COMMON CAUSE FAILURE (CCF):

A PATH TO QUANTITATIVE SUCCESS

John Erinc, Steve Seaman and Jonathan Baisch
Westinghouse Electric Corporation
1000 Westinghouse Drive
Cranberry Township, PA 16066, USA
Erincjb@westinghouse.com; Seamans@westinghouse.com; Baischje@westinghouse.com

ABSTRACT

In the development of I&C systems for nuclear plants it is critical to validate a defense in depth strategy through a thorough and complete reliability analysis program. An emerging issue is how to define and use a quantitative estimation of CCF in a system analysis. Industry standards provide insight but not necessarily a comprehensive approach. One solution is to leverage existing modeling techniques with a unique insertion of CCF probabilities. A relatively simple approach will be provided using reliability block diagrams. Three specific areas that will be explored include:

1. Definition of hardware CCF
2. Quantitative estimation in a simple system
3. Quantitative estimation in a complex system.

Key Words: CCF, Nuclear, I&C quantitative, reliability block diagram

1 INTRODUCTION:

The reliability of I&C systems in nuclear power plants is critical to providing safe operation. A defense in depth approach has been used to provide assurance that the I&C system will perform the required functionality. It is critical to understand the behavior and failure modes to provide confidence that the I&C systems will perform as required. Redundancy is widely used as a tool to address single failures in the system, but Common Cause Failure (CCF) across the redundant elements can defeat the redundancy. With the increased use digital system, the impact of CCF has received increased attention. CCF's significance can defeat the redundancy employed to improve the reliability of safety functions. Operating experience has shown that CCF is a major contributor to plant risk.

CCF as defined by IEC 62340 is the failure of two or more structures, systems or components due to a single specific event or cause. The coincidental failure of two or more structures, systems or components is caused by any latent deficiency from design or manufacturing, or from operation or maintenance errors, and which is triggered by any event induced by natural phenomenon, plant process operation or a human caused action or by any internal event in the I&C system. A great deal of the work by the industry has been focused on the cause and prevention of CCF. There has not been as much work on how to properly model the effects of CCF in the reliability analysis of the I&C system.

NUREG/CR-5485 provides guidance on a how to apply a beta factor model to the I&C systems and therefore provides an acceptable representation of the contribution of CCF to the quantitative results. With the beta factor model, only the purely independent events and a global common cause event that fails all components in a common cause group are included in the model. A variation of this is to also include common cause events that fail two and three components.

IEC 61508-6 provides guidance on estimating CCFs employing the Beta Factor method for I&C. Based on the assessment of various factors that could contribute to CCFs, a factor (β) is estimated, which is then used as a multiplier of the single channel failure rate to determine an estimate of the CCF frequency. This method has been shown to be appropriate for hardware-based I&C systems. The Beta Factor approach has the following benefits.

- Does not need component success data.
- Simplicity in use
- Provides conservative results for redundancy levels beyond two (2).

1.1 Problem Definition

For relatively simple redundant constructs, the first step in evaluation, using Reliability Block Diagram (RBD), is to calculate the failure rate of the individual blocks for each branch. Depending on the number of blocks in a branch, the series blocks of the diagram are collapsed into one block, representing any one of the component branch's functionality. One collapsed block failure rate representing the redundant branch is used with the β factor to define the CCF contribution.

$$CCF = \beta\left(\lambda_1\right)$$

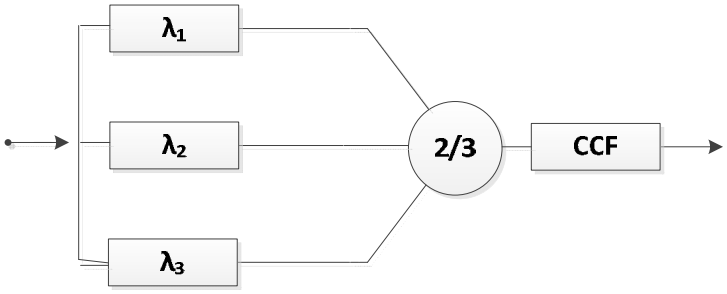

Figure 1. Simple System

The redundant blocks are combined into an abstract block representing the redundant branches. For N-out-of-M redundancy, the equation below produces the failure rate value for the branches.

