

Estimating the Common Cause Beta Factor

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

Introduction

Safety Instrumented Systems (SIS) are often designed to help protect an industrial process against potentially dangerous hazards. These systems often use redundant equipment to achieve the needed levels of protection. If the design was done to meet requirements of IEC 61511 [1] or IEC 61508 [2], probabilistic evaluation is done to verify that the design achieves risk reduction goals.

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 redundant equipment [3, 4]. The whole value of redundancy may be ruined. This is clearly recognized by IEC 61508 and probabilistic analysis now requires a quantitative assessment of common cause.

In previous work [4,5,6] 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 technology / mechanisms.
3. Increased strength against all failures.

But these general guidelines and rules do not help in establishing quantitative measures.

Common Cause Modeling

Several models exist to conceptually model common cause failures [7,8,9]. While these models offer sophistication, the simplest model called the beta model is sufficient if conservatively applied. Probability theory and simulation [10,11] state that different beta factor values must be used for different types of redundant architectures. However even this can be simplified by choosing conservative values for the beta factor.

Estimating the Common Cause Beta Factor

Choosing the Beta Factor

Studies that statistically estimate the beta factor have been done [3]. These indicate that a number in the range of 1% to 10% is valid for equipment used in conditions similar to industrial process control. A detailed statistical study analyzing the beta factor for a particular process plant is likely not available. Therefore the beta factor must be estimated based on plant conditions.

A method for doing this is provided in IEC 61508, part 6. This portion of the standard is only informative and other techniques may be used to estimate the beta factor. While other techniques for estimating the effects of common cause may be justified, the use of the methods in Part 6 of IEC 61508 make sense especially when attempting to show compliance with IEC 16508 or IEC 61511.

The approach presented in IEC 61508 requires that a series of questions be answered. For each positive answer, points are scored. Points from each question are added. Based on the total points, the beta factor number is determined from Table D.4, repeated below. For example, if the affirmative answers to the questions add up to 76 points for a transmitter, the beta factor for redundant transmitters will be 2%.

Score (S or S _D)	Corresponding value of b or b _D for the:	
	Logic system	Sensors or actuators
120 or above	0.5%	1%
70 to 120	1%	2%
45 to 70	2%	5%
Less than 45	5%	10%
NOTE 1 The maximum levels of β _D shown in this table are lower than would normally be used, reflecting the use of the techniques specified elsewhere in this standard for the reduction in the probability of systematic failures as a whole, and of common cause failures as a result of this.		
NOTE 2 Values of β _D lower than 0.5% for the logic system and 1% for the sensors would be difficult to justify.		

Table 1 - IEC 61508 Part 6, Table D.4

At first the process seems quite complicated but it can quite simple if a conservative engineering approach is used. The simplest approach is to use the maximum values from the table. For field instruments (sensors, final elements) the maximum number for the beta factor is 10%. For logic solvers, the maximum number for the beta factor is 5%. If these maximum numbers are used in the PFDavg calculations and the design meets the required SIL level, the job is finished.

Estimating the Common Cause Beta Factor

If the common cause portion of the PFDavg is significant then a more detailed review of the IEC 61508, Part 6 questions will be worth the time. Many of the questions relate to product choice. If a product is chosen from a high quality manufacturer that does full environmental testing, then points are scored (20). If detailed common cause analysis was done as part of the design then points are scored (6). If a product is chosen that has been proven in use in similar applications for at least 5 years, then points are scored (5). If the product manufacturer maintains a good field return database system with feedback to the product developers, more points are scored (4). If the product has protection against over-voltage and uses conservatively rated components then another 4 points are scored. Thirty-nine points can be scored as a result of good product selection.

Remaining questions focus on how the product is installed and maintained. Physical separation of redundant components, cabling and power supplies are counted (16 points). Different technologies used in a redundant system are given credit (13 points). Additional credit is given for:

- a) Work procedures that test different components on a staggered schedule
- b) Work procedures that require completion of one before starting another
- c) Maintenance of change procedures that do not allow repositioning of equipment without a common cause review
- d) Training of system designers and maintenance personnel in common cause
- e) Limited access to redundant equipment and
- f) Checking of environmental conditions at installation time.

