

Using Simulation to Characterize Common Cause

Dr. William M. Goble
www.exida.com
wgoble@exida.com

Introduction

Fault tolerant systems have been designed for safety critical applications including the protection of potentially dangerous industrial processes. These systems are typically evaluated and certified by agencies like TUV according to qualitative standards (VDE0801/A1, [1]) with specific rules. Many factors are taken into account including hardware diagnostic capability, level of hardware redundancy, design processes used, software diagnostics and general equipment strength. But in a VDE0801/A1 evaluation, common cause strength is not evaluated.

Over the last few years, it has become recognized that common cause failures can have a major negative impact on the safety and availability of a fault tolerant system [2]. The whole value of redundancy may be ruined. A new standard for safety related systems, IEC61508 [3], is “performance based” and requires a quantitative assessment of hardware failure probability. Common cause is recognized as an important factor but there is disagreement regarding how to account for common cause in the quantitative modeling.

In previous work [4,5] it has been proposed that common cause strength is obtained by following three principles:

1. Reduce the chance of a common stress - physical separation and electrical separation in redundant units.
2. Respond differently to a common stress - redundant units should use diverse mechanisms.
3. Increased strength against all failures.

But general guidelines and rules do not help in establishing quantitative measures. While several models exist to conceptually model common cause failures, there is little published guidance on how to establish quantitative parameters to use in these models. It is hard to assign numbers to real implementations of fault tolerant systems.

Stress – Strength Simulation

Following the fundamental concept that all failures occur when a “stress” exceeds the associated strength [6,7], probability of failure could be determined if probability density functions were known for all stress and strength parameters. Time dependent failure rates could be plotted using Monte Carlo simulations. While this technique is impractical in an absolute sense in many situations, it is valuable for comparison purposes. In Figure 1, a stress-strength relationship is characterized. A plot of failure rate as a function of time resulting from a Monte Carlo stress-strength simulation is shown in Figure 2.

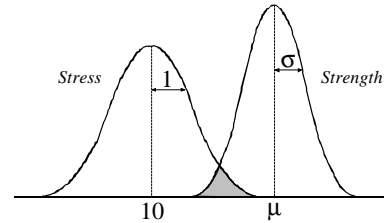


Figure 1 A Stress – Strength representation

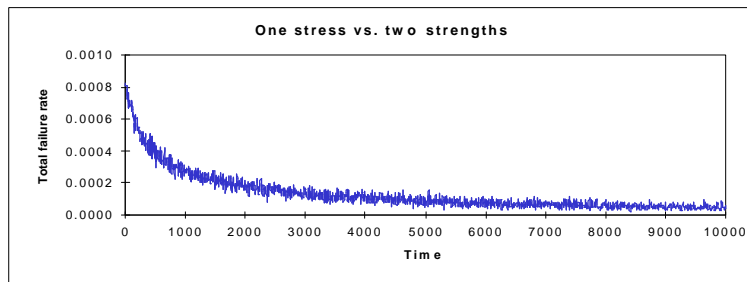


Figure 2 λ^{tot} for strength $N(+3.7, 0.5)$

Common Cause Simulation

In the context of fault tolerant safety PLCs used to protect industrial processes, a common cause failure occurs when two or more units of a redundant set fail in a short period of time due to some common stress. In most safety PLCs this can be effectively modeled with the beta model [8] especially if the definition of beta includes failures of two or more units. In some systems with three redundant units where two failures are required for system failure, it may be necessary to use a multi-parameter common cause model [9, 10].

Using Simulation to Characterize Common Cause

Stress – Strength Characterization of Common Cause

Stress – strength failure rate simulations can be used to characterize the parameters in a common cause model. If bounds and relationships to actual implementations can be established, these rules could aid in common cause parameter estimating.

Using the concept that all failures occur when some stress level exceeds the associated strength, a series of simulations were performed with different stress – strength density functions. For each simulation, sets of two and three units were each assigned a particular strength level randomly selected from the strength probability density function. A “time to failure” counter is set to zero.

The first series of simulations randomly chose a stress level and compare the strength of the “test units” to this common stress. A failure is counted is the stress is greater than the strength for a particular unit. If no failure occurs, the time count is incremented and the test is repeated until failure (or a maximum count) occurs. The “time to failure” for each unit was recorded. In some simulations, only one unit of the redundant set failed. This is not a common cause failure. In other simulations, more than one unit failed at the same time. This is a common cause failure. Analysis showed how frequently two units or three units failed due to common cause. The simulations were repeated for a series of different stress-strength probability density functions.

A second series of simulations followed the same procedure but subjected each unit to an independent randomly chosen stress level. This represents the best case use of the separation rule to increase common cause strength. Comparison of the two data sets show the value of increasing common cause strength via physical and electrical separation.

Results

The difference between the first and second set of simulations should provide upper and lower bounds on the effect of principle number one, “1. Reduce the chance of a common stress - physical separation and electrical separation in redundant units.”

Common Stress versus Independent Stress

For a fixed set of stress – strength parameters, the first set of simulations subjected the redundant units to a common stress. This represents redundant units physically mounted near each other or units with tight electrical coupling. The

Using Simulation to Characterize Common Cause

second set of simulations subjected each redundant unit to an independent stress from the same probability density function. This represents an implementation where redundant units are not physically or electrically coupled.

Overall, the probability of a common cause failure is substantially reduced when random stresses are independent. The differences were greater than expected. While it is recognized that total independence of stress levels in an actual fault tolerant implementation is not possible, the results indicate potential benefit in applying the rule. Table 1 shows a comparison of beta factors when two units were subjected to the stress. Common cause susceptibility typically dropped by two orders of magnitude.

