Common Cause Failure Modeling in Space Launch Vehicles

Frank Hark (1), Rob Ring (1), Steven D. Novack (1), Paul Britton (2),

(1) Bastion Technologies Incorporated, 17625 El Camino Real #330, TX 77058, USA, Emails: *frank.hark@nasa.gov, Robert.r.ring@nasa.gov, steven.d.novack@nasa.gov,*
(2) NASA Marshall Space Flight Center, Huntsville, AL 35812, USA ,Email: paul.t.britton@nasa.gov

ABSTRACT

Common Cause Failures (CCFs) are a known and documented phenomenon that defeats system redundancy. CCFs are a set of dependent type of failures that can be caused for example by system environments, manufacturing, transportation, storage, maintenance, and assembly. Since there are many factors that contribute to CCFs, they can be reduced, but are difficult to eliminate entirely. Furthermore, failure databases sometimes fail to differentiate between independent and dependent CCF. Because common cause failure data is limited in the aerospace industry, the Probabilistic Risk Assessment (PRA) Team at Bastion Technology Inc. is estimating CCF risk using generic data collected by the Nuclear Regulatory Commission (NRC). Consequently, common cause risk estimates based on this database, when applied to other industry applications, are highly uncertain. Therefore, it is important to account for a range of values for independent and CCF risk and to communicate the uncertainty to decision makers.

There is an existing methodology for reducing CCF risk during design, which includes a checklist of 40+ factors grouped into eight categories. Using this checklist, an approach to produce a beta factor estimate is being investigated that quantitatively relates these factors. In this example, the checklist will be tailored to space launch vehicles, a quantitative approach will be described, and an example of the method will be presented.

1. INTRODUCTION

CCF is a known and documented phenomenon that can occur due to coupling factors that result in multiple dependent failures of identical components in a redundant design configuration. Consequently, if not understood, identified, and mitigated these factors limit the benefit of system redundancy as a design approach to achieve high reliability. Because of their extremely high cost, low launch rate, and national reputation, the public expects and demands reliable launch vehicle operation and mission success. To achieve high reliability, design engineers employ functional redundancy in the design to achieve reliability goals. The success of this design approach requires steps be taken during system design and throughout the system lifecycle to limit and reduce CCF. An important step toward this end is to implement a deliberate and documented procedure throughout the design, development, and operational life of the system to understand and mitigate coupling factors that can result in CCFs. Failure to actively pursue these steps may result in highly redundant configurations with added cost, complexity, and weight that also fail to achieve their reliability goals. Furthermore, reliability prediction methodologies that do not address CCFs significantly misrepresent the true reliability of a system that relies on redundancy.

Another related issue that is a source of uncertainty in predicting design reliability of launch vehicles is sparse data. Also, problem reporting databases, when they are implemented and maintained, typically do not record operating time and other information that makes it difficult to accurately predict system reliability. Even less common are documented proximate and root cause analyses to identify whether coupling factors may have contributed to the failure or precursor to failure. Our experience in reviewing failures and anomalies suggests that CCFs have often not been identified as such.

A generic common cause failure database maintained by the Nuclear Regulatory Agency is being used by the Bastion Probabilistic Risk Assessment (PRA) team to estimate the risk of CCF for launch vehicles. Without investigating details of the specific system, these generic CCF factors may grossly under estimate the magnitude of the risk if these estimates are not adjusted to reflect significant differences in other industry applications [1]. An accepted methodology for reducing CCF is a CCF checklist to help PRA analysts identify common cause coupling factors and to use the insights gained to improve the quantitative CCF estimate [2]. The checklist is an aid to judging the overall susceptibility of the system to CCF of coupling mechanisms with specific qualities of the system. As technology advances and new system designs achieve higher levels of reliability, it is imperative that

procedures to reduce common cause are implemented early in the development cycle.

If steps are not taken to actively reduce CCFs through process, training, and design, the occurrence of CCFs may be significantly higher than the estimates documented in the NRC for the nuclear industry. According to a published paper [1], other industries have in fact experienced significantly higher occurrence of common cause failure.

There exists a need to link the magnitude of CCF risk to system qualities and to communicate the qualities that affect CCF. The systems analysis methodology detailed in this paper produces CCF estimates, based on an examination of the qualitative standards specific to the industry or system being analyzed as a first step to modeling CCF risk when no data on CCF exists. Before discussing the method, it is necessary to provide a review of the basic CCF calculation to show how this method may improve this CCF risk estimate compared to an unexamined application of generic data from the NRC.