$$F_{N/M} = \frac{M!(\lambda)^{M-N+1}}{(N-1)!(\mu)^{M-N}}$$

Using this equation requires the repair rate to be estimated, in addition to the unit failure rate. The block representing the N-out-of-M redundancy is serially added with the CCF contribution of the individual branch. Placing the CCF prior to the redundancy would lessen its impact and fail to address the contribution to all redundant branches.

$$\lambda = CCF + F_{N/M}$$

For the functions where redundancy is straightforward, the CCF blocks are added in series after each redundancy that shares a component, thus applying the CCF penalty to each redundancy. This appropriately applies the CCF penalty by not minimizing its impact. This process can be repeated for all instances of redundancy and account for the CCF contribution associated with the redundancy. This allows the RBD method to account realistically for contributions of CCF, when redundancy is a strategy for fault tolerance.

The challenge is when the relatively simple redundant constructs do not apply, such as when power schemes become complex. An example of a complex scheme is shown in Figure 2.

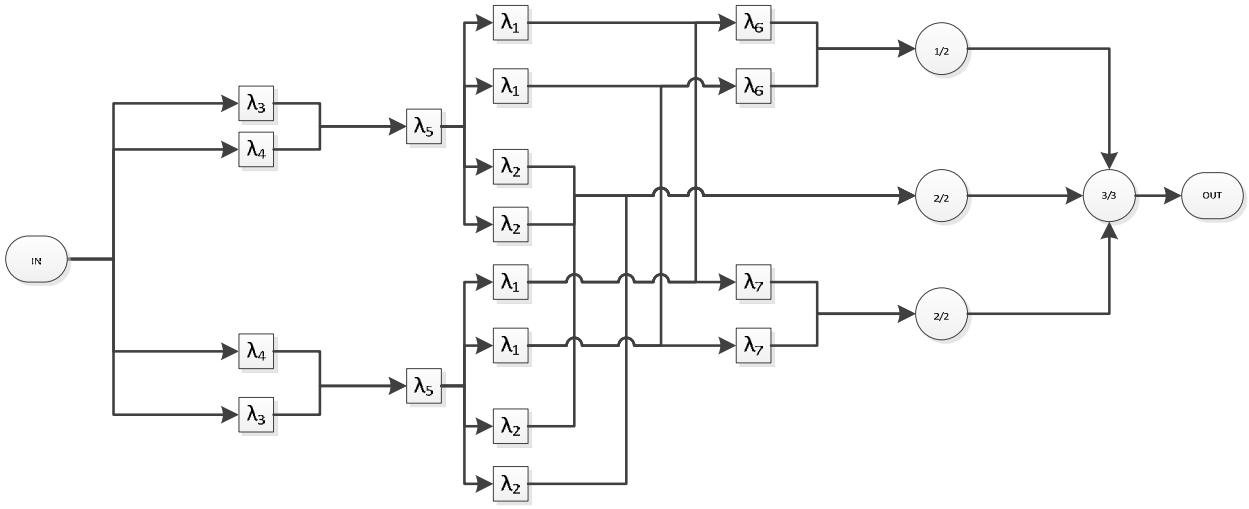

Figure 2. Complex System

Power schemes are complex and may require the use of a truth table for calculation for the reliability values. These truth tables can be extensive (1000+ rows each). The CCF contribution cannot be easily associated with each redundant branch for at least two reasons. First, placement of the CCF after each branch may result in the minimization of the CCF contribution by subsequent redundancy calculations further downstream. Second, the CCF contribution may not be completely addressed based the multiple parallel paths.

1.2 Common Cause Failure Rate and Availability

The beta-factor method adds blocks to a block diagram as a penalty to account for CCF. To determine hardware CCF availability, the failure rate of this block is a percentage of the failure rate of a common component that can experience CCF.

