How to integrate correctly hardware common cause failures in frequency calculations?

Hervé Brunelière[a*], Monica Rath[a], and Wenjie Qin[a]
[a] AREVA NP SAS, Paris La Défense, France

Abstract: Hardware common cause failures are generally the highest contributors in the I&C systems reliability and availability studies.
Comparisons of results from calculations of frequency of spurious actuations by a safety system or frequency of failures of a control system with operation feedback of such failures show that the frequency calculations are often overestimated. This is due to the use of « classic » common cause failure parameters.
This is mainly explained by the fact that, for these undesired events, failures are generally not hidden ones and are then detected within few hours. Then, for common cause failures that are not simultaneous, the first failure is often repaired before the second one appears.
This over conservatism can lead to inappropriate design choices like addition of redundancies or interlocks to minimize the frequency of an undesired event based on a calculation that does not reflect the real situation. This is then a concern for a designer and for a utility to limit as far as possible the impact of this over conservatism.
One solution is to consider only independent failures in frequency calculations. In this case, the result is underestimated as simultaneous common cause failures that are possible and credible are not considered in the result. Then, the risk is not to implement some necessary measures in the design due to over optimistic results.
The paper will discuss possible solutions to handle these types of failures in calculations based on real cases.
Illustrations will be based on a typical architecture of an I&C system based on Teleperm XS platform similar to the ones currently implemented in nuclear power plants.
The paper will also integrate discussions on relevance of the different methodologies including no consideration of CCF at all, degraded CCF factors values and possibilities of extrapolation. These methodologies will be compared based on their impact on calculation results and the consistency with operational experience.

Keywords: CCF, frequency, methodology, failure mode

1. GOALS

The goal of the paper is to make a status of AREVA NP SAS work in progress for the improvement of consideration of common cause failures in frequency calculations. Illustration example is based on a typical and theoretical architecture of an I&C system based on Teleperm XS (TXS) platform similar to the Protection Systems currently implemented in nuclear power plants.
Relevance of the different methodologies is preliminarily assessed. These methodologies are mainly compared based on their impact on calculation results and on the consistency with operational experience.

2. CONTEXT

2.1. Typical CCF methodology

In European countries, Common Cause Failures (CCF) are generally calculated using extended beta factors methodology.

The probability of failure due to CCF of k out of m identical components is assessed using following equation:

$$Q_m^k = \beta_m^k Qt \quad (1)$$

Where Qt is the probability of failure of one component

Typical values for β_n^n are:

$$\beta_2^2 = 0{,}05 \quad (2)$$

$$\beta_3^3 = 0{,}02 \quad (3)$$

$$\beta_4^4 = 0{,}01 \quad (4)$$

These data are mostly used for projects in Europe. They were even previously given in European Utility Requirements in the Probabilistic Safety Assessment chapter but were removed in last version.

This method has following properties:

- It distinguishes partial and total loss of components that are subject to CCF.
- Probability of CCF is proportional to probability of failure of one component.
- Application of the method assumes that all CCF happen simultaneously.
- The commonly used values for these extended beta factors are quite high.

The two last properties are consequence of the fact that most calculations are made for assessing probability of failure on demand of redundant mitigation means. Then the most significant contributors are Common Cause Failures of non self-monitored failures that are only detectable during periodic tests. “Standard” beta factors take then into account accumulation of faults between two periodic tests, i.e. failures revealing in a typical interval of several months. Their adequacy to failure modes that are detectable within few hours is challengeable.

2.2. Increasing need for frequency calculations

The context is evolving in the nuclear industry:

- Focus is more and more made on availability aspects in parallel to safety concerns.
- Robustness of the preventive line (all means that control the plant in order to avoid any event that could lead to occurrence of incidents and accidents) is more and more important.