2. BASIC COMMON CAUSE CALCULATION

As defined in the NASA PRA procedures guide [2] Section 7.3:

> *A common cause failure event is defined as the failure (or unavailable state_ of more than one component due to a shared cause during the system mission. Viewed in this fashion, CCFs are inseparable from the class of dependent failures and the distinction is mainly based on the level of treatment and choice of modeling approach in reliability analysis.*

There are a number of different methods for modeling CCFs and estimating the effect on system reliability such as the Multiple Greek Letter, the Alpha Model, and the Beta-Factor model. The beta-factor model is one of the simplest methods for modeling the impact of CCF and will be the focus of discussion in this paper.

To show how the beta factor estimates CCF risk, it is applied to a simple redundant system with two identical components in parallel in which at least one out of two is required to work. It is assumed that the total failure probability consists of independent and common cause failures. In this example, the total failure rate is equal to the sum of the independent failure rate and the common cause failure rate.

$$\lambda_T = \lambda_I + \lambda_{cc}$$

While assuming that $\lambda_{cc} << \lambda_I$.

A factor, β, is defined as the fraction of the total failure rate due to common cause. From this relationship, the independent failure rate (λ_I) can be calculated.

$$\beta = \frac{\lambda_{cc}}{\lambda_T}$$

$$\lambda_{cc} = \beta\lambda_T$$

$$\lambda_I = (1-\beta)\lambda_T$$

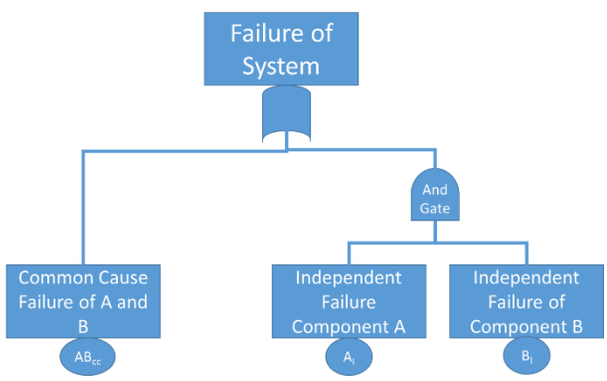

Figure 1: System Failure calculation including CCF

The total failure probability (or failure rate) can be taken from failure databases or testing. By assuming or estimating a β the failure probability of the parallel system is calculated as:

$$Failure\ of\ System = (\lambda_I t)^2 + (\lambda_c t) =$$

$$= [(1-\beta)\lambda_T t]^2 + \beta\lambda_T t$$

Assume λ_t = 1E-3 (failures/hr), t = 1 hour, β = 0.1

$$= [1E\text{-}03*(1E\text{-}03)*1]^2 + 0.1*1E\text{-}03*1$$

The first term is the independent failure contribution and second term is the CCF contribution, which is equal to:

$$=8.1E\text{-}03 + 1.0E\text{-}01.$$

Even when λ_{cc} is much less than λ_I (and β is less than 0.1) it shows that the CCF risk estimate dominates system risk. In addition, the β is the main driver of the overall system risk estimate.

Again, most databases only track total failures and make no distinction between independent and CCF. The NRC estimates for a range of generic component groups vary CCF β from 5-10% of total failures. From the same study cited earlier [1], failure data showed CCFs in some industries as high as 33% of total failures. This shows the importance of estimating a β that accounts for specific qualities of the system being modeled for CCF.

We have established the basics of estimating CCF risk and have shown how important the β is to the CCF estimate. We now will review factors that contribute to this phenomenon.

3. FACTORS THAT CONTRIBUTE TO COMMON CAUSE FAILURE

There are a set of primary factors that are significant contributors to CCFs and are described by eight areas that effect CCF coupling mechanisms:

1. Separation/segregation
2. Diversity/ redundancy
3. Complexity/maturity of design/experience
4. Use of assessments/ analysis and feedback data
5. Procedures/ human interface (e.g. maintenance/testing)
6. Competence/ training/ safety culture
7. Environmental control (e.g., temperature, humidity, personnel access)
8. Environmental testing

1. **Separation/segregation:**

This first group is the most often quoted factor associated with CCFs. Redundant subsystems in close proximity can be susceptible to the same faults. Keeping systems segregated helps limit these common cause coupling factors. A famous example is a fire or a leakage that causes corrosion. There is a famous example of an early flight of the DC-10 which failed to separate multiple redundant hydraulic controls is well documented in the literature. [Wetherholt paper]:

> *An actual example demonstrating single physical point failure is the case of United Airlines Flight 232 which was flying from Denver, Colorado to Chicago-O'Hare. On July 19, 1989 on the DC-10, the number 2 engine (on the tail of the plane) experienced a failure which threw shrapnel into the hydraulic lines passing through a 10 inch wide channel in the tail. All three redundant hydraulic systems lost fluid, leading to loss of flight control surface actuation.*

This should make it clear that the more separation/segregation of redundant components can be achieved the less this factor influences CCFs. However, there are limits to how much separation can be achieved — separated for systems that are tightly constrained by volume limitations, such as in aerospace applications.

2. Diversity/ Redundancy: the more diverse the better in regards to the design and maintenance of redundant subsystems. It is important to examine whether redundant systems were developed from separate requirements, by distinctly different design groups, with independent testing and design verification teams. Common cause coupling is decreased by adding more diversity.

3. Complexity/maturity/experience: A complex design with many components makes discovering coupling factors more difficult. The maturity of the design, along with testing off-nominal situations that stress the system, will bring coupling factors to light. The amount of experience designers/operators/maintainers have with a redundant system will also affect the common cause coupling factors and the overall susceptibility to CCF.

Analysis and feedback data: The more analysis methods, data tracking, and feedback to the program that is done the better the control/reduction of CCF will be for a given system. Some of the questions to be addressed in this category are: Has a detailed Failure Modes and Effects Analysis been completed? Is there an active problem reporting and analysis program for the system? Has a comprehensive reliability allocation and risk assessment been completed? Is root cause analysis performed after the occurrence of a system fault or failure? Are these analyses and data effectively communicated to the design engineers and management, and are these insights used to make the appropriate changes in the design, operational procedures, and training programs? Analysis and data feedback effectively used to improve the system can reduce common cause failure coupling factors.

4. Procedures/human interface: This aspect of CCF covers operation and maintenance as regarding human interfaces. Some of the questions to be addressed in this category are: Are there specific maintenance procedures for diverse/redundant systems/components

that suggest a staggered or non-staggered approach? Are maintenance actions and faults documented and investigated with respect to other redundant systems/components. Do maintenance manuals address possible common-cause coupling factors, for example assuring components are separated in case of a cable/connections re-routing. Is diverse equipment maintained by different shifts of staff? Are procedures updated after failure investigations? Is personnel training modified and updated following failure investigation findings?

5. **Competence/training/culture:** The safety culture plays a role in reducing CCFs. Some of the questions to be addressed in this category are: Have designers been trained to understand CCF? Do designers have a variety of technical background and experience? Does the industry put an emphasis on increasing reliability and safety? Have installers and maintenance personnel been trained to understand CCF? Have maintenance personnel been trained to understand CCF? Are maintenance personnel periodically retrained and updated on the results of failure assessments?

6. **Environmental control:** The environment itself can cause or initiate CCF mechanisms. Some of the questions to be addressed in this category are: Is the environment adequately controlled and regulated? Will the system encounter extreme environments? How will the system respond to localized, rare, extreme events? (E.g. earthquakes, flooding, loss of power from grid, etc.)

7. **Environmental testing:** Some of the questions to be addressed in this category are: Has the system been tested for the environmental conditions in which it operates (e.g. extended low or high temperatures, salt spray, vibration, etc.)? Has the system response been tested for electro-magnetic radiation?

Now that the eight areas that affect CCFs have been described, the next step is to present the methodology for developing a quantitative estimate of β.

4. BASIC METHODLOGY FOR ESTIMATING BETA FACTOR REALATED TO EIGHT COMMON CAUSE CATEGORIES

The first step in estimating the common cause beta factor is to assume a Maximum Common Cause Value (MCCV). One of three possible values must be selected (10%, 20%, or 30%). MCCV is based on judgment and experience and represents the maximum industry beta value based on a number of root cause considerations particular to the industry, such as its safety culture, management effectiveness, budget and schedule constraints, training effectiveness, maintenance program, and industry failure history. For example, in an industry that has a strong safety culture compared to other industries, one might select the lowest level of MCCV = 10%. Other industries that have a poor safety culture might have the highest MCCV = 30%.