Since the beta-factor serves as a scaling factor for the failure rate (λ_E), and there is an inverse correlation between availability and failure rate, the CCF availability can be calculated based on the beta-factor and the component availability. The following shows the development of the CCF availability equation.

$$. \ _E = \left\{1 + \lambda_E \left[(1 \quad _D)\frac{T_S}{2} + MRT\right]\right\}^{-1} \Rightarrow \ _E{}^{-1} \ 1 \ = \lambda_E \left[(1 \quad _D)\frac{T_S}{2} + MRT\right]$$

$$\lambda_E = \left[A_E{}^{-1} \ 1 \ \right] * \left[(1 \quad _D)\frac{T_S}{2} + MRT\right]^{-1} \qquad (1)$$

Incorporating the beta-factor in the Equation (1) (as $\beta\lambda_E$) and replacing λ_E:

$$A_{E\_CCF} = \left\{1 + \beta\lambda_E \left[(1 \quad P_D)\frac{T_S}{2} + MRT\right]\right\}^{-1} \Rightarrow \ _{E\_CCF}$$

$$= \frac{1}{1 \quad \frac{A_E{}^{-1} \ 1}{\cancel{(1 \quad P_D)\frac{T_S}{2} + MRT}} \cancel{\left[(1 \quad P_D)\frac{T_S}{2} + MRT\right]}}$$

$$A_{E\_CCF} = \frac{1}{\beta\left(\frac{1}{A_E} - 1\right) + 1} \qquad (2)$$

The result is the availability that incorporates CCF.

1.3 CCF Availability versus CCF Failure Rate Calculation

Now that the CCF availability equation (#-2) has been derived a simple and complex example will be examined and comparisons of CCF availability and CCF failure rate methods will show that equation #-2 is a viable alternative to incorporate CCF into RBDs.

The CCF Beta factor used in the model has to be determined using the method in IEC-61508-2 Annex D. For this paper a Beta of 2% was selected as it is a common scaling factor for I&C system hardware.

The following equations are used for the RBD calculations:

Series Availability:

$$Av = \ A * B * C * D \quad (3)$$

2oo3 Voter Availability:

$$Av_{2oo3} \quad 3Av^2 \ 2 \ Av^3 \quad (4)$$

Failure Rate from Availability:

$$\lambda = \frac{\frac{1}{Av}-1}{(1-P_d)*\frac{T_S}{2}+MTTR} \quad (5)$$

CCF Failure Rate:

$$\lambda_{CCF} = \beta * \lambda_{Av} \quad (6)$$

Availability from Failure Rate:

$$Av_{CCF} = \frac{1}{(1+\lambda*(1-P_D)*\frac{T_S}{2}+MTTR} \quad (7)$$

Availability Parallel Paths (1oo2):

$$Av_{parallel} \quad 1-(1 \quad v)-(1 \quad v) \quad (8)$$

1.3.1 Simple RBD Example

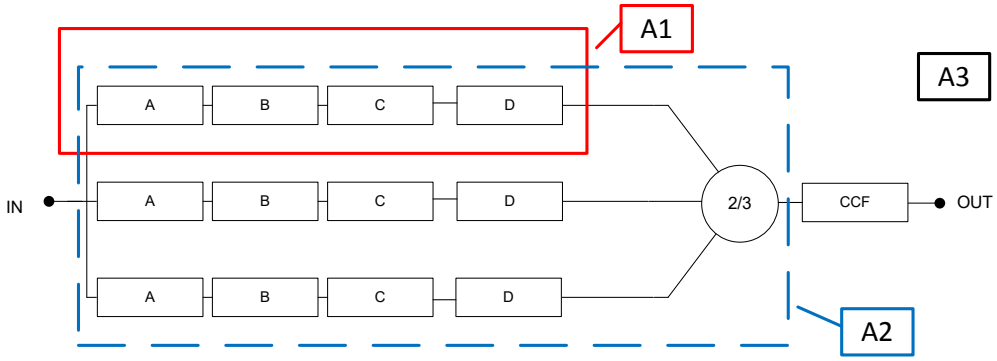

Figure 3. 2oo3 Voter with CCF

Figure 3 depicts a 2oo3 voter with a CCF block. Analysis is provided below using equations as listed in the equations column of Table II. Table II provides the analysis results. Component failure rates, Sample times, probability of detection, and MTTR are taken from a real analysis and found in Table I.

Table I. Component Reliability Attributes					
Component	**λ (Failures/hr.)**	**P_D**	**T_S (hr.)**	**MTTR (hr.)**	**Availability**
A	1.17E-06	0	2208	24	$9.986820E^{-01}$
B	7.24E-07	0	2208	24	$9.991840E^{-01}$
C	9.93E-07	0	2208	24	$9.988811E^{-01}$
D	3.00E-08	0	2208	24	$9.999661E^{-01}$

In both cases the common cause failure block is added in series after the 2oo3 function.