Example – 2oo3 Pressure Transmitters

A design is being evaluated where three Rosemount 3051S pressure transmitters are chosen. The transmitters are connected to a logic solver programmed to detect over-range and under-range currents as a diagnostic alarm. The process is not shutdown when an alarm occurs on one transmitter. The logic solver has a two out of three (2oo3) function block that votes to trip when two of the three transmitters indicate the need for a trip.

Following the questions from the sensor portion of Table D.1 of IEC 61508, Part 6, the following results are obtained.

Estimating the Common Cause Beta Factor

Item	X _{SA}	Y _{SA}	Example	Score
Are all signal cables for the channels routed separately at all positions?	1.0	2.0	Not guaranteed	0.0
If the sensors/actuators have dedicated control electronics, is the electronics for each channel on separate printed-circuit boards?	2.5	1.5	Transmitters are separate	4.0
If the sensors/actuators have dedicated control electronics, is the electronics for each channel indoors and in separate cabinets?	2.5	0.5	Transmitters are in different housings	3.0
Do the devices employ different physical principles for the sensing elements for example, pressure and temperature, vane anemometer and Doppler transducer, etc.	7.5		No – transmitters are identical	0.0
Do the devices employ different electrical principles/designs for example, digital and analogue, different manufacturer (not re-badged) or different technology	5.5		No – transmitters are identical	0.0
Do the channels employ enhanced redundancy with MooN architecture, where $N > M + 2$	2.0	0.5	No – 2oo3	0.0
Do the channels employ enhanced redundancy with MooN architecture, where $N = M + 2$	1.0	0.5	No – 2oo3	0.0
Are separate test methods and people used for each channel during commissioning?	1.0	1.0	No - impractical	0.0
Is maintenance on each channel carried out by different people at different times?	2.5		No - impractical	0.0
Does cross-connection between channels preclude the exchange of any information other than that used for diagnostic testing or voting purposes?	0.5	0.5	No cross channel information between transmitters	1.0
Is the design based on techniques used in equipment that has been used successfully in the field for > 5 years?	1.0	1.0	3051S based on well proven design	2.0
Is there more than 5 years experience with the same hardware used in similar environments?	1.5	1.5	Extensive experience in process control	3.0
Are inputs and outputs protected from potential levels of over-voltage and over-current?	1.5	0.5	Transient voltage and current protection provided	2.0
Are all devices/components conservatively rated? (for example, by a factor of 2 or more)	2.0		Design has conservative rating factors proven by field reliability	2.0
Have the results of the failure modes and effects analysis or fault tree analysis been examined to establish sources of common cause failure and have predetermined sources of common cause failure been eliminated by design?		3.0	FMEDA done by third party – exida. No common cause issues	3.0
Were common cause failures considered in design reviews with the results fed back into the design? (Documentary evidence of the design review activity is required.)		3.0	Design review is part of the development process. Results are always fed back into the design	3.0
Are all field failures fully analysed with feedback into the design? (Documentary evidence of the procedure is required.)	0.5	3.5	Field failure feedback procedure reviewed by third party – exida. Results are fed back into the design.	4.0
Is there a written system of work which will ensure that all component failures (or degradations) are detected, the root causes established and other similar items are inspected for similar potential causes of failure?	0.5	1.5	Proof test procedures are provided but they cannot insure root cause failure analysis.	0.0
Are procedures in place to ensure that: maintenance (including adjustment or calibration) of any part of the independent channels is staggered, and, in addition to the manual checks carried out following maintenance, the diagnostic tests are allowed to run satisfactorily between the completion of maintenance on one channel and the start of maintenance on another?	2.0	1.0	Procedures are not sufficient to ensure staggered maintenance.	0.0