The next step is assess each of the eight common cause susceptibility categories and for each, assign a Susceptibility Score of 1, 5, or 10 corresponding to the susceptibility category of Low, Medium, or High, respectively. The total Common Cause Score (CCS) is a sum of the products calculated by multiplying the number of categories (N_{low}, N_{medium}, N_{high}) assigned to each score by its Susceptibility Score.

$$CCS = 1 \cdot N_{low} + 5 \cdot N_{medium} + 10 \cdot N_{high}$$

The maximum possible CCS score with 8 high categories is T = 80. Then the CCF Beta is calculated as follows:

$$CCF\ Beta = \frac{CCS}{T} \times MCCV$$

For Table 1 given below with all low Susceptibility Scores, CCS=8, T=80, MCCV=30%

$$CCF\ Beta = \frac{8}{80} \times .30 = 3\%,$$

Table 1: basic evaluation for CCF with all low values

Area	Low	Medium	High
Separation/segregation	x		
Diversity/ Redundancy	x		
Complexity/maturity/experience	x		
Analysis and feedback data	x		
Procedures/human interface	x		
Competence/training/culture	x		
Environmental control	x		
Environmental testing	x		
sum of x's	8	0	0
Scoring	1	5	10
x * scoring	8	0	0
			CCS
	Total of x * scoring		8

This, incidentally would be the minimum CCF Beta this method allows using this assumed MCCV.

5. INDUSTRY EXAMPLE #1: STRONG SAFETY CULTURE

Now that the basis of the methodology has been described, we next apply it to an industry with a strong safety culture to illustrate how the result compares to the generic database values.

MCCV for this industry is assumed to be 20% since this industry makes an effort to reduce common cause failures.

Separation/segregation: This industry has successfully applied this design principle by physically separating redundant components; therefore. This is judged this factor to be low for common cause.

Diversity/ Redundancy: This example industry uses functional redundancy and diversity in the design, and also ensures diversity in maintenance procedures (for example, by having written maintenance procedures that require different maintenance operators checking out redundant subsystems, or by staggering the testing of redundant subsystems). In general, this industry is aware of CCFs. However, most designs in this example industry are 40 or more years old, and since not much was known about CCF during early design, this is judged to be medium.

Complexity/maturity/experience: By its nature Example #1 industry is complex. It is also decades old with many years of operating experience and is subject to strict government oversight and regulation. This is judged to be medium.

Analysis and feedback data: Example #1 industry also collects and maintains extensive data on CCF multiple plants and many years of operating experience as required by its government's regulatory agency. This is judged to be a low contributor to CCF.

Procedures/human interface: The regulatory agency overseeing this industry's design and maintenance procedures expend resources to minimize CCFs. The agency also oversees industry operators to ensure procedures meet exceedingly well defined standards. This is judged to be a low contributor.

Competence/training/culture: The oversight agency regulating this industry requires operators to have specific training. In addition, the agency monitors and strictly enforces standards.

Environmental control: The plant operating environment within this industry is well controlled. This would be assumed to be low factor for CCF. However, other environmental factors include extreme weather and natural disasters (such as Earth quakes and floods) that raises this to medium.

Environmental testing: This industry expends significant effort in testing for environmental conditions such as rare weather and disaster events (i.e. earthquakes) for the design basis risk. Procedures and failure studies are conducted and published industry wide to disseminate information. This is judged to be a low contributor to CCFs.

These results are summarized in Table 2 below

$$CCF\ Beta = \frac{CCS}{T} \times MCCV$$

So for the table given below, CCS=20, T=80, and MCCV=20%.

Table 2: CCF Example #1 Evaluation

Area	Low	Medium	High
Separation/segregation	x		
Diversity/ Redundancy		x	
Complexity/maturity/experience		x	
Analysis and feedback data	x		
Procedures/human interface	x		
Competence/training/culture	x		
Environmental control		x	
Environmental testing	x		
sum of x's	5	3	0
Scoring	1	5	10
sum of x * scoring	5	15	0
			CCS
	Total of x * scoring		20

$$CCF\ Beta = \frac{20}{80} \times .20 = 5\%,$$

This methods estimates the generic CCF beta for this example industry at 5%.

6. EXAMPLE #2 POOR SAFETY CULTURE

In this hypothetical example, the industry has a poor safety record, operations are very hazardous, the working environmental conditions are harsh, and government oversight is not as intense as in example #1. For this industry, MCCV is assumed to be 30% since it has not made a significant effort to reduce common cause failures.