Table II. Simple Case Calculations				
Calc. #	**Calculation**	**Equations**	**Figure Call Out**	**Availability**
1	Availability of One Leg of 2oo3	(3)	Figure 1.5.1-1 A1	$9.967168E^{-01}$
2	Availability of the 2oo3	(4)	Figure 1.5.1-1 A2	$9.999677E^{-01}$
3	CCF Availability Method (using one leg 2oo3)	(2)	N/A	$9.999341E^{-01}$
4	Failure Rate of One Leg of 2oo3	(5)	N/A	$2.920208E^{-06}$ failures/hr.
5	CCF Failure Rate	(6)	N/A	$5.840416E^{-08}$ failures/hr.
6	CCF Availability from Failure Rate	(7)	N/A	$9.999341E^{-01}$
7	Availability of 2oo3 w/ CCF	(3)	Figure 1.5.1-1 A3	$9.999019E^{-01}$

As can be seen in calculations 3 and 6 the CCF availability is the same with both methods. Thus for calculation 7 the availability with CCF is the same. For the simple case these two methods are equivalent and equation #-2 holds.

1.3.2 Complex RBD Example

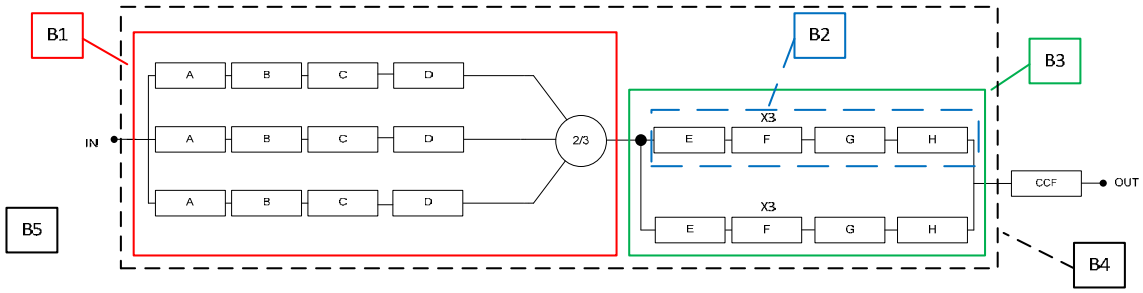

Figure 4. Complex RBD for CCF Availability Method

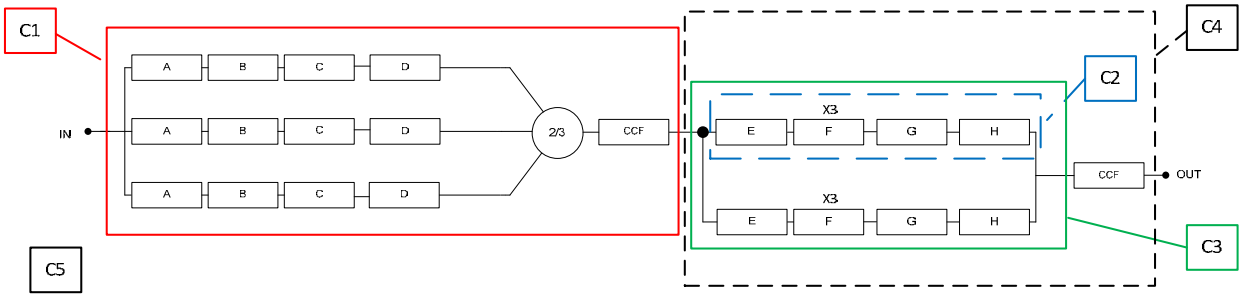

Figure 5. Complex RBD for CCF Failure Rate Method

Progressing from the simple case, this example adds a set of parallel components in series with the first example. A comparison of Figures 4 and 5 shows the purpose of the CCF Availability Method and its advantages. Placing a CCF adder at the end of a complex RBD instead of inline for each redundancy is simple, in terms of calculations and understanding, and provides very similar results (as shown by this example) to the more complex inline method.

This example will compare the availability method (EQN (2)) applied after the entire RBD has been simplified against the failure rate method that will be applied to each set of parallel paths, i.e. a CCF block for the 2oo3 and a CCF block for the parallel path. Component failure rates, Sample times, probability of detection, and MTTR are taken from a real analysis and found in Table III.
Table IV provides the CCF Availability analysis results and references the equations used to achieve them. Table V provides the CCF failure rate analysis results and references the equations used to achieve them.