Estimating the Common Cause Beta Factor

Do the documented maintenance procedures specify that all parts of redundant systems (for example, cables, etc.), intended to be independent of each other, must not be relocated?	0.5	0.5	Management of change procedures require a review of proposed changes. However, relocation may inadvertently be done.	0.0
Is all maintenance of printed-circuit boards, etc. carried out off-site at a qualified repair centre and have all the repaired items gone through a full pre-installation testing?	0.5	1.5	Repair is done by returning material to the factory, therefore this requirement is met.	2.0
Do the system diagnostic tests report failures to the level of a field-replaceable module?	1.0	1.0	Logic solver is programmed to detect current out of range and report the specific transmitter.	2.0
Have designers been trained (with training documentation) to understand the causes and consequences of common cause failures	2.0	3.0	Control system designers have not been trained.	0.0
Have maintainers been trained (with training documentation) to understand the causes and consequences of common cause failures	0.5	4.5	Maintenance personnel have not been trained.	0.0
Is personnel access limited (for example locked cabinets, inaccessible position)?	0.5	2.5	A tool is required to open the transmitter therefore this requirement is met.	3.0
Will the system be operating within the range of temperature, humidity, corrosion, dust, vibration, etc., over which it has been tested, without the use of external environmental control?	3.0	1.0	Environmental conditions are checked at installation.	4.0
Are all signal and power cables separate at all positions?	2.0	1.0	No	0.0
Has a system been tested for immunity to all relevant environmental influences (for example EMC, temperature, vibration, shock, humidity) to an appropriate level as specified in recognized standards?	10.0	10.0	Rosemount has complete testing of all environmental stress variables and run-in during production testing.	20.0
Totals				58

Table 2 Example version of Table D.1, Part 6 IEC 61508

A score of 58 results in a beta factor of 5%. If the owner-operator of the plant would institute common cause training and more detailed maintenance procedures specifically oriented toward common cause defense, a score of greater than 70 could be obtained. Then the beta factor would be 2%.

Note that the diagnostic coverage for the transmitter is not being considered. Additional points can be obtained when diagnostics are taken into account. However this assumes that a shutdown occurs whenever any diagnostic alarm occurs. In the process industries this could even create dangerous conditions. Therefore the practice of automatic shutdown on a diagnostic fault is rarely implemented. IEC 61508, Part 6 has a specific note addressing this issue. The note states:

“NOTE 5 In the process industries, it is unlikely to be feasible to shut down the EUC when a fault is detected within the diagnostic test interval as described in table D.2. This methodology should not be interpreted as a requirement for process plants to be shut down when such faults are detected. However, if a shut down is not

implemented, no reduction in the b-factor can be gained by the use of diagnostic tests for the programmable electronics. In some industries, a shut down may be feasible within the described time. In these cases, a non-zero value of Z may be used.”

In this example, automatic shutdown on diagnostic fault was not implemented so no credit for diagnostics was taken.

Conclusion

Estimating the beta factor can seem a complicated and perhaps even impossible task. This statement would be true is one attempted to use a detailed statistical approach based on studies of field inspection data. However, the IEC 61508 standard provides a relatively simple but conservative approach to the problem. Using this approach one can easily obtain an estimate that can be used in SIF probabilistic verification calculations.

References

1. IEC61511, Functional Safety, Application in the process industries, 2003.
2. IEC61508, *Functional safety: safety-related systems*, 1998/2000.
3. 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.
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. Goble, W. M., *Control System Safety Evaluation and Reliability*, ISA, Raleigh, N.C., 1998.
7. Fleming, "A Probabilistic Model for MooN Mode Failures in Redundant Safety Systems," General Atomic Report, GA-13284, 1974.
8. Bukowski, J. V., and Goble, W. M., "An Extended Beta Model to Quantize the Effects of Common Cause Stressors," SAFECOMP'94, Springer, London, 1994.

9. Mosleh, A. and Siu, N., "A Mult-Parameter Common Cause Failure Model," CRTS-B9-12, Center for Technology Risk Studies, College Park, MD. 1987.

10. 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.

11. van Beurden, I. J. W. R. J., Stress-Strength simulations for common cause modeling, RME, Eindhoven University of Technology, Eindhoven, Netherlands, August 1997.