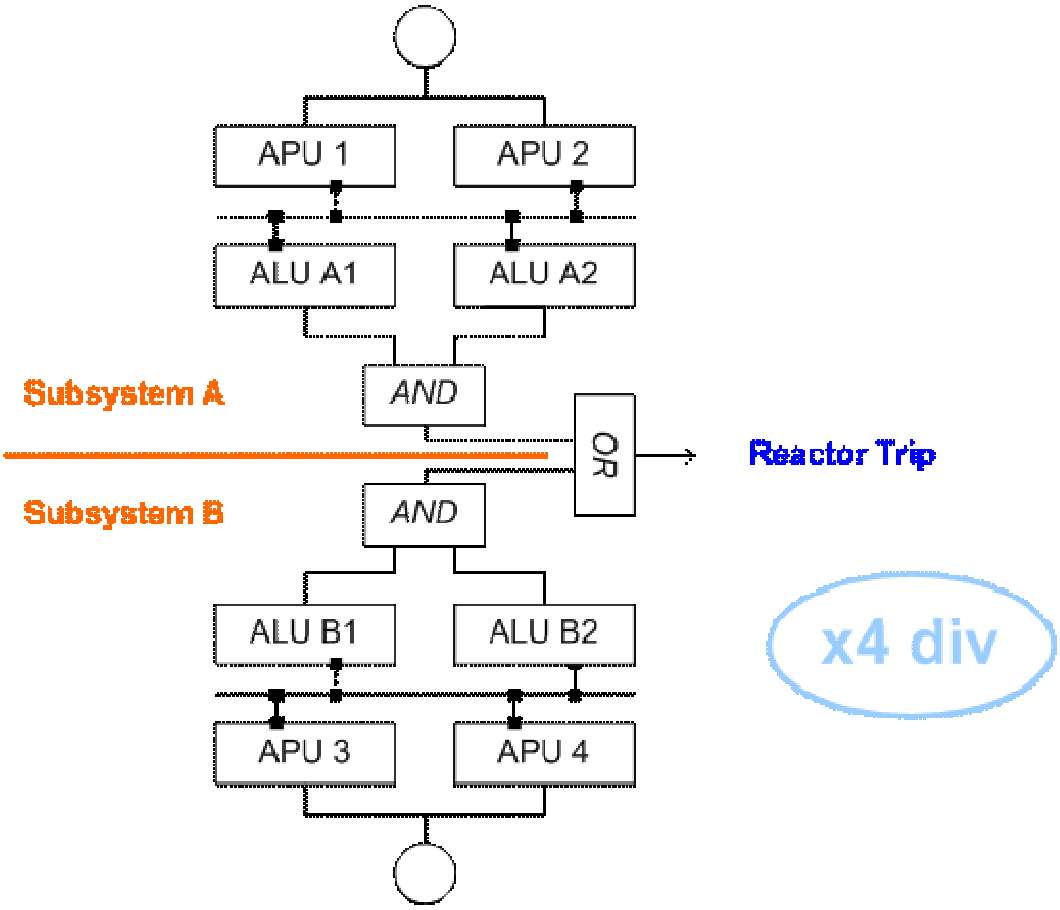
It is then necessary to focus on undesired events like failure of control functions, occurrence of a postulated initiating event or spurious actuation of safety functions. These events are of course quantitatively evaluated by calculating their frequencies.

3. ILLUSTRATION EXAMPLE

In order to show concretely how the subject raised by this paper is of importance, it is chosen to make an illustration example based on a theoretical architecture of a Protection System based on Teleperm XS platform. Frequency of spurious Reactor Trip actuation is assessed with different assumptions on CCF values.

3.1. System architecture and other main assumptions

Figure 1: Simplified architecture of the theoretical Teleperm XS based Protection System (one division)



Reactor Trip functions are implemented in the Acquisition and Processing Units (named APUx) and Acquisition and Logic Units (named ALUs) of the four divisions. In each APU, the result of each threshold is transferred in the ALUs of the four divisions. The ALUs are performing 2-out-of-4 logic between redundant signals from APUs. If threshold result(s) have a faulty status, the voting logic is degraded as follows:

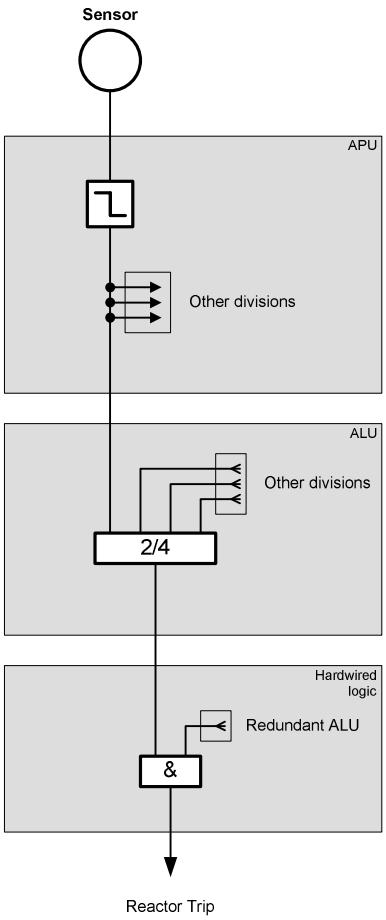
Table 1: Degradation of voting logics inside the theoretical Teleperm XS based Protection System

Number of faulty inputs	Voting logic
0	2-out-of-4
1	2-out-of-3
2	1-out-of-2
3 or 4	Actuation

In every division, the two ALUs of each sub-system are generating de-energized orders, which are combined with a functional AND logic (electrical OR). For reactor trip order of one division, the signals coming from both sub-systems are combined with a functional OR logic (electrical AND).

The functional structure is given in Figure 2.

Figure 2: Logical implementation of Reactor Trip functions in the theoretical Teleperm XS based Protection System (one division)



Main assumptions related to the calculations are given hereafter:

- Sensors, actuators and support systems are not considered. Only automation system failures are taken into account.
- Every spurious failure is assumed to be detected and repaired in an interval of less than 8 hours (time between occurrence of the failure and start up of the new or repaired I&C module).
- Software failures are not considered here as their potential for CCF is to be considered separately for hardware failures and their integration is not useful for the aim of this paper.

3.2. Results with conservative beta factors

3.2.1. Results with conservative beta factors

When calculating their frequencies with common cause factors as described in section 2.1:

- Frequency of spurious reactor trip due to the theoretical Protection System is 2.4E-05 per hour which corresponds to 2.1E-01 per year, i.e. one reactor trip every 4,8 years only due to hardware failures.
- Main contributors to the result are Common Cause Failures of components (that are assumed to happen simultaneously).

3.2.2. Results without assuming CCF

The model for assessing the frequency of a spurious reactor trip signal by hardware failures of the same theoretical Protection System is now updated to eliminate any potential for CCF. Only independent failures are possible. This is in the logic of a probabilistic interpretation of IEC 62340 standard [1] in which CCF have to be assumed only at the moment of the demand.

The same calculation now shows significantly different conclusions:

- Frequency of spurious reactor trip due to the theoretical Protection System is 4.6E-07 per hour which corresponds to 4.0E-03 per year, i.e. one reactor trip every 250 years only due to hardware failures.
- The main contributors are independent failures of two components, the second failure occurring before the repairing of the first one, i.e. between 0 and 8 hours after first failure.

3.2. Conclusion from these assessments

As the second result is 52 times lower than the first one, it shows that this strategy for assessing CCF turns to be the key point of the correct frequency evaluation.

The frequency calculations in the first case are overestimated. This is mainly due to the use of the so called “classic” Common Cause Failure parameters and the consideration of simultaneous failures.
For these undesired events, failures are generally not hidden ones and are then detected within a few hours. Then, most of the time, the first failure is repaired before the second one appears.
This over conservatism can lead to unnecessary design choices like addition of redundancies or interlocks to minimize the frequency of an undesired event. This is then a concern for a designer and for a utility to limit this over conservatism at a maximum.

The frequency calculations in the second case are underestimated. Indeed, there remains a potential that common cause failures happen in a very short interval. This may be the case for failures corresponding for example to shutdown of systems or systems stopping to proceed. This is less credible for spurious operations of functions if designed fall-back position is non actuation of safety function, as “fail to 1” failure modes in high-quality I&C systems generally have a very low potential to happen by common cause.
This under conservatism leads to over optimistic results and, depending on what is calculated, gives a bad representation of the safety or the availability of the plant.