Table III. Component Reliability Attributes					
Component	**λ (Failures/hr.)**	**P_D**	**T_S (hr.)**	**MTTR (hr.)**	**Availability**
A	1.17E-06	0	2208	24	$9.986820E^{-01}$
B	7.24E-07	0	2208	24	$9.991840E^{-01}$
C	9.93E-07	0	2208	24	$9.988811E^{-01}$
D	3.00E-08	0	2208	24	$9.999661E^{-01}$
E	7.61E-07	0	2208	24	$9.991423E^{-01}$
F	5.41E-07	0	2208	24	$9.952733E^{-01}$
G	1.00E-07	0	2208	24	$9.998872E^{-01}$
H	1.61E-07	0	2208	24	$9.998181E^{-01}$

Table IV. Complex Evolved Case CCF Availability Method				
Calc. #	**Calculation**	**Equations**	**Figure Call Out**	**Availability**
1	Availability of the 2oo3 (from Table 1.5.1-2)	(4)	Figure 4 B1	$9.999667E^{-01}$
2	Availability One Leg of the Parallel Path	(3)	Figure 4 B2	$9.847508E^{-01}$
3	Availability Parallel Path	(8)	Figure 4 B3	$9.997675E^{-01}$
4	Availability of the Simple Evolved Example	(3)	Figure 4 B4	$9.997352E^{-01}$
5	CCF Availability Method	(2)	N/A	$9.999947E^{-01}$
6	Availability with CCF of the Simple Evolved Example	(3)	Figure 4 B5	**$9.997299E^{-01}$**

Table V. Complex Evolved Case CCF Failure Rate Method				
Calc. #	**Calculation**	**Equations**	**Figure Call Out**	**Availability**
1	Availability of the 2oo3 with CCF (from Table 1.5.1-2)	(3)	Figure 5 C1	$9.999019E^{-01}$
2	Availability One Leg of the Parallel Path (from Table 1.5.2-2)	(3)	Figure 5 C2	$9.847508E^{-01}$
3	Failure Rate of the Parallel Path Leg	(5)	Figure 5 C2	$1.372813E^{-05}$ failures/hr.
4	Parallel Path CCF Failure Rate	(6)	N/A	$2.745626E^{-07}$ failures/hr.
5	Parallel Path CCF Availability from Failure Rate	(7)	N/A	$9.996904E^{-01}$
6	Availability Parallel Path (From Table 1.5.2-3)	(8)	Figure 5 C3	$9.997675E^{-01}$
7	Availability Parallel Path with CCF	(3)	Figure 5 C4	$9.994579E^{-01}$
8	Availability with CCF of the Simple Evolved Example	(3)	Figure 5 C5	**$9.993598E^{-01}$**

1.3.3 Simple Evolved Example Methods Comparison

The availability with CCF for the simple evolved case was calculated using the CCF availability method and the CCF failure rate method. The difference in results is provided in Table VI.

Table VI. CCF Availability vs. Failure Rate Method	
CCF Availability Method	0.9997299
CCF Failure Rate Method	0.9993598
Difference	0.0003700705

2 CONCLUSIONS

These two methods, under the constraints of this paper, produce very similar results with a difference of 0.0003700705. More importantly for reliability analysis purposes these two availabilities are in the same order of magnitude. Using this approach for high integrity system I&C, lends itself to addressing complex architectures that are encountered. This approach can be used in the safety I&C, depending on the level of precision demanded in the analysis.

With future sensitivity analysis this technique can be improved and its accuracy validated. This sensitivity can extend to surveillance times, mean time to repair complexity and software CCF inclusion.

3 REFERENCES

1. A. Mosleh, D.M. Rasmuson, F.M. Marshall, NUREG/CR-5485, "*Guidelines on Modeling Common-Cause Failure in Probabilistic Risk Assessment*," U.S. Nuclear Regulatory Commission, (November 1998).
2. IEC 62340:2007, "*Nuclear power plants – Instrumentation and control systems important to safety – Requirements for coping with common cause failure (CCF)*", International Electrotechnical Commission, (2007).
3. IEC 61508-6, "*Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*", International Electrotechnical Commission, (2010).