy)


Sandia National Laboratories