Failure Rate (failures per hour) - λ	Strength Parameters - μ, σ	Common Stress β	Independent Stress β
142×10^{-6}	+3.7, 0.5	0.388	0.0028
48.2×10^{-6}	+4.7, 1.0	0.155	0.0048
14×10^{-6}	+4.7, 0.5	0.114	0.000

Table 1 β factors comparing common stress to independent stress

Common Cause versus Failure Rate

The results showed a relationship between failure rate and beta factor. The lower the failure rate the lower beta factor. This confirms principle three, "3. Increased strength against all failures." The higher the strength, the less chance of failure and lower chance of common cause failure. Table 2 shows common stress beta versus failure rate.

Failure Rate (failures per hour) - λ	Strength Parameters - μ, σ	Common Stress β
2846×10^{-6}	+2.7, 0.5	0.448
142×10^{-6}	+3.7, 0.5	0.388
14×10^{-6}	+4.7, 0.5	0.114

Table 2 β factors decreasing with failure rate

Common Cause versus Strength Variation

Common cause beta factors were clearly related to the variation in the strength distribution. This makes sense especially when taken to the limit. If all units in a redundant architecture had identical strength, they would always fail simultaneously. The beta factor would be one. Of course this is not realistic but it does imply that identical units that respond in the same way to a common stress will be more likely to have common cause failures. This supports principle two, "2.

Using Simulation to Characterize Common Cause

Respond differently to a common stress - redundant units should use diverse mechanisms.” For diversity to be effective, the redundant units must have different strengths for any given stress. Table 3 shows beta factors as a function of strength variation.

Failure Rate (failures per hour) - λ	Strength Parameters – μ, σ	Common Stress β
174×10^{-6}	+3.7, 1.0	0.366
142×10^{-6}	+3.7, 0.5	0.388
88×10^{-6}	+3.7, 0.1	0.408

Table 3 β factors increasing with strength variation

3.3.4 Common Cause versus Architecture

The probability of common cause failure is related to architecture [11]. When triplicated systems are exposed to a common stress, probabilities are as much as three times greater than dual systems over a range of stress-strength distributions where failure rates are low. The actual common cause failure rate will include sets of two failures in combination with sets of three failures [11]. For the simulation parameters chosen, a triplicated system had about twice the common cause failure rate. Table 4 shows beta factors for common stress simulations. Table 5 shows beta factors for independent stress cases.

Failure Rate (failures per hour) - λ	Strength Parameters – μ, σ	DUAL	TRIPLE
48.2×10^{-6}	+4.7, 1.0	0.155	0.269
174×10^{-6}	+3.7, 1.0	0.366	0.539

Table 4 β factors comparing dual versus triple for a common stress

Failure Rate (failures per hour) - λ	Strength Parameters – μ, σ	DUAL	TRIPLE
48.2×10^{-6}	+4.7, 1.0	0.0048	0.01
174×10^{-6}	+3.7, 1.0	0.054	0.09

Table 5 β factors comparing dual versus triple for an independent stress

4. Conclusion

Stress-strength simulation can provide guidance in estimating parameters for common cause models. The simulation results can be formulated into one of several different common cause models, especially those based on failure rates

(beta, extended beta, multi-parameter). The results to date show a strong benefit to reducing the chance of a common stress by physical separation of redundant units. The results show that higher strength designs with lower failure rates will have lower common cause failure rates. The results show that redundant units that respond differently to a common stress (different strength possibly due to diversity) will have lower common cause failure rates.

References

1. DIN V VDE0801 with Amendment A1, *Principles for computers in safety related systems*, Deutsche Elektrotechnische Kommission, January 1990, Amendment A1, November 1995.
2. Rutledge, P.J. and Mosleh, A., "Dependent-Failures in Spacecraft: Root Causes, Coupling Factors, Defenses, and Design Implications," *1995 Proceedings of the Annual Reliability and Maintainability Symposium*, IEEE, 1995.
3. IEC61508, *Functional safety: safety-related systems*, June 1997.
4. Bukowski, J. V. and Goble, W. M., "Common Cause - Avoiding Control System Failures," *Proceedings of Phila. ICS94 Conference*, Instrument Society of America, 1994.
5. Goble, W. M., "Safety of Programmable Electronic Systems - Critical Issues, Diagnostics and Common Cause Strength," *Proceedings of the IChemE Symposium*, IChemE, 1995.
6. Brombacher, A. C., *Reliability by Design CAE Techniques for Electronic Components and Systems*, J. Wiley, Chichester, 1992
7. Goble, W. M., *Control System Safety Evaluation and Reliability*, ISA, Raleigh, N.C., 1998.
8. Fleming, "A Probabilistic Model for Moon Mode Failures in Redundant Safety Systems," General Atomic Report, GA-13284, 1974.
9. Bukowski, J. V., and Goble, W. M., "An Extended Beta Model to Quantize the Effects of Common Cause Stressors," SAFECOMP'94, Springer, London, 1994.
10. Mosleh, A. and Siu, N., "A Mult-Parameter Common Cause Failure Model," CRTS-B9-12, Center for Technology Risk Studies, College Park, MD. 1987.
11. Bukowski, J. V. and Lele, A., "The Case for Architecture-Specific Common Cause Failure Rates and How They Affect System Performance," *1997 Proceedings of the Annual Reliability and Maintainability Symposium*, IEEE, 1997.
12. van Beurden, I. J. W. R. J., Stress-Strength simulations for common cause modeling, RME, Eindhoven University of Technology, Eindhoven, Netherlands, August 1997.