3.3. What can we do?

With such an amplitude in the obtained results, it appears necessary to find a way to calibrate the model. Actions are ongoing to see how benefits from operational experience can be used for the purpose of this calibration.

If it is decided to stick to the use of beta factors methodology, it appears necessary to lower the values of CCF parameters that are used in frequency calculations.

3.4. Some examples of results with lower beta values

3.4.1. Example 1

A proposal of revaluation of beta factors is:

$$\beta av_n^n = \beta_n^n / 10 \quad (5)$$

The idea is that most CCF are not simultaneous. Then it seems achievable to prove that less than 10% of them happen in an interval of 8 hours

Tuned values for βav_n^n (n from 2 to 4) are then:

$$\beta av_2^2 = 5E-03 \quad (6)$$
$$\beta av_3^3 = 2E-03 \quad (7)$$
$$\beta av_4^4 = 1E-03 \quad (8)$$

When calculating their frequencies with such common cause factors:

- Frequency of spurious reactor trip due to the theoretical Protection System is 2.8E-06 per hour which corresponds to 2.4E-02 per year, i.e. one reactor trip every 41 years only due to hardware failures.
- The resulting main contributors are still Common Cause Failures of components happening in a short interval.

3.4.2. Example 2

As βav_n^n corresponds to the percentage of cases where, if one component fails in a group of n identical components, the (n-1) other ones would fail in the few hours, it can be assumed that the higher is the n value, the higher is the factor between typical beta factors and revaluated beta factors used for frequency assessments.

A proposal is for n = 2 to 4.

$$\beta av_n^n = \beta_n^n / (5+n) \quad (9)$$

This seems reasonable at least when n is not too high.

Tuned values for βav_n^n are then:

$$\beta av_2^2 = 7{,}14E-03 \quad (10)$$
$$\beta av_3^3 = 1{,}25E-03 \quad (11)$$
$$\beta av_4^4 = 5{,}56E-04 \quad (12)$$

When calculating their frequencies with such common cause factors:

- Frequency of spurious reactor trip due to the theoretical Protection System is 6,2E-06 per hour which corresponds to 5,4E-02 per year, i.e. one reactor trip every 19 years only due to hardware failures.
- The resulting main contributors are still Common Cause Failures of components happening in a short interval.
  - In 76% of the cases, 2 failures happen in this interval
  - In 24% of the cases, at least 3 failures happen in this interval

4. CONCLUSION

This paper discusses possible management of hardware CCF in frequency calculations. It is based on a typical I&C system with a design which is similar to systems implemented in nuclear power plants. In order to be an example of calculation that can be compared to operational experience, spurious reactor trip by a Protection System is taken as example.

Result with classic beta factors appears too conservative. One solution is to assume that all failures are independent. In this case, the result is underestimated. The factor 52 between the results of both scenarios shows the importance of this parameter.

This paper also introduces work to assess relevance of different methodologies to model as adequately as possible common cause hardware failures. These methodologies can easily be compared based on their impact on calculation results (lower or higher frequency).

At this stage, it can be assumed that the final chosen solution could be:

- Use of degraded CCF factor values compared to “classic ones”.
- Use of corrective factors or functions to adapt the preliminary calculated results according to similar scenarios from operational experience.

Future work is to assess the results compared to:

- Uncertainties that can be assumed (does this methodology give reliable and trustable results or not?).
- Consistency with operational experience.
- Level of confidence that the final result is still conservative (is it possible to defend this calculation in front of a safety authority?).

Data from NUREG ([2]) is also analyzed in parallel.

The recommendations that will come from this work may be different according to the different applications and to the different components.

Additionally, there are systems where some components of a type are in operation and other ones are in standby. Components in standby are actuated in case of failure of first ones. The subject of potential Common Cause Failure between these components that are identical, but for which initial operating conditions are different, also needs to be addressed.

References

[1] IEC 62340 - Nuclear power plants – Instrumentation and control systems important to safety – Requirements for coping with common cause failure (CCF) – December 2007
[2] NUREG/CR-6268 - Common-Cause Failure Database and Analysis
System: Event Data Collection, Classification, and Coding