Separation/segregation: The physical working environment is somewhat limited, but relatively large compared to other systems, such as spacecraft. With careful design consideration, redundant systems can be adequately separated/segregated. However, the industry lacks awareness of CCF and historically has valued cost savings more than safety. Therefore this is deemed, for current industry standards, as a high contributor to CCFs.

Diversity/ Redundancy: Where system redundancy is present the focus is on demanding production goals rather than safe operations. Without more specific information or design details, this is judged to be medium.

Complexity/maturity/experience: This industry has made significant advances in technology and performance in the last two decades without associated increases in safety measures. With a poor record of compliance with respect to government regulations and a limited number of on-site government inspectors compared, this category is a high contributor to CCFs.

Analysis and feedback data: While some effort is made, no specific government regulation or oversight is made for detailed analysis or use of feedback data. In addition, competition between companies means data is not shared among industry participants. Lastly, different companies have different levels of analysis. This is judged to be high contributor to CCFs.

Procedures/human interface: This industry requires extensive human interface and experience. Many processes should be well documented and require many work intensive steps. This makes this a high contributor to CCFs.

Competence/training/culture: The standards in this industry require a high level of competence. Training requirements vary among companies but still maintain a certain level. Culture varies among the different companies. This is judged to be a medium contributor to CCFs.

Environmental control: Depending upon the operating location, environmental conditions range from mild to extreme. Typically, the environment is harsh and working conditions are extremely difficult. This is assumed to be a medium contributor to CCFs.

Environmental testing: The harsh environments should require more testing for hardware and system processes. This one is estimated to be a medium contributor to CCFs.

These results are summarized in the Table 3 below

$$CCF\ Beta = \frac{CCS}{T} \times MCCV$$

So for the table given below, CCS=60, T=80, and MCCV=30%.

Table 3: Example #2 CCF Example Evaluation

Area	Low	Medium	High
Separation/segregation			x
Diversity/ Redundancy		x	
Complexity/maturity/experience			x
Analysis and feedback data			x
Procedures/human interface			x
Competence/training/culture		x	
Environmental control		x	
Environmental testing		x	
sum of x's	0	4	4
Scoring	1	5	10
x * scoring	0	20	40
			CCS
	Total of x * scoring		60

$$CCF\ Beta = \frac{60}{80} \times .30 = \ 23\%,$$

This methods estimates the generic CCF beta this example industry at 23%.

7. SUMMARY AND CONCLUSIONS

Systems require ever higher levels of reliability and in many cases this is achieved by increase redundancy. Without care, increasing redundancy may lead to increased CCFs coupling thereby reducing the benefit of increased system reliability. Until more data is collected and analyzed it will be difficult to judge just how high CCF risk is. However, using generic data, which are specifically designed to reduce common cause mechanisms, leads one to suspect that other industries may grossly underestimate CCF risk and also significantly overestimate system reliability.

We have reviewed the β factor CCF model and shown how it effects overall system reliability and how important that it in reliability predictions. We have provided a methodology that relates eight areas of susceptibility to common cause coupling factors to the β estimate. We then assessed the common cause β for two example industries: Example #1 Strong Safety Culture and Example #2 Poor Safety Culture and in both cases estimated reasonable β values based on data assumed to be known through an examination of eight factors that contribute to common cause failure.

Much work has been done to detail the factors that affect CCFs. By using this proposed method there is a better justification for generic CCF based on these factors that may lead to more realistic or credible CCF risk and overall system reliability when system specific data is not available. These results can then be used to highlight system design details that could investigated to reduce the system's susceptibility to CCF before data can be collected and investigate specifically to reduce CCF.

This method serves two purposes: 1) allows an analyst to better model CCF with factors specific to a system that doesn't have CCF data, and; 2) better communicate CCF coupling mechanisms to system designers, operators and maintainers. The more effort to educate industries about CCF coupling mechanisms, the more systems can be made that reduce CCF in the future.

7. REFERENCES

1. Hauge, S., Hoem A.S., Hokstad P., Habrekke, S, Lundteigen, M.A., *Common Cause Failures in Safety Instrumented Systems*, SINTEF Technology and Society, May 20, 2015.
2. Stamatelatos, M., *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners version 1.1*, Office Of Safety and Mission Assurance, NASA Headquarters, August, 2002.
3. *Procedures for Treating Common Cause Failures in Safety and Reliability Studies*, NUREG/ CR-4780
4. Wetherholt, J, Heimann, T.J. *Common Cause Failure Modes*, MSFC SMA, 2011